medialaws

Rivista di diritto dei media
2/2018 maggio

DIRETTORE
RESPONSABILE
EDITOR-IN-CHIEF
Oreste Pollicino (Università Bocconi)

DIRETTORI
EDITORS
Giulio Enea Vigevani (Università di Milano – Bicocca)
Carlo Melzi d'Eril (Avvocato in Milano)

VICEDIRETTORI
VICE-EDITORS
Marco Cuniberti (Università di Milano)
Giovanni Maria Riccio (Università di Salerno)
Marina Castellaneta(Università di Bari)
Marco Orofino (Università di Milano)

SEDE
CONTACTS
ACCMS Studio Legale
Via Podgora 13 – 20122 Milano
e-mail: submissions@medialaws.eu

REDAZIONE
EDITORIAL BOARD
Marco Bassini (*coordinatore*) (Università Bocconi)
Serena Sileoni (*vice coordinatore*) (Università di Milano – Bicocca)
Nicola Canzian (Università di Milano – Bicocca)
Giovanni De Gregorio (Università di Milano – Bicocca)
Fabio Ferrari (Università di Verona)
Valerio Lubello (Università Bocconi)
Omar Makimov Pallotta (Università di Macerata)
Silvia Vimercati (Università di Milano – Bicocca)

COMITATO SCIENTIFICO – **STEERING COMMITTEE**

Shulamit Almog (*University of Haifa*), Giuseppe Busia (*Garante per la protezione dei dati personali*), Licia Califano (*Garante per la protezione dei dati personali*), Angelo Marcello Cardani (*Autorità per le garanzie nelle comunicazioni*), Marta Cartabia (*Corte costituzionale*), Massimo Ceresa-Gastaldo (*Università Bocconi*), Pasquale Costanzo (*Università di Genova*), Marilisa D'Amico (*Università di Milano*), Filippo Donati (*Università di Firenze*), Tommaso Edoardo Frosini (*Università Suor Orsola Benincasa*), Maurizio Fumo (*Suprema Corte di Cassazione*), Alberto Maria Gambino (*Università Europea – Roma*), Michael Geist (*University of Ottawa*), Glauco Giostra (*La Sapienza – Università di Roma*), Enrico Grosso (*Università di Torino*), Uta Kohl (*University of Southampton*), Krystyna Kowalik-Bańczyk (*Tribunale dell'Unione europea*), Fiona Macmillan (*Birbeck College – University of London*), Michela Manetti (*Università di Siena*), Christopher Mardsen (*University of Sussex*), Manuel David Masseno (*Instituto Politécnico de Beja*), Roberto Mastroianni (*Università "Federico II" – Napoli*), Luigi Montuori (*Garante per la protezione dei dati personali*), Antonio Nicita (*Autorità per le garanzie nelle comunicazioni*), Miquel Pequera (*Universitat Oberta de Catalunya*), Vincenzo Pezzella (*Suprema Corte di Cassazione*), Giovanni Pitruzzella (*Autorità Garante della Concorrenza e del Mercato*), Francesco Pizzetti (*Università di Torino*), Andrea Pugiotto (*Università di Ferrara*), Margherita Ramajoli (*Università di Milano – Bicocca*), Sergio Seminara (*Università di Pavia*), Salvatore Sica (*Consiglio di Presidenza della Giustizia Amministrativa*), Francesco Viganò (*Corte costituzionale*), Lorenza Violini (*Università di Milano*), Nicolò Zanon (*Corte costituzionale*), Vincenzo Zeno-Zencovich (*Università di Roma Tre*)

COMITATO DEGLI ESPERTI PER LA VALUTAZIONE – **ADVISORY BOARD**

Maria Romana Allegri
Giulio Allevato
Ernesto Apa
Benedetta Barbisan
Fabio Basile
Marco Bellezza
Daniela Bifulco
Carlo Blengino
Monica Bonini
Irene Calboli
Simone Calzolaio
Quirino Camerlengo
Marina Caporale
Andrea Cardone
Corrado Caruso
Stefano Catalano
Adolfo Ceretti
Francesco Clementi
Giovanna Corrias Lucente
Filippo Danovi
Monica Delsignore
Giovanna De Minico
Marius Dragomir
Roberto Flor
Federico Furlan
Giovanni Battista Gallus
Marco Gambaro
Gianluca Gardini
Ottavio Grandinetti
Antonino Gullo
Simone Lonati
Erik Longo
Federico Lubian
Nicola Lupo
Paola Marsocci
Claudio Martinelli
Alberto Mattiacci
Alessandro Melchionda
Massimiliano Mezzanotte
Francesco Paolo Micozzi
Donatella Morana
Piergiuseppe Otranto
Anna Papa
Paolo Passaglia
Irene Pellizzone
Sabrina Peron
Bilyana Petkova
Marina Pietrangelo
Federico Gustavo Pizzetti
Augusto Preta
Giorgio Resta
Francesca Rosa
Andrej Savin
Salvatore Scuto
Monica Alessia Senor
Giulia Tiberi
Bruno Tonoletti
Emilio Tosi
Lara Trucco
Luca Vanoni
Gianluca Varraso
Thomas Wischmeyer

ANNO 2018 – CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

MediaLaws - Rivista di diritto dei media è una rivista quadrimestrale telematica, ad accesso libero, che si propone di pubblicare saggi, note e commenti attinenti al diritto dell'informazione italiano, comparato ed europeo.

La rivista nasce per iniziativa di Oreste Pollicino, Giulio Enea Vigevani, Carlo Melzi d'Eril e Marco Bassini e raccoglie le riflessioni di studiosi, italiani e stranieri, di diritto dei media.

I contributi sono scritti e ceduti a titolo gratuito e senza oneri per gli autori. Essi sono attribuiti dagli autori con licenza Creative Commons "Attribuzione – Non commerciale 3.0" Italia (CC BY-NC 3.0 IT). Sono fatte salve, per gli aspetti non espressamente regolati da tale licenza, le garanzie previste dalla disciplina in tema di protezione del diritto d'autore e di altri diritti connessi al suo esercizio (l. 633/1941).

Il lettore può utilizzare i contenuti della rivista con qualsiasi mezzo e formato, per qualsiasi scopo lecito e non commerciale, nei limiti consentiti dalla licenza Creative Commons "Attribuzione – Non commerciale 3.0 Italia" (CC BY-NC 3.0 IT), in particolare menzionando la fonte e, laddove necessario a seconda dell'uso, conservando il logo e il formato grafico originale.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

La qualità e il rigore scientifici dei saggi della Rivista sono garantiti da una procedura di *double-blind peer review* affidata a un comitato di esperti per la valutazione individuato secondo criteri di competenza e rotazione e aggiornato ogni anno.

MediaLaws - Rivista di diritto dei media
Regolamento per la pubblicazione dei contributi

1. "MediaLaws – Rivista di diritto dei media" è una rivista telematica e ad accesso aperto che pubblica con cadenza quadrimestrale contributi attinenti al diritto dell'informazione.

2. Gli organi della rivista sono il Comitato di direzione, il Comitato scientifico e il Comitato degli esperti per la valutazione. L'elenco dei componenti del Comitato di direzione e del Comitato scientifico della rivista è pubblicato sul sito della stessa (www.medialaws.eu/rivista). Il Comitato degli esperti per la valutazione è sottoposto ad aggiornamento una volta l'anno.

3. La rivista si compone delle seguenti sezioni: "Saggi", "Note a sentenza" (suddivisa in "Sezione Europa", "Sezione Italia" e "Sezione straniera"), "Cronache" e "Recensioni e riletture". I singoli numeri potranno altresì ospitare, in via d'eccezione, contributi afferenti a sezioni diverse.

4. La sezione "Saggi" ospita contributi che trattano in maniera estesa e approfondita un tema di ricerca, con taglio critico e supporto bibliografico.

5. La sezione "Note a sentenza" ospita commenti alle novità giurisprudenziali provenienti dalle corti italiane, europee e straniere.

6. La sezione "Cronache" ospita commenti a questioni e novità giuridiche di attualità nella dimensione nazionale, europea e comparata.

7. La sezione "Recensioni e riletture" ospita commenti di opere rispettivamente di recente o più risalente pubblicazione.

8. La richiesta di pubblicazione di un contributo è inviata all'indirizzo di posta elettronica submissions@medialaws.eu, corredata dei dati, della qualifica e dei recapiti dell'autore, nonché della dichiarazione che il contributo sia esclusiva opera dell'autore e, nel caso in cui lo scritto sia già destinato a pubblicazione, l'indicazione della sede editoriale.

9. La direzione effettua un esame preliminare del contributo, verificando l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

10. In caso di esito positivo, la direzione procede ad assegnare il contributo alla sezione opportuna.

11. I saggi sono inviati alla valutazione, secondo il metodo del doppio cieco, di revisori scelti dall'elenco degli esperti per la valutazione della rivista secondo il criterio della competenza, della conoscenza linguistica e della rotazione. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore. La direzione garantisce l'anonimato della valutazione.

12. La direzione comunica all'autore l'esito della valutazione.
Se entrambe sono positive, il contributo è pubblicato.
Se sono positive ma suggeriscono modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. La direzione si riserva la facoltà di sottoporre il contributo così come modificato a nuova valutazione, anche interna agli organi della rivista. Se solo una valutazione è positiva, con o senza modifiche, la direzione si riserva la facoltà di trasmettere il contributo a un terzo valutatore. Se entrambe le valutazioni sono negative, il contributo non viene pubblicato.

13. Per pubblicare il contributo, l'Autore deve inviare una versione definitiva corretta secondo le regole editoriali della rivista pubblicate sul sito della stessa, un abstract in lingua italiana e inglese e un elenco di cinque parole chiave. Il mancato rispetto dei criteri editoriali costituisce motivo di rigetto della proposta.

14. Le valutazioni vengono archiviate dalla direzione della rivista per almeno tre anni.

15. A discrezione della direzione, i saggi di autori di particolare autorevolezza o richiesti dalla direzione possono essere pubblicati senza essere sottoposti alla procedura di referaggio a doppio cieco ovvero essere sottoposti a mero referaggio anonimo, previa segnalazione in nota.

Saggi
Nuove tecnologie e diritti umani

14 **La "federalizzazione" dei diritti fondamentali, all'incrocio tra etica, scienza e diritto**
Antonio Ruggeri

32 **Dati, grandi dati, dati granulari e la nuova epistemologia del giurista**
Vincenzo Zeno-Zencovich

39 **Tutela dei diritti fondamentali nell'era digitale e contesto valoriale: una indagine transatlantica**
Oreste Pollicino

53 **Lo spazio digitale come oggetto di un diritto reale?**
Attilio Gorassini

64 **Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione**
Giandonato Caggiano

82 **Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione**
Marco Orofino

105 **La tutela dell'oblio tra intimità e condivisione senza filtri**
Aurora Vesto

119 **Impiego di droni armati nella lotta al terrorismo e accesso alla giustizia da parte delle vittime**
Nicola Colacino

132 **Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani**
Letizia Seminara

146 **La digitalizzazione della pubblica amministrazione**
Francesco Martines

158 **Informazione e comunicazione digitale nel processo di modernizzazione della pubblica amministrazione**
Anna Lazzaro

Saggi
L'art. 21 ha settant'anni

171 **I delitti contro il sentimento religioso: tra incriminazione dell'opinione e tutela della libertà di manifestazione del pensiero**
Fabio Basile

Saggi
Fake news, pluralismo informativo e responsabilità in rete

183 **Le *fake news* sui social network: un'analisi economica**
Vincenzo Visco Comandini

Saggi
La riforma Orlando: intercettazioni, riservatezza, diritto di cronaca

214 **Le nuove intercettazioni tra selettività arbitraria e ridimensionamento delle garanzie difensive**
Silvia Buzzelli

223 **I captatori informatici: una riforma troppo contenuta per uno strumento investigativo così pervasivo**
Barbara Indovina

Altri saggi

235 **Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-*ter*, c. 2, n. 1, c.p.)**
Sergio Seminara

251 Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations
Manuel David Masseno, Cristiana Santos

267 Economia della privacy: una rassegna della letteratura
Jacopo Arpetti

298 *Sharing economy*: l'esperienza italiana della XVII legislatura alla luce degli orientamenti europei
Guido d'Ippolito

Note a sentenza
Sezione Italia

318 La Corte costituzionale ribadisce che le esternazioni di un parlamentare non sono *legibus solutae*
Claudio Martinelli, Jessica De Vivo

324 Il *revirement* della Cassazione: la responsabilità per omesso controllo si applica al direttore della testata telematica
Silvia Vimercati

339 La posta elettronica è sempre un "mezzo di pubblicità"?
Iolanda Campolo

344 La copia cartacea dello screenshot ha valore probatorio
Andrea Ranghino

349 Responsabilità del direttore per omesso controllo e del giornalista per diffamazione: autonomia delle fattispecie e ricadute sulle formule assolutorie
Laura Ninni

354 Le testate telematiche e la tutela costituzionale
Sabrina Peron

368 Tra diritto all'oblio e libertà di informazione: la sussistenza dell'interesse pubblico alla diffusione di una notizia
Francesca Paruzzo

377 Responsabilità ISP: chi decide se un contenuto è diffamatorio?
Marco Bellezza

381 Deindicizzazione globale degli URL su Google: sì del Garante Privacy, in attesa della Corte di giustizia
Filippo Frigerio

Note a sentenza
Sezione comparata

388 Consumatori tedeschi vs. Facebook: la condanna del *social network* per violazione della normativa sul trattamento dei dati personali
Egle Urso

Note a sentenza
Sezione Europa
Corte di giustizia

394 Caso Peugeot, secondo la Corte di giustizia UE un canale promozionale su YouTube non è un servizio di media audiovisivo
Ernesto Apa

Note a sentenza
Sezione Europa
Corte europea

401 I gesti simbolici, anche se provocatori, rientrano nell'ambito della critica politica
Marina Castellaneta

410 Secret filming and the right to inform under an European constitutional perspective. The case of *Alpha Doryforiki v. Greece*
Giovanni De Gregorio

Cronache e commenti

420 Sull'eccesso di delega del decreto legislativo di adeguamento del Codice Privacy alla disciplina del Regolamento (UE) 679/2016
Giovanni De Gregorio

430 Il referendum svizzero sul canone radiotelevisivo: una conferma della centralità del servizio pubblico
Giulio Enea Vigevani

434 "Street heart": urban murals as common goods
Giovanni Maria Riccio, Federica Pezza

440 *Fake news* e libertà di informazione
Filippo Donati

447 La regolamentazione in materia di Intelligenza artificiale, robot, automazione a che punto siamo
Cecilia Trevisi

Recensioni

459 A proposito del volume "Civiltà giuridica della comunicazione"
Carlo Melzi d'Eril

Indice
Index

Articles
New technologies and human rights

14 The federalization of fundamental rights, between law, sicence and ethics
Antonio Ruggeri

32 Data, Big Data, granular data and the new legal epistemology
Vincenzo Zeno-Zencovich

39 Protection of fundamental rights in the digital age and judicial framing in a comparative perspective
Oreste Pollicino

53 The digital space
Attilio Gorassini

64 Balancing fundamental rights and protection of national security in the data retention context
Giandonato Caggiano

82 Protection of personal data and national security: some notes on a critical relationship
Marco Orofino

105 The right to be forgotten: right to be let alone and unrestricted sharing of data
Aurora Vesto

119 The use of drones in counter-terrorism operations and the access to justice for victims
Nicola Colacino

132 Secret surveillance and new technologies in the European law of human rights
Letizia Seminara

146 The impact of Information and Communication Technologies (ICT) on public authorities
Francesco Martines

158 Information and digitalization of the public authorities
Anna Lazzaro

Articles
Article 21 of the Constitution turns 70

171 The crimes against religious sentiment, between criminalizing opinions and protecting free speech
Fabio Basile

Articles
Fake news, pluralism and ISP liability

183 Fake news and social network: an economic analysis
Vincenzo Visco Comandini

Articles
The Orlando Reform: interceptions, privacy and freedom of information

214 The new legal framework of wiretapping and the rising challenges for the right to defense
Silvia Buzzelli

223 Trojan horses: a too light reform for a such pervasive investigative tool
Barbara Indovina

Other essays

235 Some observations on the crime of unauthorized access to computer or telecommunications systems committed by a public servant
Sergio Seminara

251 Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations
Manuel David Masseno, Cristiana Santos

267 Privacy and economics: an overview
Jacopo Arpetti

298 **Sharing economy: the Italian framework and the European guidelines**
Guido d'Ippolito

Notes and comments
Italy

319 **The Italian Constitutional Court rules on the limits of freedom of speech of members of Parliament**
Claudio Martinelli, Jessica De Vivo

324 **The Italian Supreme Court of Cassation's revirement: online editors are now liable for lack of control**
Silvia Vimercati

339 **The relevance of the use of email for aggravated defamation**
Iolanda Campolo

344 **The printed copy of a screenshot recognized as evidence by the Italian Supreme Court**
Andrea Ranghino

349 **The relationship between the crime of lack of control of editors and liability of journalists for defamatory statements**
Laura Ninni

354 **Constitutional guarantees and online newspapers**
Sabrina Peron

368 **Right to be forgotten and freedom of expression: the public interest in accessing information**
Francesca Paruzzo

377 **ISP liability: who determines whether a content is defamatory?**
Marco Bellezza

381 **Global delisting of URLs from Google: greenlight from the Italian Data Protection Authority, while awaiting for the Court of justice**
Filippo Frigerio

Notes and comments
Comparative Law

388 **German consumers v. Facebook: the decision of the Court of Berlin**
Egle Urso

Notes and comments
Europe
Court of Justice

394 **A channel hosting promotional videos does not amount to an audiovisual media service: the Court of Justice ruling in the Peugeot case**
Ernesto Apa

Notes and comments
Europe
European Court

401 **Setting fire to photograph of the nation's royal couple falls within the scope of political criticism, in the view of the European Court of Human Rights**
Marina Castellaneta

410 **Secret filming and the right to inform under an European constitutional perspective. The case of Alpha Doryforiki v. Greece**
Giovanni De Gregorio

New legislation

420 **The Italian legislation adapting the Data Protection Code to the GDPR and its compliance with the delegation law**
Giovanni De Gregorio

430 **Swiss vote to retain license fee for public broadcaster**
Giulio Enea Vigevani

434 **"Street heart": urban murals as common goods**
Giovanni Maria Riccio, Federica Pezza

440 Fake news and freedom of information
Filippo Donati

447 Artificial Intelligence, robotics and regulation: what's up?
Cecilia Trevisi

Recensioni

459 Book review: Civiltà giuridica della comunicazione by Giovanni Paolo Accinni
Carlo Melzi d'Eril

Anche questo numero della *Rivista di diritto dei media* raccoglie contributi che intercettano diversi ambiti nei quali le innovazioni legislative e giurisprudenziali si appalesano di grande momento. Il fascicolo comprende, anzitutto, una serie di scritti in cui sono confluite le riflessioni maturate dal convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno", organizzato lo scorso anno presso l'Università degli Studi di Messina sotto il coordinamento della prof.ssa Carmela Panella, cui va il nostro sentito ringraziamento. Gli atti del convegno offrono una panoramica sulla complessità del rapporto tra *diritto*, scienza e *diritti* rispetto a una molteplicità di settori, fra cui spiccano la protezione dei dati personali e la tutela della riservatezza, che rivestono un'importanza particolare in questo momento storico alla luce dell'applicazione del nuovo Regolamento generale per la protezione dei dati personali ("GDPR").

In continuità con il numero precedente, nella sezione dedicata ai saggi è inoltre dato spazio a diversi focus tematici: i settant'anni dell'art. 21 della Costituzione; il dibattito sul contrasto alla diffusione di *fake news*; la riforma Orlando.

Significativi anche gli sviluppi giurisprudenziali registratisi negli ultimi mesi di cui questo numero dà conto. In materia penale, si segnala una decisione della Corte di Cassazione sull'applicazione dell'art. 57 c.p. (reato di omesso controllo) al direttore della testata telematica, che muta un orientamento di segno opposto che si era consolidato negli ultimi anni. In ambito civile, si registra un'importante ordinanza della Cassazione nel caso *Venditti* che si sofferma sul c.d. "diritto all'oblio" e sul rapporto con il diritto di cronaca. Invece il Tribunale di Milano, con un'ordinanza della sezione I civile, è ritornato a occuparsi dell'estensione delle garanzie costituzionali per la stampa nei confronti dei giornali telematici. Inoltre, è annotata una rilevante decisione della Corte costituzionale sull'ambito della insindacabilità per opinioni espresse nell'esercizio delle funzioni parlamentari, originata dalla vicenda che vedeva coinvolti il sen. Calderoli e l'on.le Kyenge.

Anche nella sezione dedicata a cronache e commenti si rassegnano alcuni significativi svolgimenti a livello domestico e comparato. Meritano segnalazione, tra le più attuali, le vicende dell'adeguamento della legislazione italiana al famigerato GDPR e del referendum svizzero sulla proposta di abolizione del canone per il servizio pubblico radiotelevisivo.

Sono stati sottoposti a procedura di referaggio, in conformità al Regolamento della Rivista, i saggi di: Oreste Pollicino, Attilio Gorassini, Giandonato Caggiano, Marco Orofino, Aurora Vesto, Nicola Colacino, Letizia Seminara, Francesco Martines, Anna Lazzaro, Fabio Basile, Vincenzo Visco Comandini, Silvia Buzzelli, Barbara Indovina, Sergio Seminara, Guido d'Ippolito, Manuel David Masseno e Cristiana Santos, Jacopo Arpetti.

La direzione ha ritenuto di dispensare dalla procedura di referaggio, in conformità all'art. 15 del Regolamento, i saggi di Antonio Ruggeri e Vincenzo Zeno-Zencovich.

Su decisione della direzione, sono state altresì sottoposte alla suddetta procedura le note a sentenza di Silvia Vimercati, Sabrina Peron e Francesca Paruzzo.

Saggi

Nuove tecnologie e diritti umani

La "federalizzazione" dei diritti fondamentali, all'incrocio tra etica, scienza e diritto*

Antonio Ruggeri

Abstract

Lo scritto preliminarmente evidenzia che l'ottimale riconoscimento dei nuovi diritti fondamentali, specie di quelli maggiormente toccati dallo sviluppo scientifico e tecnologico, è dato dal riferimento a *consuetudini culturali* invalse nel corpo sociale e delle quali si rendano quindi interpreti e garanti, ciascuno per la propria parte, legislatore e giudici. Si segnala quindi come la tutela dei diritti stessi resti demandata alla "leale cooperazione" di tutti gli operatori. Al legislatore spetta infatti la posizione di discipline duttili ed essenziali, ai giudici poi la loro specificazione-attuazione congrua rispetto ai casi: tutti comunque dovendo fare i conti con lo sviluppo scientifico e tecnologico ed attingendo alle illuminanti indicazioni offerte dall'etica. In questo quadro, si assiste alla "federalizzazione" dei diritti, testimoniata da "catene" di atti giurisdizionali che vengono a formazione a più livelli ordinamentali e istituzionali, all'insegna del principio della massimizzazione della tutela. Un modello, questo, che risulta particolarmente avvalorato nel presente contesto segnato da una integrazione sovranazionale avanzata e dallo sviluppo impetuoso della scienza e della tecnica, pur sempre bisognoso tuttavia di alimentarsi e rigenerarsi costantemente dall'etica.

The article argues that the protection of new fundamental rights, most notably of those significantly affected by the advancements in science and technology, relies on the reference to cultural attitudes that are seriously taken into account by lawmakers and courts. Thus, it is said that the effective protection of the same is grounded on the fair cooperation among all the relevant actors. Whereas lawmakers are expected to lay down flexible and minimal legal frameworks, it is up to courts to implement the same with respect to specific cases. Both lawmakers and courts, however, should face the challenges raised by new technologies by taking ethics into consideration. In this respect, a federalization of fundamental rights is witnessed by the emergence at different levels of a "chain" of case law aimed at granting fundamental rights the highest degree of protection. This model is stimulated by the process of supranational integration and is spurred by the unprecedented developments in science and technology; however, it still needs to be grounded on the driving force of ethics.

Sommario

1. Alla ricerca della ottimale salvaguardia dei diritti fondamentali attraverso il concorso e il giusto dosaggio di etica, scienza e diritto. – 2. Il rischio della deriva soggettivistica in ordine alla ricognizione dei diritti fondamentali e il modo più adeguato a pararlo, facendo riferimento a consuetudini culturali di riconoscimento invalse nel corpo sociale e delle quali si rendano quindi interpreti e garanti gli operatori (in ispecie, i giudici). – 3. La salvaguardia dei diritti attraverso la cooperazione di legislatori e giudici: agli uni

* L'articolo è stato inviato su richiesta della direzione e pertanto non è stato sottoposto a referaggio.

spettando la posizione della disciplina iniziale, di principio, e agli altri la produzione delle regole idonee a svolgerli in relazione alle peculiari esigenze dei casi, tutti comunque dovendo fare i conti con lo sviluppo scientifico e tecnologico ed attingendo alle illuminanti indicazioni offerte dall'etica. – 4. La "federalizzazione" dei diritti, testimoniata dalle "catene" di atti giurisdizionali che vengono a formazione a più livelli ordinamentali e istituzionali, all'insegna del principio della massimizzazione della tutela, quale si mette a fuoco e realizza nelle singole esperienze processuali, ricevendo luce ed orientamento sia dalla scienza che dall'etica. – 5. La lezione che viene da Corte cost. n. 84 del 2016 e i tre insegnamenti che la stessa ci somministra. – 6. Riassumendo e concludendo: le conferme che vengono al modello "federale" di salvaguardia dei diritti dal presente contesto segnato da una integrazione sovranazionale avanzata e dallo sviluppo impetuoso della scienza e della tecnica, pur sempre bisognoso tuttavia di alimentarsi e rigenerarsi costantemente dall'etica.

Keywords: Modello "federale" dei diritti fondamentali, Tutela dei diritti all'incrocio tra etica, scienza e diritto, Nuove tecnologie, Etica, Scienza e tecnica

1. Alla ricerca della ottimale salvaguardia dei diritti fondamentali attraverso il concorso e il giusto dosaggio di etica, scienza e diritto

Siamo oggi chiamati nuovamente a confrontarci su questioni plurime e complesse che fanno capo al tema dei rapporti tra la tutela dei diritti fondamentali e lo sviluppo scien-

tifico e tecnologico[1], questioni che si pongono su un terreno infido e scivoloso, reso ancora più tale dalle non poche ed animate discussioni che si pongono in relazione a ciascuno dei termini della relazione in parola e, più ancora, agli stessi nella loro combinazione.

Scienza e diritto non sono tuttavia, per diffuso riconoscimento, i soli attori sulla scena: accanto ad essi e con centralità di ruolo si pone anche l'etica, sicché i rapporti in parola possono essere visti, così come lo sono, da tre angoli visuali; ed è chiaro che i modi d'impostare lo studio e i suoi esiti ricostruttivi possono risultare (ed effettivamente risultano) non coincidenti. Non si tratta qui, ovviamente, di andare a stabilire chi ha torto e chi ragione: i punti di vista possono essere legittimamente divergenti, per la banale ragione che diversi sono i metodi di esame messi in atto, gli strumenti di lavoro, i linguaggi adoperati, il modo complessivo con cui è trattata la sostanza in gioco dagli stessi evocata.

Non mi riconosco alcun titolo per tornare a riguardare a questi rapporti da un angolo visuale diverso da quello del solo ambito a me familiare, il giuridico. Peraltro, anche da quest'ultimo (così come dagli altri), in realtà, non v'è – come si sa – un solo punto di vista: il pluralismo metodologico-teorico, per fortuna, attraversa e copre ciascuno di tali ambiti e tutti assieme. Siamo, insomma, tutti divisi, anche (e, forse, soprattutto)

---

[1] Il tema è da tempo oggetto di plurime e varie osservazioni: solo per una prima informazione e con specifico riguardo al ruolo di tecnici e scienziati nel corso delle esperienze processuali, v. G. Silvestri, *Scienza e coscienza: due premesse per l'indipendenza del giudice*, in *Diritto pubblico*, 2, 2004, 411 ss.; A. D'Aloia (a cura di), *Bio-tecnologie e valori costituzionali. Il contributo della giurisprudenza costituzionale*, Torino, 2005; G. D'Amico, *Scienza e diritto nella prospettiva del giudice delle leggi*, Messina, 2008, e, dello stesso, ora, *Dalla libertà della ricerca scientifica al diritto alla scienza: un antidoto allo* scientific divide*?*, in corso di stampa in *Biolaw Journal* (www.biodiritto.org); E. Castorina, *Scienza, tecnica e diritto costituzionale*, in www.rivistaaic.it, 4, 2015; S. Penasa, *Giudice "Ercole" o giudice "Sisifo"? Gli effetti del dato scientifico sull'esercizio della funzione giurisdizionale in casi scientificamente connotati*, in www.forumcostituzionale.it, 17 dicembre 2015; L. Chieffi (a cura di)., *La medicina nei tribunali*, in, Bari, 2016; L. Chieffi, *Scientific questions nel diritto giurisprudenziale*, in www.federalismi.it, 7, 2017; G. Sorrenti, *Note minime sul rapporto tra ius, ethos e scientia*, in www.osservatorioaic.it, 2, 2017. Infine, tra i contributi alle nostre Giornate, A. Giusti, *Il giudice, la persona e i temi eticamente sensibili*, in *paper*. Quanto, poi, al peso della scienza, rispettivamente, nella giurisprudenza costituzionale e in quella eurounitaria, v., nell'ordine, A. Iannuzzi, *Istruttoria e valutazioni tecnico-scientifiche*, relazione al Convegno del Gruppo di Pisa su *La Corte costituzionale e i fatti: istruttoria ed effetti delle decisioni*, Milano, 9-10 giugno 2017, in www.gruppodipisa.it, e F. Munari, *Il ruolo della scienza nella giurisprudenza della Corte di giustizia in materia di tutela della salute e dell'ambiente*, in *Il Diritto dell'Unione europea*, 1, 2017, 129 ss. Con specifico riguardo alle esperienze d'inizio-vita, cui si farà più avanti cenno, v., poi, nella ormai incontenibile lett., S. Agosta, in molti scritti, tra i quali *Bioetica e Costituzione*, I, *Le scelte esistenziali di inizio-vita*, Milano, 2012, e *Spingersi dove neppure alle più avanzate acquisizioni tecnico-mediche è consentito: la sfida del diritto all'epoca della rivoluzione biologica*, in www.rivistaaic.it, 1, 2014, , spec. al § 2, e, ora, *In fuga dai divieti: un'occasione di riflessione sulla proibizione italiana della gestazione per altri*, in corso di stampa in *Quaderni costituzionali*, 1, 2018; S. Penasa, in numerosi contributi, tra i quali l'ampio studio monografico su *La legge della scienza: nuovi paradigmi di disciplina dell'attività medico-scientifica. Uno studio comparato in materia di procreazione medicalmente assistita*, Napoli, 2015; S. Agosta - G. D'Amico - L. D'Andrea (a cura di)., *La procreazione medicalmente assistita. Bilancio di un'esperienza, problemi e prospettive*, Napoli, 2017; B. Liberali, *Problematiche costituzionali nelle scelte procreative. Riflessioni intorno alla fecondazione medicalmente assistita e all'interruzione volontaria di gravidanza*, Milano, 2017; S. Niccolai - E. Olivito (a cura di), *Maternità, filiazione, genitorialità. I nodi della maternità surrogata in una prospettiva costituzionale*, Napoli, 2017; infine, A.C. Nazzaro, *Discrezionalità legislativa e ruolo del giudice nella nuova dimensione (bio)etica della famiglia*, in www.rivistaaic.it, 1, 2018. Tra i contributi alle nostre Giornate, v. A. Di Stasi, *La nozione di embrione umano nella giurisprudenza delle corti europee*; F. Perrini, *Il tentativo della Corte europea dei diritti dell'uomo di comporre il contrasto tra scienza e diritto: le principali problematiche sollevate dalla legge italiana sulla procreazione medicalmente assistita*; A. La Spina, *Tecnologie riproduttive e circolazione dello status della persona*; A. Marchese, *La fecondazione post mortem: esiste un confine biologico per l'inizio della vita umana*; S. Agosta, *Il perdurante allontanamento tra diritto vivente giurisprudenziale e vigente legislativo sulla surrogazione di maternità (ed i possibili modi di ricongiungimento in una prospettiva costituzionalmente orientata)*, tutti in *paper*.

noi giuristi. Gli scienziati, infatti, sono proprio quelli meno esposti ad un pluralismo esasperato ed incontrollabile: magari, ci mettono molto tempo prima di mettersi d'accordo su certe cose; e non saprei ora dire se sono più quelle su cui ormai si registra un universale consenso ovvero le altre su cui ancora si hanno accese dispute o, diciamo pure, si brancola nel buio pesto. Certo è però che ormai nessuno afferma che la terra è un disco piatto o che il sole gira attorno ad essa. A certe conclusioni, sulle quali gli studiosi convengono, si perviene alle volte battendo vie diverse ma l'importante è appunto intendersi sul risultato. Gli studiosi di discipline umano-sociali, invece, possono, per loro strutturale vocazione, legittimamente restare – dove più e dove meno – divisi. Rammento, al riguardo, una bellissima pagina di V.E. Orlando in cui si coglieva efficacemente la diversità dei modi di operare di un filosofo e di uno scienziato: il secondo – soleva dire il fondatore della scienza del diritto pubblico in Italia – non può mai «servirsi di una spugna per cancellare da una lavagna tutto quello che c'era scritto; … ciò può esser forse possibile per un filosofo, ma non per uno scienziato, poiché quel processo distruttivo, se fosse giustificato, negherebbe che una scienza fosse preesistita»[2]. Il vero è, però, che noi giuristi (segnatamente, quelli di discipline positive), per un verso, non discutiamo più su alcune categorie che consideriamo acquisite al nostro patrimonio scientifico e delle quali quotidianamente ci avvaliamo (ad es., che esistano accanto alle persone fisiche le persone giuridiche o che esistano le fonti del diritto) ma seguitiamo – dicevo, per fortuna – a ripensare criticamente anche a taluni concetti fondamentali delle nostre discipline (ad es., su cosa siano o quali siano i diritti fondamentali o quali siano le fonti del diritto).

Il punto critico attorno al quale ruota il nostro confronto di oggi può riassumersi nella seguente domanda: quali categorie del passato dobbiamo abbandonare ovvero fare oggetto di corposo aggiustamento e di quali nuove categorie abbiamo bisogno in relazione allo (e per effetto dello) sviluppo scientifico e tecnologico?

In questa domanda – come si vede – l'etica è del tutto assente. La mia idea è tuttavia che tanto coloro che fanno scienza così detta (e impropriamente detta) "esatta" quanto coloro che fanno scienza giuridica (e umano-sociale in genere) non possono restare insensibili all'influenza dell'etica, neppure se lo vogliono. Magari, cioè, non ne hanno piena consapevolezza ma, per il fatto di essersi formati in un certo contesto culturale comunque attraversato e pervaso dall'etica, ne restano pur sempre impressionati. Può essere (ed effettivamente è) diversa la misura di siffatto condizionamento, non la sua esistenza.

V'è un dato sicuro che può addursi a sostegno di quest'assunto; e ne dico ora restando – per la ragione sopra enunciata – al solo ambito giuridico in seno alla quale questa succinta riflessione si situa e svolge. Ed è che le Carte che danno il riconoscimento dei diritti fondamentali, la Costituzionale come pure quelle di origine esterna, non sono altro che la positivizzazione dell'etica, o diciamo meglio di "un'etica": la prima e più

[2] *Introduzione* a G. Jellinek, *La dottrina generale del diritto dello Stato*, tr. it. a cura di M. Petrozziello, Milano, 1949, IX (ho fatto più volte richiamo di questo pensiero, a partire dal mio *Il Consiglio dei ministri nella Costituzione italiana*, Milano, 1981, 4 in nt. 5). Si è di recente intrattenuto, con fini argomenti, sui problemi del metodo A. Morelli, *Come lavora un costituzionalista? Per un'epistemologia della scienza del diritto costituzionale*, in *Quaderni costituzionali,* 3, 2016, 513 ss. e, dello stesso, *Comparazione e ipotesi scientifiche: appunti per uno studio sulle forme di governo*, in www.federalismi.it, 1, 2017.

genuina ed espressiva traduzione in termini giuridicamente significanti di un progetto etico grandioso ed armonioso negli elementi in cui si articola e che ha quale suo punto costante di riferimento la persona umana, la sua vita, la dignità, insomma un "progetto etico antropocentrico". Perciò, i diritti fondamentali null'altro sono – a me pare[3] –, *in nuce*, se non bisogni elementari dell'uomo (e non – si badi – del solo cittadino[4]) senza il cui appagamento l'esistenza stessa non sarebbe – secondo la efficace sintesi che ne fa l'art. 36, c. 1, della nostra legge fondamentale – «libera e dignitosa».

Sia che si guardi ai diritti fondamentali per il modo con cui è ad essi offerta tutela in seno alla Comunità internazionale o ad organizzazioni sovranazionali, quale l'Unione europea, sia che si ponga mente alla tutela che viene dalla Costituzione e sia pure che si considerino congiuntamente l'una e l'altra protezione, nelle forme peculiari ma anche integrate cui esse danno vita[5], ebbene non è possibile tenere innaturalmente distinto o, peggio, contrapposto il punto di vista etico rispetto a quello giuridico. Nel momento stesso in cui l'etica si è fatta (e fa) diritto, per il tramite delle Carte suddette, il diritto, a sua volta, si fa (e deve farsi) etica, che lo voglia o no; e che lo vogliano o no sono appunto chiamati a volgere verso di essa lo sguardo coloro – studiosi ed operatori – che fanno del diritto il loro quotidiano lavoro.

Tutto ciò posto, lo sviluppo scientifico e tecnologico ci obbliga però – come si diceva – a ripensare *ab ovo* persino alle nostre più antiche e salde credenze. I cultori di ciascuno dei tre ambiti qui posti a raffronto difficilmente riconosceranno la *primauté* culturale di coloro che operano fuori del proprio; si tratta, nondimeno, di stabilire fino dove si può (e deve) dar spazio ad indicazioni provenienti *ab extra*, quale uso cioè farne per le esigenze peculiari di ciascun ambito.

Non ho dubbi a riguardo del fatto che la soluzione più adeguata sia quella che induce a ricercare il giusto equilibrio, il dosaggio opportuno tra componente etica, scientifica, giuridica, al fine dell'ottimale appagamento dei diritti, specie di quelli che, in misura maggiore di altri, sono esposti al condizionamento dell'etica per un verso, dello sviluppo scientifico e tecnologico per un altro. L'importante per il giurista, teorico od operatore che sia, è riconoscere con umiltà di non poter fare a meno dell'apporto che gli può esser offerto da chi giurista non è. L'apertura verso le suggestioni ed indicazioni provenienti da altri ambiti non è (e non dev'essere) incondizionata ma vigile ed oculata;

---

[3] Mi sono sforzato di argomentare questa tesi nel mio *Cosa sono i diritti fondamentali e da chi e come se ne può avere il riconoscimento e la tutela*, Intervento al Convegno del Gruppo di Pisa su *Cos'è un diritto fondamentale?*, Cassino 10-11 giugno 2016, in Consulta OnLine, II, 30 giugno 2016, 263 ss.

[4] Su questo punto, di cruciale rilievo, non posso ora tornare ad indugiare. È vero che ci sono diritti non egualmente riconosciuti a tutti (a partire – come si sa – da quelli politici); peraltro, anche in ambito economico-sociale non poche differenze (o, diciamo pure, discriminazioni) residuano, non soltanto tra cittadini e non cittadini ma persino in seno a questi ultimi. Il vero è che l'ambizioso e nobile disegno volto a fare della nostra una società di persone liberi ed eguali va portandosi avanti con non poca fatica e vero e proprio travaglio ma è ancora lontano dalla meta vagheggiata dal Costituente e mirabilmente enunciata nella "coppia assiologica fondamentale" – come a me piace chiamarla – di cui agli artt. 2 e 3 della Carta, nelle loro mutue ed inscindibili implicazioni (su di che, v., sopra tutti, G. Silvestri, *Dal potere ai princìpi. Libertà ed eguaglianza nel costituzionalismo contemporaneo*, Roma-Bari, 2009).

[5] Secondo una ispirata affermazione contenuta in Corte cost., 27 ottobre 1999, n. 388 la Costituzione e le altre Carte dei diritti «si integrano reciprocamente nella interpretazione». Purtroppo, come l'esperienza ha più volte confermato, la stessa giurisprudenza non sembra essere sempre rimasta fedele a questa esigente direttiva metodica d'azione.

in particolare, l'attenzione costante nei riguardi delle indicazioni date dagli scienziati non deve far perdere di vista quello che è un principio fondamentale che presiede allo svolgimento dell'attività scientifica, lo orienta e controlla, il principio della possibile falsificazione delle risultanze dell'attività stessa, da cui trae quindi giustificazione e alimento il principio giuridico di precauzione[6]. E non deve neppure portare a trascurare il punto di vista etico, proprio perché – come si diceva – ad esso danno forma e voce i massimi documenti normativi, le Carte dei diritti; ed "eticamente orientata" ha, perciò, da essere l'interpretazione di tali documenti, più ancora di quanto pure non sia tenuta ad essere l'interpretazione di altri[7]. La qual cosa, ad ogni buon conto, non può portare alla sopraffazione del punto di vista etico su quello giuridico al punto di portare all'abbandono dei vincoli che discendono da canoni giuridici indisponibili, quali quelli che presiedono all'interpretazione dei testi normativi[8] o all'esercizio delle pubbliche funzioni[9] e, in generale, alla tipicità dei ruoli istituzionali[10]: canoni che, nondimeno, sovente vengono trasgrediti non già in nome dell'etica ma per ragioni contingenti (e alle volte inconfessabili) con essa frontalmente contrastanti.

---

[6] Un campo di esperienza nel quale il principio in parola pone inquietanti e laceranti interrogativi alle nostre coscienze è quello su cui prendono forma e giungono a maturazione le vicende d'inizio e fine-vita. Si pensi solo alla questione assai vessata riguardante la sorte degli embrioni non impiantati, in relazione alla quale si è avuta una discussa (e discutibile) pronunzia della Consulta cui si farà richiamo più avanti, o al grumo di problemi relativi al fine-vita, laddove il principio di precauzione dovrebbe indurre a somma vigilanza prima di far luogo a decisioni ahimè irreversibili. Come si vedrà a momenti, si tratta allora di stabilire a chi possa riconoscersi il titolo di assumere decisioni siffatte e in che modo si possa (e debba) al riguardo procedere.

[7] È evidente, infatti, che i testi di legge – per fare ora solo un esempio – richiedono di essere intesi alla luce della Costituzione e delle altre Carte, in applicazione cioè della tecnica comunemente chiamata dell'interpretazione conforme [in merito alla quale, tra i molti altri, G. Sorrenti, *L'interpretazione conforme a Costituzione*, Milano, 2006 e, della stessa, *La Costituzione "sottintesa"*, in Aa. Vv., *Corte costituzionale, giudici comuni e interpretazione adeguatrice*, Milano, 2010, 3 ss., e *La (parziale) riconversione delle "questioni di interpretazione" in questioni di legittimità costituzionale*, in Consulta OnLine, 2, 2016, 293 ss.; M. Luciani, *Interpretazione conforme a Costituzione*, in *Enciclopedia del diritto.*, *Ann*ali, IX (2016), 391 ss., e, ora, G. Repetto, *Il canone dell'incidentalità costituzionale. Trasformazioni e continuità nel giudizio sulle leggi*, Napoli, 2017, 99 ss.; con specifico riferimento all'ordinamento dell'Unione, v. G. Pistorio, *Interpretazione e giudici. Il caso dell'interpretazione conforme al diritto dell'Unione europea*, Napoli, 2012, e A. Bernardi (a cura di), *L'interpretazione conforme al diritto dell'Unione europea. Profili e limiti di un vincolo problematico*, Napoli 2015]. L'orientamento etico della interpretazione delle Carte, perciò, naturalmente si trasmette a cascata all'interpretazione delle fonti restanti che da quelle traggono giustificazione e alimento.

[8] Così, ad es., non può revocarsi in dubbio che la lettera degli enunciati delimiti pur sempre, in maggiore o minore misura, l'area entro la quale va effettuata la ricerca dei loro significati, non potendosi convertire innaturalmente l'interpretazione nella sostanziale riscrittura dei testi.

[9] La questione si pone in termini pressanti in special modo per la giurisdizione e, con particolare gravità, per la giurisdizione costituzionale, essendosi assistito in più occasioni ad una sua forte torsione ad opera dello stesso giudice delle leggi, per effetto della quale l'anima politica ha preso il sopravvento su quella giurisdizionale (la più emblematica testimonianza di questo *trend* che parrebbe non avere fine e non conoscere confini si è avuta, ad avviso di molti, con Corte cost., 11 febbraio 2015, n. 10).

[10] La confusione dei ruoli, in talune congiunture, è apparsa tale da portare un'attenta dottrina a teorizzare questo stato di cose, assumendo che la stessa Carta costituzionale non consentirebbe di distinguere in modo netto tra funzione di garanzia e funzione di direzione politica (O. Chessa, *Il Presidente della Repubblica parlamentare. Un'interpretazione della forma di governo*, Napoli, 2010). Senza far passare sotto silenzio carenze di dettato esibite dalla Carta e fattesi col tempo viepiù evidenti, vengono tuttavia così ad imputarsi ad essa responsabilità che sono invece degli operatori e del sistema politico da cui le attività di quelli traggono alimento e orientamento. Si tornerà, ad ogni buon conto, sul punto di cruciale rilievo più avanti, spec. sul finire di questa riflessione.

2. Il rischio della deriva soggettivistica in ordine alla ricognizione dei diritti fondamentali e il modo più adeguato a pararlo, facendo riferimento a "consuetudini culturali" di riconoscimento invalse nel corpo sociale e delle quali si rendano quindi interpreti e garanti gli operatori (in ispecie, i giudici)

Dalle notazioni appena svolte, seppur bisognose di ben altro approfondimento di quello che è qui consentito, possono di già aversi utili indicazioni per la soluzione di alcune questioni aventi specifico rilievo istituzionale, in particolare di due, peraltro tra di loro strettamente intrecciate: l'una riguardante il modo con cui la tutela internazionale e sovranazionale si pone in rapporto a quella costituzionale e nazionale in genere e l'altra riguardante il modo con cui giudici e legislatori, quale che sia il livello ordinamentale al quale operano, sono chiamati ad operare al fine di assicurarla. Al fondo, infatti, di tali questioni sta proprio quella di ordine generale, metodologico, relativa alla misura in cui studiosi ed operatori del diritto devono aprirsi alle indicazioni di natura etica e scientifico-tecnologica.

Non ho dubbi a riguardo del fatto che la selezione in seno al materiale copioso di risultati offerti dagli scienziati debba aver luogo applicando con somma oculatezza il criterio del maggior credito possibile dagli stessi riscosso, vale a dire della loro diffusione e del loro radicamento, nella massima misura consentita dalle condizioni oggettive date. D'altronde, questo stesso è, a mio modo di vedere, il metro da utilizzare con profitto al fine di stabilire se un certo bisogno o una certa aspettativa compone, o no, un autentico diritto fondamentale, specificamente laddove non soccorra allo scopo il riconoscimento positivo ad opera di una Carta dei diritti ovvero per mano del legislatore[11].

Una delle critiche più ricorrenti avverso il c.d. strapotere dei giudici è proprio quella che colpisce la loro vocazione (a dire di molti, irrefrenabile) ad "inventarsi", al posto del legislatore, ad ogni piè sospinto nuovi diritti, apprestando loro una tutela che essi non meriterebbero (alle volte, anzi, si è in presenza di comportamenti che richiederebbero piuttosto di essere sanzionati). È chiaro, infatti, che, quando la società è divisa, la scelta del decisore di turno riceve il plauso convinto da parte di uno schieramento e la

[11] … le cui opzioni – è appena il caso qui di rammentare – restano nondimeno soggette al sindacato di costituzionalità; e, poiché a quest'ultimo vanno incontro anche quelle operate con legge costituzionale, la questione definitoria di fondo, relativa a ciò che è in sé e per sé un diritto fondamentale rimane, e – come si vedrà a momenti – richiede di appoggiarsi a fondamento ancora più solido di quello che può esser offerto da qualsivoglia strumento positivo, ferma ad ogni buon conto restando la presunzione di validità che gioca pur sempre a beneficio di quest'ultimo.

Tutto ciò posto, non è poi, ovviamente, di secondario rilievo stabilire se il riconoscimento di un nuovo diritto fondamentale richieda il ricorso alla procedura aggravata predisposta per la venuta alla luce delle leggi costituzionali ovvero se possa aversi a mezzo di leggi comuni; ed è appena il caso qui di accennare di passaggio al fatto che, per il primo corno dell'alternativa, anche le Carte dei diritti aventi origine esterna richiederebbero di essere eseguite con leggi approvate con la medesima procedura. Plurime e convergenti ragioni, altrove rappresentate, depongono a mia opinione proprio a favore di questa tesi, che nondimeno – come si sa – non trova riscontro nell'esperienza, come pure sollecitano, in vista del raggiungimento di un adeguato equilibrio istituzionale, a porre mano con urgenza all'aggiornamento del catalogo dei diritti fondamentali enunciati in Costituzione (la qual cosa è da molti esclusa in partenza, in forza dell'assiomatico convincimento che sulla parte sostantiva – e meno che mai sui principi fondamentali della Carta – non possa esercitarsi il potere di revisione costituzionale).

critica aspra da parte del fronte opposto.

La definizione sopra data di ciò che è un diritto fondamentale – com'è chiaro – non risolve il problema ma lo sposta in avanti: come facciamo, dunque, a stabilire quali bisogni elementari dell'uomo sono davvero tali e non danno perciò modo, se non sufficientemente appagati, di condurre un'esistenza «libera e dignitosa»? Cosa s'intende, cioè, con questa locuzione?

Ora, la migliore risorsa di cui disponiamo contro una deriva soggettivistica esasperata e, dunque, a conti fatti, contro l'arbitrio dell'interprete e decisore di turno[12] è data proprio da un diffuso e radicato consenso formatosi attorno alla natura e finalità di tali bisogni tanto in seno al corpo sociale quanto – qui è il punto – specificamente nella sua parte costituita dagli uomini di cultura che fanno dell'etica e della scienza il loro impegno di lavoro. I bisogni in discorso si convertono, dunque, in diritti fondamentali per effetto di "consuetudini culturali" ampiamente accreditate e sorrette dalla più larga e convinta adesione sociale[13].

Se si conviene su questa premessa, che è di metodo prima ancora che di teoria, molte questioni possono essere avviate lungo i giusti binari in vista di una loro complessiva e soddisfacente soluzione.

Al piano dei rapporti inter-ordinamentali (segnatamente, per il modo con cui ad essi danno vita le Corti europee e quelle nazionali), è all'insegna del parametro suddetto che può, ad es., essere assoggettato a verifica il modo con cui la Corte dell'Unione fa luogo alla ricognizione (*rectius*, elaborazione) delle c.d. "tradizioni costituzionali comu-

[12] … tanto più, poi, laddove dovesse trattarsi di un decisore avverso le cui pronunzie non è previsto alcun sindacato da parte di altri operatori, esponendosi unicamente alla critica diffusa degli uomini di cultura (la qual cosa, peraltro, non rimane alle volte sterile, potendo col tempo portare a mutamenti d'indirizzo nella pratica giuridica). Il rischio è, infatti, che, se non si attivano gli opportuni anticorpi (nel senso che si preciserà tra un momento nel testo), i massimi garanti innaturalmente si convertano in mostruosi poteri costituenti permanenti, riscrivendo a piacimento le Carte per la cui salvaguardia ed affermazione sono stati istituiti. Mi sovviene spesso, quando parlo di queste cose, l'angoscioso interrogativo posto nella VI Satira di Giovenale, al quale pur tuttavia occorre sforzarsi di dare risposta: «*quis adnotabit ipsos adnotatores?*».

[13] L'essenza della Costituzione – negli ordinamenti di tradizioni liberali, i diritti fondamentali – si trova dunque racchiusa negli strati più profondi del corpo sociale e si tratta quindi di stabilire quali sono i modi più idonei a portarla alla luce e rappresentarla. *Nihil novi sub soli*, come si vede: già nella tradizione romanistica e quindi secondo l'insegnamento dei massimi cultori della scienza del diritto pubblico in Italia (part., V.E. Orlando e S. Romano), al diritto in genere e al diritto costituzionale in ispecie veniva demandato il compito di disvelare ciò che è profondamente radicato nel corpo sociale. Di questa concezione, ancora oggi, si fa portatrice una dottrina particolarmente accreditata (P. Grossi). Ho ripercorso questa vicenda nel mio *La "materia" costituzionale, i modi della sua trattazione manualistica, i segni lasciati dal contesto politico-istituzionale sull'una e sugli altri (profili storico-teorici)*, in www.rivistaaic.it, 4, 2017, e *ivi* riferimenti.

ni"[14], nonché dei principi di struttura dei singoli Stati membri, cui fa riferimento l'art. 4.2 TUE[15], i quali peraltro molte volte rifluiscono nelle prime, secondo quanto è stato da ultimo confermato con riguardo al principio di legalità in materia penale dal caso *Taricco*[16]. Dal suo canto, anche la Corte EDU rilegge e filtra la Convenzione facendo applicazione del criterio del consenso e rimettendosi in considerevole misura al margine

[14] Sul rilievo che queste ultime assumono pur dopo la venuta alla luce della Carta dell'Unione, v., sopra tutti, i contributi di L. Trucco, *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione europea. Un'analisi delle strategie argomentative e delle tecniche decisorie a Lussemburgo*, Torino, 2013 e O. Pollicino, *Corte di giustizia e giudici nazionali: il moto "ascendente", ovverosia l'incidenza delle "tradizioni costituzionali comuni" nella tutela apprestata ai diritti dalla Corte dell'Unione*, in L. D'Andrea - G. Moschella - A. Ruggeri - A. Saitta (a cura di), *Crisi dello Stato nazionale, dialogo intergiurisprudenziale, tutela dei diritti fondamentali*, Torino, 2015, 93 ss., e *Della sopravvivenza delle tradizioni costituzionali comuni alla Carta di Nizza: ovvero del mancato avverarsi di una (cronaca di una) morte annunciata*, in L. D'Andrea - G. Moschella - A. Ruggeri - A. Saitta (a cura di), *La Carta dei diritti dell'Unione Europea e le altre Carte (ascendenze culturali e mutue implicazioni)*, Torino, 2016, 91 ss.; cfr., inoltre, M. Cartabia, *Convergenze e divergenze nell'interpretazione delle clausole finali della Carta dei diritti fondamentali dell'Unione europea*, in www.rivistaaic.it, 3, 2017, , 4 ss.; P. Mori, *Taricco II o del primato della Carta dei diritti fondamentali e delle tradizioni costituzionali comuni agli Stati membri*, in www.dirittounioneeuropea.eu, *Oss.* dicembre 2017; N. Lazzerini, *sub* art. 52, in R. Mastroianni - O. Pollicino - S. Allegrezza - F. Pappalardo - O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, 1073 ss., e i contributi di S. Cassese, M. Graziadei – R. De Caria, M.E. Comba e O. Porchia, che sono in *Rivista trimestrale di diritto pubblico*, 4, 2017.

[15] Sui problemi interpretativi che il disposto in parola solleva, v., tra gli altri, A. Von Bogdandy- S. Schill, *Overcoming Absolute Primacy: Respect for National Identity under the Lisbon Treaty*, in *Common market law review*, 48, 2011, 1417 ss.; G. Martinico, *Lo spirito polemico del diritto europeo. Studio sulle ambizioni costituzionali dell'Unione*, Roma, 2011, spec. 206 ss., del quale v., inoltre, *Il potenzionale sovversivo dell'identità nazionale alla luce dell'ordinanza 24/2017 della Corte costituzionale*, in Aa. Vv., *Il caso* Taricco *e il dialogo fra le Corti. L'ordinanza 24/2017 della Corte costituzionale*, cit., 241 ss.; in questo vol., praticamente in tutti gli scritti è fatto richiamo al principio di cui all'art. 4.2; S. Gambino, *Identità costituzionali nazionali e primauté eurounitaria*, in *Quaderni costituzionali,* 3, 2012, 533 ss.; M. Starita, *L'identità costituzionale nel diritto dell'Unione europea: un nuovo concetto giuridico?*, in F. Viola (a cura di), *Lo stato costituzionale di diritto e le insidie del pluralismo*, Bologna, 2012, 139 ss.; B. Guastaferro, *Beyond the exceptionalism of Constitutional Conflicts: The* Ordinary *Functions of the Identity Clause*, in *Yearbook of European Law*, 1, 2012, 263 ss., e, della stessa, *Legalità sovranazionale e legalità costituzionale. Tensioni costitutive e giunture ordinamental*, Torino, 2013, spec. 190 ss.; F. Vecchio, *Primazia del diritto europeo e salvaguardia delle identità costituzionali. Effetti asimmetrici dell'europeizzazione dei controlimiti*, Torino, 2012; A. Saiz Arnaiz - C. Alcoberro Llivinia (a cura di), *National Constitutional Identity and European Integration*, Antwerp 2013; M. Cartabia, *sub* art. 4, in A. Tizzano (a cura di), *Trattati dell'Unione europea*, Milano, 2014, 23 ss.; T. Cerruti, *Valori comuni e identità nazionali nell'Unione europea: continuità o rottura?*, in www.federalismi.it, 24, 2014, e, pure *ivi*, G. Caponi - V. Capuozzo - I. Del Vecchio - A. Simonetti, *Omogeneità costituzionale europea e identità nazionali: un processo di integrazione circolare tra valori costituzionali europei e teoria dei controlimiti*; E. Cloots, *National Identity in EU Law*, Oxford, 2015; M. Condinanzi, *I controlimiti come sintesi ideale tra primato da affermare e identità nazionale da rispettare*, in B. Nascimbene (a cura di), Costa/Enel*: Corte costituzionale e Corte di giustizia a confronto, cinquant'anni dopo*, Milano, 2015, 119 ss.; P. Cruz Villalón, *La identidad constitucional de los Estados miembros: dos relatos europeos*, in *Scritti in onore di A. D'Atena*, I, Milano, 2015, 729 ss.; E. Cloots, *National Identity in EU Law,* Oxford, 2015; G. Di Federico, *L'identità nazionale degli stati membri nel diritto dell'Unione europea. Natura e portata dell'art. 4, par. 2, TUE*, Napoli, 2017.

[16] Non è casuale la circostanza per cui tanto la Corte di giustizia nella sua pronunzia del dicembre 2017, in risposta alla domanda postale in via pregiudiziale dalla Consulta, quanto quest'ultima hanno fatto leva proprio sulle tradizioni comuni al fine di definire nel modo più adeguato il caso, riprendendo e portando a frutto un'indicazione venuta da una sensibile dottrina (M. Bassini - O. Pollicino, *The opinion of Advocate General Bot in Taricco II: Seven "Deadly" Sins and a Modest Proposal*, in www.verfassungsblog.de, 2 agosto 2017, nonché in www.penalecontemporaneo.it, 13 settembre 2017, e, degli stessi Autori, *Defusing the Taricco bomb through fostering constitutional tolerance: all roads lead to Rome*, in www.verfassungsblog.de, 5 dicembre 2017, e in www.penalecontemporaneo.it, 11 dicembre 2017). Ed è ancora alle tradizioni in parola che il nostro giudice delle leggi ha fatto appello nella discussa (e discutibile) sent. n. 269 del 2017, trattando del modo con cui vanno protette le norme della Carta dell'Unione sostanzialmente coincidenti con norme della Costituzione laddove risultino violate da discipline legislative.

di apprezzamento degli Stati[17], vale a dire, in buona sostanza, ai modi con cui prendono forma i diritti fondamentali nel tessuto sociale ed è ad essi data voce nelle più salde e diffuse esperienze giuridiche[18].

In seno ad uno stesso ordinamento, poi, il modo più adeguato per preservare l'equilibrio tra legislatore e giudici da un canto, giudice e giudice dall'altro[19], è proprio quello di sottoporre le singole decisioni – tanto quelle a finalità generale[20] quanto le altre valevoli per il singolo caso – al filtro delle consuetudini culturali in parola.

Il problema, nondimeno, ancora una volta, non può considerarsi del tutto risolto. Perché il punto non è solo stabilire se un bisogno può, o no, fregiarsi del titolo di "diritto fondamentale" ma anche, a seguire, quale trattamento debba essergli riservato, vale a dire quale tutela gli vada accordata.

3. La salvaguardia dei diritti attraverso la cooperazione di legislatori e giudici: agli uni spettando la posizione della disciplina iniziale, di principio, e agli altri la produzione delle regole idonee a svolgerli in relazione alle peculiari esigenze dei casi, tutti comunque dovendo fare i conti con lo sviluppo scientifico e tecnologico ed attingendo alle illuminanti indicazioni *offerte dall'etica*

Qui è il nodo di ordine istituzionale.

A mio modo di vedere, secondo modello costituzionale, la salvaguardia dei diritti fondamentali richiede il fattivo concorso di tutti gli operatori: immaginare che essa possa essere data a modo esclusivamente da alcuni o, peggio, solo da una ristretta cerchia e persino da un solo operatore (ad es., la Corte costituzionale) sarebbe un errore imperdonabile, foriero di gravissimi rischi per gli stessi diritti (e di coloro che ne sono

[17] In argomento, v., almeno, J. García Roca, *El margen de apreciación nacional en la interpretación del CEDH: integración y pluralism europeos*, in L. Mezzetti - A. Morrone (a cura di), *Lo strumento costituzionale dell'ordine pubblico europeo. Nei sessant'anni della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (1950-2010)*, Torino, 2011, 87 ss.; A. Legg, *The Margin of Appreciation in International Human Rights Law. Deference and Proportionality*, Oxford, 2012; D. Tega, *I diritti in crisi. Tra Corti nazionali e Corte europea di Strasburgo*, Milano, 2012, spec. 88 ss. e 110 ss.; i contributi che sono nella parte II.A di G. Repetto (a cura di), *The Constitutional Relevance of the ECHR in Domestic and European Law. An Italian Perspective*, Cambridge 2013; E. Cannizzaro - B.I. Bonafè, *Beyond the archetypes of modern legal thought. Appraising old and new forms of interaction between legal orders*, in Aa. Vv., *Transnational Law. Rethinking European Law and Legal Thinking*, a cura di M. Maduro - K. Tuori - S. Sankari, Cambridge, 2014, 84 ss.; C. Cinelli, *Corte europea dei diritti dell'uomo, Corte costituzionale italiana e margine di apprezzamento*, in *Rivista di diritto internazionale*, 3, 2014, 787 ss.

[18] Non è poi senza significato che proprio ad indirizzi interpretativi "consolidati" della Corte EDU (ed a pronunzie-pilota, che sono, in buona sostanza, ad essi equivalenti) abbia fatto riferimento la giurisprudenza costituzionale (spec. nella discussa sent. del 26 marzo 2015, n. 49), ad essi circoscrivendo il vincolo della interpretazione conforme delle leggi ad opera dei giudici nazionali (sui non pochi né lievi problemi che questa indicazione solleva, v., ora, A. Randazzo, *La tutela dei diritti fondamentali tra CEDU e Costituzione*, Milano, 2017, 159 ss.).

[19] … al piano sia delle relazioni inter-ordinamentali che di quelle intra-ordinamentali (e, dunque, tra Corti europee e Corti nazionali per un verso, giudici costituzionali e giudici comuni per un altro verso).

[20] … tra le quali vanno congiuntamente annoverate, pur non tacendosene i tratti peculiari di ciascuna di esse, leggi e sentenze delle Corti parimenti produttive di effetti *erga omnes*.

portatori) perché varrebbe come rimettere, a conti fatti, la ricognizione degli stessi all'insindacabile apprezzamento dei pochi o del solo decisore di turno.

Confesso di guardare con molta diffidenza e – a dirla tutta – con una certa stanchezza alla nota *querelle* tra i fautori di uno "Stato legislativo" e quelli di uno "Stato giurisdizionale". Si trascura infatti che nel DNA dello "Stato costituzionale" – il solo appellativo ad esso appropriato – è quel principio della separazione dei poteri, pur nelle forme varie e flessibili in cui si è storicamente e positivamente tradotto[21], che ad ogni buon conto richiede la proficua collaborazione, nella tipicità dei ruoli e delle responsabilità, di tutti gli operatori in vista del conseguimento dei fini-valori costituzionali.

Ora, proprio sullo specifico terreno della salvaguardia dei diritti fondamentali – il primo e più importante elemento costitutivo ed identificativo della Costituzione, secondo l'efficacissima formula di sintesi dell'art. 16 della Dichiarazione del 1789 – si apprezza (e deve apprezzarsi) la cooperazione in parola: al legislatore spettando il "riconoscimento" dei diritti, nella sua ristretta e propria accezione che evoca il portare alla luce ciò che si rinviene nel profondo del corpo sociale, nel mentre la "tutela" è specificamente rimessa ai giudici. La disciplina legislativa, poi, proprio nel presente contesto fortemente segnato dallo sviluppo scientifico e tecnologico, dovrebbe risultare connotata da agilità di disposti e duttilità di struttura, vale a dire da un pugno di indicazioni essenziali, *per principia*, rimettendosi quindi per i loro opportuni svolgimenti e gli adeguamenti al mutare delle circostanze ai giudici, destinatari di una sorta di "delega" loro conferita dal legislatore e bisognosa di essere portata a frutto nelle singole vicende processuali e secondo apprezzamenti – dove più e dove meno – largamente discrezionali[22]. Laddove, di contro, il legislatore dovesse spingersi in discipline troppo minute e dettagliate, tanto più se infarcite di divieti[23], solleciterebbe naturalmente i giudici costituzionali a caducarle per irragionevolezza e, sulla base delle indicazioni date da questi, i giudici comuni ad una non di rado complicata e sofferta opera di reperimento di nuove regole idonee a prendere il posto delle prime. Talvolta, poi, non potendosi far luogo a decisioni manipolative dei testi, a motivo dei limiti cui esse vanno per loro

[21] … in merito alle quali v. spec. la poderosa riflessione storico-teorica di G. Silvestri, *La separazione dei poteri*, I e II, Milano (risp., 1979 e 1984), sul cui pensiero v. G Grasso, *Crisi economico-finanziaria, globalizzazione, teoria dei cicli funzionali (in margine a "La separazione dei poteri" di Gaetano Silvestri)*, in www.rivistaaic.it, 2/2015.

[22] L'opzione per una disciplina legislativa "mite" o "leggera", con specifico riguardo alle esperienze d'inizio e fine-vita, è stata ripetutamente caldeggiata da numerosa dottrina [riferimenti in P. Veronesi, *La legge sulla procreazione assistita alla prova dei giudici e della Corte costituzionale*, in *Quaderni costituzionali*, 3, 2004, 524; S. Agosta, *Bioetica e Costituzione*, I, *Le scelte esistenziali di inizio-vita*, cit., spec. 38 ss., ma *passim*; A. Patroni Griffi, *Il bilanciamento nella fecondazione assistita tra decisioni politiche e controllo di ragionevolezza*, in www.rivistaaic.it, 3, 2015, spec. al § 5; C. Casonato, in molti scritti, tra i quali *La fecondazione eterologa e la ragionevolezza della Corte*, in www.confronticostituzionali.eu, 17 giugno 2014; R. Conti, *Diagnosi preimpianto, fine vita, sperimentazione su embrioni criocongelati. Prove di dialogo incrociato fra Corti*, in *Biolaw Journal* (www.biodiritto.org), 3, 2015, 168, e, se si vuole, anche il mio *Procreazione medicalmente assistita e Costituzione: lineamenti metodico-teorici di un modello ispirato ai valori di dignità e vita*, in Aa. Vv., *La procreazione medicalmente assistita*, cit., 257 ss., nonché in www.federalismi.it, 10, 2016, spec. al § 2.4].

[23] … quali quelli di cui era dotata la legge sulla procreazione medicalmente assistita, che hanno quindi obbligato il giudice costituzionale a far luogo al suo vero e proprio sostanziale rifacimento, convertendo alcune originarie e rigide chiusure in previsioni temperate e, perlomeno fino ad un certo punto, aperte. Efficacissimo il titolo dato da A. D'Aloia ad una sua succinta ma densa riflessione su questa vicenda: *L'(ex) 40*, in *Quaderni costituzionali*, 4, 2015, 997 ss.

natura incontro[24], si fa ricorso a manipolazioni occulte, ammantate delle candide vesti dell'interpretazione conforme, delle quali tanto i giudici costituzionali quanto i giudici comuni si rendono, pur nella diversità dei ruoli, artefici[25].

Il punto è che non si ha il necessario riscontro nell'esperienza del modello ora succintamente rappresentato, che demanda alla legge la produzione dei principi a corredo del riconoscimento dei diritti e alle sentenze dei giudici la loro specificazione-attuazione a mezzo delle regole di volta in volta congrue alle complessive esigenze dei casi[26]. Le note, diffuse e gravi, ancorché molte volte non sanzionate[27], responsabilità dovute alla latitanza del legislatore obbligano ad una innaturale torsione dei ruoli e, dunque, in buon sostanza, i giudici tutti (costituzionali e non) ad un'opera di "supplenza" – com'è usualmente e con una certa approssimazione chiamata – nei riguardi del legislatore stesso. Perché il vero è che il legislatore riluttante non può essere costretto ad un *facere*, il giudice invece deve pur sempre dare risposta alle domande che gli sono rivolte, altri-

[24] … e, segnatamente, del limite del rispetto della discrezionalità del legislatore, del quale tuttavia si sono fatti (e si fanno) usi fortemente oscillanti e – diciamo pure – creativi. Questa della discrezionalità è, infatti, una tecnica decisoria che, al pari peraltro di quella del "diritto vivente" posta in essere lungo il versante dei rapporti col giudiziario, si rivela molte volte *bonne à tout faire*, una sorta di *deus ex machina* che, come nelle antiche tragedie, consente di venire in soccorso degli uomini al fine di poter sciogliere le matasse più aggrovigliate.

[25] Alle formidabili risorse dell'interpretazione si è, poi, costretti a far ricorso laddove si punti al rifacimento del parametro, non essendo ovviamente immaginabile la caducazione dello stesso (specificamente laddove risulti dalla stessa Costituzione, mentre è possibile sanzionare norme di leggi costituzionali o di altre fonti anche di rango costituzionale e pur se avente origine esterna).

[26] Prendo qui nuovamente le distanze da una tesi largamente diffusa, della quale ancora di recente si è fatta interprete un'accreditata dottrina [M. Luciani, *Funzioni e responsabilità della giurisdizione. Una vicenda italiana (e non solo)*, in www.rivistaaic.it, 3, 2012, spec. al § 4, ma *passim* e, dello stesso, *Garanzie ed efficienza nella tutela giurisdizionale*, in www.rivistaaic.it, 4, 2014], secondo cui i giudici sarebbero sempre e solo chiamati a dare applicazione delle leggi. In realtà, v'è modo e modo di farlo, a seconda della struttura nomologica degli enunciati legislativi, composta da maglie ora più ed ora meno larghe, e prima ancora, naturalmente, a seconda che gli enunciati stessi si diano, non potendosi escludere in partenza i casi di loro mancanza, al ricorrere dei quali il giudice è costretto a fare utilizzo dei soli materiali normativi disponibili, alle volte costituiti unicamente dai principi della Carta costituzionale o di altre Carte. Ora, etichettare con un solo nome tutte queste esperienze a me parrebbe essere oggettivamente forzato. La stessa distinzione corrente tra principi e regole si pone quale una evidente semplificazione di un quadro internamente assai più articolato e composito, specie ove si consideri che sia le une che le altre norme esibiscono una diversa estensione di dettato (su ciò, di recente, O. Chessa, *I giudici del diritto. Problemi teorici della giustizia costituzionale*, Milano, 2014, spec. 297 ss.; C. Pinelli, *Principi, regole, istituti*, in *Diritto pubblico*, 1, 2015, 35 ss.; M.V. Ballestre - R. Guastini, *Dialogando su principi e regole*, in *Materiali per una storia della cultura giuridica*, 1, 2017, 127 ss.).

[27] … tanto al piano politico, a motivo delle note carenze in ordine alla funzionalità dei meccanismi di responsabilità sia istituzionale che diffusa, quanto a quello giuridico, non riuscendosi a trovare rimedio alle omissioni assolute del legislatore. Non è riuscita, infatti, ad oggi a farsi strada la coraggiosa proposta affacciata da R Conti, *Il rilievo della CEDU nel "diritto vivente": in particolare il segno lasciato dalla giurisprudenza "convenzionale" nella giurisprudenza dei giudici comuni*, in Aa. Vv., *Crisi dello stato nazionale, dialogo intergiurisprudenziale, tutela dei diritti fondamentali*, cit., 87 ss., volta a consentire un ristoro economico per quanti risultino danneggiati dall'inerzia del legislatore. A mia volta, già in altri luoghi [tra i quali, il mio *In tema di interpretazione e di interpreti nello Stato costituzionale (a proposito di un libro recente)*, in *"Itinerari" di una ricerca sul sistema delle fonti*, XIX, *Studi dell'anno 2015*, Torino, 2016, 530 s., e nt. 41] mi sono dichiarato favorevole a questa indicazione, a condizione che risulti provato che la lesione del diritto sia «conseguenza "diretta, immediata e necessaria" del vuoto legislativo». D'altro canto, alle stesse omissioni relative è possibile molte volte porre riparo solo in parte e a certe condizioni, obbligando le stesse il giudice delle leggi ad una laboriosa (e, alle volte, francamente ardita) ricucitura del tessuto legislativo lacerato, fatto oggetto – fin dove possibile – di copiose integrazioni e di manipolazioni in genere (sulle sentenze "normative" della Corte costituzionale, per tutti, v. G. Silvestri, *Le sentenze normative della Corte costituzionale*, in *Scritti su la giustizia costituzionale in onore di V. Crisafulli*, I, Padova, 1985, 755 ss. e C. Panzera, *Interpretare, manipolare, combinare. Una nuova prospettiva per lo studio delle decisioni della Corte costituzionale*, Napoli, 2013).

menti non renderebbe giustizia.
La "supplenza" è una metafora che, nei fatti, può significare (ed effettivamente significa) molte cose[28]. Sta di fatto che non poche volte i giudici costituzionali si trovano investiti del compito di dover disegnare la cornice del quadro al posto del legislatore, somministrando quindi ai giudici comuni i principi dai quali possono estrarsi le regole richieste dai casi; e ciò possono fare a modo ispirandosi all'etica, specie nelle sue più elevate espressioni positive, quali risultano dalla Carta costituzionale e dalle altre Carte.

4. La "federalizzazione" dei diritti, testimoniata dalle "catene" di atti giurisdizionali che vengono a formazione a più livelli ordinamentali e istituzionali, all'insegna del principio della massimizzazione della tutela, quale si mette a fuoco e realizza nelle singole esperienze processuali, ricevendo luce ed orientamento sia dalla scienza che dall'etica

Come si è tentato di mostrare in altri luoghi[29], vengono pertanto non di rado a formarsi "catene" di atti che alle volte si avviano fuori delle mura domestiche, per mano di questa o quella Corte europea, e quindi si immettono in ambito interno, laddove ricevono un primo loro prolungamento ad opera di una pronunzia del giudice costituzionale e, a seguire, da pronunzie dei giudici comuni, grazie alle quali pervengono infine alla loro maturazione e chiusura.
In circostanze siffatte si assiste, a mio modo di vedere, alla produzione di un effetto unitario, proprio della "catena", che sovrasta e comprende quelli dei singoli "anelli" che la compongono, i quali nondimeno non perdono la loro peculiare e singolare connotazione. Senza però lo sforzo congiunto da tutti prodotto e convergente verso la meta comune, la trasformazione della realtà (l'effetto giuridico, appunto[30]), all'insegna dei valori costituzionalmente protetti, non avrebbe modo di farsi apprezzare.
È proprio così che, a mia opinione, viene a prendere forma un modello di "federalizzazione" dei diritti, nel quale da tempo mi riconosco[31] e che – come si tenta qui di mostrare – proprio al crocevia di etica, scienza e diritto riceve la sua più nitida rappresentazione e giustificazione.
Che la legge debba andare incontro al limite sopra indicato, dotandosi di un corpo di norme essenziali ed elastiche, è avvalorato proprio dal modo con cui il diritto viene

[28] Sulle complessive, rilevanti valenze delle metafore nell'esperienza giuridica, acute notazioni sono nel contributo alle nostre Giornate di O. Pollicino, *Metafore, Judicial framing e tutela dei diritti fondamentali nell'era digitale*, in *paper*, e, ora, in A. Morelli - O. Pollicino, *Le metafore della rete. Linguaggio figurato, judicial frame e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto*, in corso di stampa in www.rivistaaic.it.

[29] … tra i quali, il mio *Costituzione, sovranità, diritti fondamentali, in cammino dallo Stato all'Unione europea e ritorno, ovverosia circolazione dei modelli costituzionali e adattamento dei relativi schemi teorici*, in www.federalismi.it, 11, 2016, spec. al § 6.

[30] Su ciò la magistrale e ad oggi insuperata lezione teorica di A. Falzea, *Efficacia giuridica*, in *Enciclopedia del diritto*, XIV, 1965, 432 ss.

[31] Tra gli altri miei scritti, può, volendo, vedersi il mio *Come costruire e preservare le tradizioni dei diritti in Europa?*, in *Consulta OnLine*, III, 17 dicembre 2015, 835 ss., spec. 845 ss.

a contatto con l'etica da un lato, la scienza e la tecnologia dall'altro. Queste ultime, in ispecie, col loro modo frenetico ed incalzante di rinnovarsi sollecitano vigorosamente il legislatore a tenersi alla larga dal far luogo a discipline rigide e statiche, incapaci di adeguarsi a situazioni continuamente cangianti ed estremamente varie. Chi, invece, è in grado di tenere il passo degli avanzamenti scientifici e tecnologici è proprio il giudice, al di là del livello ordinamentale al quale opera e della natura dell'attività svolta. D'altronde, solo il giudice è in grado di utilizzare al meglio, per le peculiari esigenze del caso, i materiali normativi disponibili, confrontandoli e – fin dove possibile – integrandoli nell'interpretazione e stabilendo dove si situa l'ottimale salvaguardia delle esigenze stesse, con specifico riguardo ai diritti fondamentali visti nel loro fare sistema tanto *inter se* quanto con altri interessi, individuali e collettivi, meritevoli di protezione[32].
Nel principio della massimizzazione della tutela[33] tutte le Carte si riconoscono: espressamente, la CEDU e la Carta dell'Unione (entrambe all'art. 53), che ritagliano per sé un ruolo sussidiario rispetto alla salvaguardia dei diritti assicurata in ambito interno, ed implicitamente – a mio modo di vedere – la stessa Costituzione (segnatamente agli artt. 2 e 3, nel loro porsi in rapporto coi principi fondamentali restanti). Come si è tentato di mostrare in altri luoghi, ad esso è anzi da assegnare generale valenza, giocando non soltanto quale criterio di selezione della norma o del sistema di norme idoneo a portare ancora più in alto il livello di tutela rispetto ad altra norma o sistema normativo, ma anche (e soprattutto) quale criterio di orientamento (anzi, di pre-orientamento) dei processi interpretativi.
Se il criterio non si discute, il problema resta però aperto e si ripropone ogni volta, dovendosi stabilire come far luogo senza soverchie incertezze ai riscontri richiesti dal

[32] All'idea di sistema la giurisprudenza costituzionale ha fatto (e fa) insistito richiamo: v., *ex plurimis*, decc. 22 luglio 2011, n. 236; 28 novembre 2012, n. 264; 15 gennaio 2013, n. 1; 9 maggio 2013, n. 85; 4 luglio 2013, n. 170 e 18 luglio 2013, n. 202; 11 febbraio 2015, n. 10 e 26 marzo 2015, n. 49; 24 marzo 2016, n. 63; 26 maggio 2017, n. 124 e 14 dicembre 2017, n. 269.

[33] … a riguardo del quale, nella ormai copiosa lett., R. Conti, *sub* art. 53, in G. Bisogni - G. Bronzini - V. Piccone (a cura di), *La Carta dei diritti dell'Unione europea. Casi e materiali*, Taranto 2009, 639 ss.; L. Trucco, *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione europea*, cit., 159 ss.; A. D'ALoia, *Europa e diritti: luci e ombre dello schema di protezione multilevel*, in *Il Diritto dell'Unione europea*, 1, 2014, 1 ss., spec. 32 ss.; G. D'Amico, *La massima espansione delle libertà e l'effettività della tutela dei diritti*, in A. Pin (a cura di), *Il diritto e il dovere dell'uguaglianza. Problematiche attuali di un principio risalente*, Napoli, 2015, 17 ss.; C. Amalfitano - M. Condinanzi, *Unione europea: fonti, adattamento e rapporti tra ordinamenti*, Torino, 2015, 126 ss. e 168 ss.; G.M. Salerno, *I diritti fondamentali tra le tradizioni costituzionali comuni e i controlimiti a tutela dell'identità costituzionale*, in *Il Filangieri*, *Quaderno 2014* su *Unione europea e principi democratici*, Napoli, 2015, 103 ss.; C. Panzera, *Rispetto degli obblighi internazionali e tutela integrata dei diritti sociali*, in Consulta OnLine, 2, 2015, spec. 492 ss.; nella stessa *Rivista*, A. Spadaro, *Sull'aporia logica di diritti riconosciuti sul piano* internazionale*, ma negati sul piano* costituzionale. *Nota sulla discutibile "freddezza" della Corte costituzionale verso due Carte internazionali: la CSE e la CEAL*, 504 ss. e, dello stesso, ora, *La "cultura costituzionale" sottesa alla Carta dei diritti fondamentali dell'Unione europea, fra modelli di riferimento e innovazioni giuridiche*, in Aa. Vv., *La Carta dei diritti dell'Unione Europea e le altre Carte (ascendenze culturali e mutue implicazioni)*, cit., spec. 55 ss.; *ivi* pure C. Salazar, *I diritti sociali nel "gioco delle tre Carte": qualche riflessione*, 217 ss., e L. D'Andrea, *A mo' di sintesi: ordinamento europeo e costituzionalismo contemporaneo*, spec. 314 ss.; L. Cappuccio, *La massima espansione delle garanzie tra Costituzione nazionale e Carte dei diritti*, in *Scritti in onore di G. Silvestri*, I, Torino, 2016, 412 ss.; A.O. Cozzi, *Diritti e principi sociali nella Carta dei diritti fondamentali dell'Unione europea. Profili costituzionali*, Napoli, 2017, 92 ss., spec. 111 ss.; M. Cartabia, *Convergenze e divergenze nell'interpretazione delle clausole finali della Carta dei diritti fondamentali dell'Unione europea*, cit., spec. 12 ss.; M. Condinanzi – P. Iannuccelli, *sub* art. 53, in Aa. Vv., *Carta dei diritti fondamentali dell'Unione europea*, cit., 1085 ss. Infine, A. Randazzo, *La tutela dei diritti fondamentali tra CEDU e Costituzione*, cit., spec. 222 ss., ma *passim*; N. Colacino, *Obblighi internazionali e ordinamento costituzionale a dieci anni dalle sentenze gemelle: breve cronaca di un lungo assedio*, in www.dirittocomparati.it, 3, 2017, § 3, e F. De Vanna, *I 'controlimiti' tra disordine delle fonti ed equilibrio del diritto*, in www.federalismi.it, 23, 2017, spec. al § 3.

criterio stesso. È poi fuor di dubbio che i punti di vista delle Corti possono reciprocamente, legittimamente divergere; ed è chiaro che le tensioni finiscono poi con lo scaricarsi sui terminali delle operazioni di giustizia, i giudici comuni, i quali possono trovarsi messi in croce ogni qual volta siano chiamati a dar seguito a pronunzie delle Corti europee e della Corte costituzionale reciprocamente incompatibili.
Non posso riprendere qui la vessata questione dei conflitti tra giudicati, che richiederebbe approfondimenti per i quali questa sede risulta evidentemente inadeguata[34].
Su un punto però occorre, prima di chiudere, fermare l'attenzione; ed è che in occasione dell'applicazione del principio della miglior tutela e delle sue opportune verifiche occorre pur sempre orientare l'analisi verso le risultanze della scienza e le indicazioni offerte dall'etica: è proprio dal punto di vista di quest'ultima, anzi, che gli stessi esiti della scienza vanno vagliati ed apprezzati, portandoli quindi ad effetto per le esigenze della pratica giuridica.

5. La lezione che viene da Corte cost. n. 84 del 2016 e i tre insegnamenti che la stessa ci somministra

Scienza ed etica entrano prepotentemente sulla scena già al momento in cui si tratta di dare senso ad enunciati riguardanti i diritti (specie ad alcuni di essi che ne sono maggiormente impressionati), al fine di stabilire se e quale uso possa farsene nella pratica giuridica. Se ne hanno molte e convergenti testimonianze in giurisprudenza: ne riporto qui solo una, particolarmente attendibile, al di là poi del fatto che si condivida il risultato processuale raggiunto.
Ci dice, infatti, Corte cost. 13 aprile 2016, n. 84 in tema di divieto di utilizzo di embrioni crioconservati a finalità di ricerca, che, laddove la scienza è divisa, la Costituzione rimane muta[35]: l'indecidibilità del caso nel merito, allora, naturalmente si converte nella inammissibilità della questione. Allo stesso tempo in cui il giudice delle leggi arretra e si

[34] Riferimenti, di recente, in A. Randazzo, *La tutela dei diritti fondamentali tra CEDU e Costituzione*, cit., 249 ss. In giurisprudenza, dopo la nota e discussa pronunzia della Consulta del 7 aprile 2011, n. 113 (per la materia penale), v., più di recente e con riguardo al giudicato civile e amministrativo, Corte cost. 26 maggio 2017, n. 123 [sulla quale le note di A. Randazzo, *A proposito della sorte del giudicato amministrativo contrario a pronunzie della Corte di Strasburgo (note minime alla sent. n. 123 del 2017 della Corte costituzionale)*, in Consulta OnLine, 3, 2017, 460 ss. e, nella stessa *Rivista*, R. G. Conti, *L'esecuzione delle sentenze della Corte edu nei processi non penali dopo Corte cost. n. 123 del 2017*, 2, 2017, 333 ss.; inoltre, E. Bindi – A. Pisaneschi, *La Corte costituzionale non consente la revocazione delle sentenze amministrative passate in giudicato per contrasto con la sentenza della Corte EDU*, www.giustamm.it e G.V.A. Petralia, *Conflitto tra giudicato nazionale e sentenze delle Corti europee: nota a margine di Corte costituzionale n. 123/2017*, in www.rivistaaic.it, 4, 2017] e 18 gennaio 2018, n. 6 [col commento di P. Tomaiuoli, *L'"altolà" della Corte costituzionale alla giurisdizione dinamica (a margine della sentenza n. 6 del 2018)*, in Consulta OnLine, 1, 2018, 1 ss.].

[35] Si faccia caso alla differenza che si ha tra le lacune costituzionali (nella loro propria e ristretta accezione), che un'accreditata dottrina qualifica come "lacune di costruzione", dipendenti da indebite carenze dell'impianto costituzionale, e ciò che invece si ha laddove gli enunciati non manchino e però risulti impossibile assegnare loro significato non venendo allo scopo in soccorso esperti e scienziati (sulle lacune costituzionali, tema *ab antiquo* vessato, di recente, v. Q. Camerlengo, *Nel silenzio della Costituzione*, in *Diritto e società.*, 2, 2014, 267 ss., e, se si vuole, il mio *Lacune costituzionali*, in www.rivistaaic.it, 2, 2016,).

lava pilatescamente le mani[36], viene sollecitato ad attivarsi il legislatore. La Costituzione resta, dunque, silente ma la legge comune può (e deve) parlare[37]. Nel frattempo, però, il giudice cosa può ovvero deve fare?

Qui è, infatti, il punto. Come si fa a stabilire dove si situa la miglior tutela di tutti i beni della vita in campo se la Costituzione è muta?

Ebbene, la vicenda è assai istruttiva per plurime ragioni; per ciò che qui maggiormente importa, per tre di esse.

La prima è la conferma che l'interpretazione costituzionale, in relazione ad alcuni enunciati, non può portarsi avanti e pervenire alla meta senza il soccorso della scienza, della quale dunque – piaccia o no – non può farsi comunque a meno.

La seconda è che i diritti possono essere messi a fuoco e intesi nella loro stessa struttura costitutiva, come pure reciprocamente combinati (e soppesati), unicamente attingendo a quelle "consuetudini culturali di riconoscimento", di cui poc'anzi si diceva, risultanti perciò anche (e talora soprattutto) da indicazioni convergenti degli scienziati, dall'essersi cioè formato un autentico "diritto vivente scientifico" idoneo quindi a convertirsi e risolversi in "diritto vivente" *tout court*, tanto più rilevante laddove, come nella vicenda appena richiamata, riferito ad enunciati costituzionali.

La terza è che nessun bilanciamento può in ogni caso farsi da una prospettiva eticamente neutra o inespressiva. La Corte apparentemente non si pronunzia, o meglio dichiara di non potersi pronunziare; in realtà, così facendo, sa benissimo di avallare, a conti fatti, lo *status quo*, confermando "per l'intanto" il divieto di destinazione degli embrioni alla ricerca, un divieto nondimeno non discendente – potrebbe crisafullianamente dirsi: "a rime obbligate" – dalla Costituzione ma, all'inverso, disponibile (solo, però, per il legislatore). Rimane, comunque, oscuro come possa il legislatore stesso determinarsi e far luogo alla scelta migliore perdurando le divisioni tra gli scienziati e, di conseguenza, restando muta la Costituzione, quasi che sia indifferente che si opti per l'una ovvero l'altra soluzione. *In nuce*, si tratta di vedere se il principio di precauzione si volga a copertura della integrità dell'embrione, che pur tuttavia dopo un certo tempo (la cui durata è, nondimeno, controversa) si rende inutilizzabile a finalità riproduttiva, ovvero – come a me sembra – a copertura della ricerca, i cui benefici non richiedono ovviamente di essere qui messi ulteriormente in chiaro.

---

[36] In questo senso se ne discorre nel mio *Questioni di costituzionalità inammissibili per mancanza di consenso tra gli scienziati (a margine di Corte cost. n. 84 del 2016, in tema di divieto di utilizzo di embrioni crioconservati a finalità di ricerca)*, in www.biodiritto.org (*Biolaw Journal*), 2, 2016, 245 ss.; nella stessa *Rivista*, altri commenti di vario segno; v., poi, tra i molti altri, E. Chieregato, *La resistenza del divieto di donazione di embrioni alla ricerca scientifica tra margine di apprezzamento europeo e deferenza al legislatore*, in www.forumcostituzionale.it, 4 giugno 2016; V. Tigano, *De dignitate non disputandum* est*? La decisione della Consulta sui divieti di sperimentazione sugli embrioni e di revoca del consenso alla PMA*, in www.penalecontemporaneo.it; G. Sorrenti, *Note minime sul rapporto tra ius, ethos e scientia*, cit.

[37] … restando, ovviamente, le scelte al riguardo fatte insindacabili alla luce di un parametro costituzionale, in tesi insussistente o… "muto", salvo ad ogni buon conto il sindacato secondo ragionevolezza: una ragionevolezza – possiamo ormai dire – "eticamente" ispirata.

6. Riassumendo e concludendo: le conferme che vengono al modello "federale" di salvaguardia dei diritti dal presente contesto segnato da una integrazione sovranazionale avanzata e dallo sviluppo impetuoso della scienza e della tecnica, pur sempre bisognoso tuttavia di alimentarsi e rigenerarsi costantemente dall'etica

Riassumendo e concludendo.

Gli equilibri, fluidi e precari, tra i protagonisti della vita istituzionale (e, segnatamente, legislatori e giudici) non restano affidati in ordine alla loro messa a punto e definizione esclusivamente a ragioni di contesto politico, economico, sociale in genere; sono altresì da mettere in conto l'incidenza crescente esercitata dallo sviluppo scientifico-tecnologico, per un verso, e, per un altro verso, l'orientamento che viene dall'etica.

In questo quadro internamente articolato, attraversato da non poche tensioni e connotato da perduranti carenze e contraddizioni, vengono meno risalenti e consolidate credenze nel mentre si fanno strada a forza istanze e bisogni un tempo sconosciuti e che premono per il loro appagamento, il massimo possibile alle difficili e, per certi, versi proibitive condizioni del tempo presente. Gli ordinamenti sono sollecitati a prestazioni di mutua solidarietà, tanto più avvertita quanto più avanza la loro integrazione[38].

Allo stesso tempo, in seno a ciascuno di essi cadono antiche barriere e vere e proprie contrapposizioni, quale quella che voleva nettamente distinto il ruolo dei decisori politici da quello dei garanti. Specie (ma non solo) laddove si tratti di dare tutela ai diritti fondamentali (e, particolarmente, a quelli nuovi o nuovissimi), tutti gli attori istituzionali sono chiamati a prestazioni che si dispongono in modo seriale componendo ed alimentando processi complessi, in seno ai quali prendono forma "catene" di atti tutti – quale più quale meno – espressivi di una intrinseca, ineliminabile *vis* innovativa. "Normative" sono infatti, per loro congenita natura e vocazione, le leggi che danno il primo e – secondo modello – necessario "riconoscimento" dei diritti, specie a mezzo di disposizioni di principio, e "normative" sono altresì le pronunzie dei giudici costituzionali che vi danno il primo, diretto e immediato svolgimento (talvolta esse pure a mezzo di ulteriori formule di principio) come pure, a seguire, le pronunzie degli stessi giudici comuni, chiamati non di rado a far luogo a regole "attuative" (e non meramente "applicative") dei principi stessi[39].

Il modello vincente – come si è tentato di mostrare – è quello di una "federalizzazione" dei diritti fondamentali, specie appunto di quelli scientificamente sensibili. Lo richiede un contesto segnato da una integrazione sovranazionale avanzata e dall'infittirsi

[38] Perdurano, tuttavia, ostacoli alle volte insormontabili che ne rendono assai complicata e sofferta la realizzazione: basti solo pensare al modo con cui è stata (ed è) gestito dall'Unione e dagli Stati il fenomeno delle migrazioni di massa.

[39] Come si è tentato in altri luoghi di mettere in chiaro, la normatività infatti non discende esclusivamente dall'attitudine degli atti che ne sono provvisti a produrre effetti generali (ciò che, peraltro, è proprio non soltanto delle leggi ma anche delle sentenze di alcuni giudici, e segnatamente di quelli costituzionali) ma anche da connotati strutturali degli atti stessi e, di riflesso, dalla *vis* innovativa dagli stessi espressa nei singoli casi, pur laddove – come per le decisioni dei giudici comuni – la loro efficacia resti poi circoscritta alle singole esperienze processuali alle quali si applicano.

dei vincoli discendenti dalla Comunità internazionale, un contesto in seno al quale lo stesso Stato costituzionale è profondamente cambiato e proiettato verso ulteriori cambiamenti dei quali ancora ci sfugge il complessivo modo di essere[40]. Basti solo pensare alla circostanza per cui, a fronte del vecchio modello di ordinamento al cui vertice si disponeva in sovrana solitudine una sola Costituzione, quale fondamento, fine e confine assiologico-normativo dello stesso, oggi si ha una costellazione di Carte che si affiancano e integrano la Costituzione: tutte chiamate a darsi mutuo sostegno ed a concorrere ciascuna alla incessante alimentazione e rigenerazione delle altre.

È ovvio che, in un contesto siffatto, la pluralità delle Carte (e delle Corti che ne sono istituzionalmente garanti) fa crescere le opportunità di tutela dei diritti ma rende viepiù complicato e impegnativo il compito di chi è deputato a darla, dilatandone i margini di apprezzamento discrezionale. Si tratta quindi di vedere in che modo e fin dove l'operato degli attori istituzionali possa essere tenuto sotto controllo, orientato, sorretto.

Soccorrono allo scopo – come si è veduto – un criterio, espressivo di un'autentica direttiva metodica d'azione, e uno strumento: l'uno è dato dalla ricerca della massimizzazione della tutela, già in sede d'interpretazione degli enunciati, più e prima ancora che della loro applicazione ai casi; l'altro dal riferimento a consuetudini culturali di riconoscimento dei diritti diffuse e radicate nel corpo sociale, tanto più laddove si dispongano e svolgano a plurimi livelli ordinamentali, facendosene quindi interpreti e garanti tanto le Corti europee quanto quelle nazionali[41]. Come si è tentato di mostrare, è questa, a conti fatti, la migliore risorsa di cui disponiamo al fine di dare risposta a domande di giustizia alle volte pressanti, comunque esigenti, che rimandano a bisogni elementari dell'uomo ai quali si fatica a venire incontro in modi complessivamente appaganti.

Scienza e tecnologia possono fare molto a tal fine ma rimangono cieche se non sono sorrette, illuminate, rigenerate dall'etica, così come hanno da esserlo gli operatori del diritto.

La centralità della persona umana, kantianamente intesa sempre e solo come fine e mai come mezzo, è il solo punto fermo dal quale tutti – studiosi ed operatori – possono stabilmente tenersi nel loro quotidiano, impegnativo e non di rado sofferto lavoro.

[40] Un'attenta riflessione di sintesi sul modo di essere e di divenire dello Stato costituzionale è in A. Spadaro, *Le evoluzioni contemporanee dello Stato di diritto*, in *Lo Stato*, 8, 2017, 139 ss.; volendo, si può poi vedere anche il mio *Lo Stato costituzionale e le sue "mutazioni genetiche"*, in *Quaderni costituzionali*, 4, 2014, 837 ss.

[41] È poi appena il caso qui di rilevare di sfuggita che gli operatori non si limitano a recepire meccanicamente e passivamente le tradizioni costituzionali profondamente radicate nel tessuto sociale ma coi loro atti concorrono al loro incessante rinnovo, assicurandone in tal modo la trasmissione alle generazioni che verranno. La qual cosa si rende particolarmente visibile nei casi in cui decisioni coraggiose dei giudici danno voce a diritti incipienti o ancora in formazione, imprimendo una spinta vigorosa alla loro affermazione in strati sempre più larghi del corpo sociale.

Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*

Vincenzo Zeno-Zencovich

Abstract

Il contributo analizza alcune delle questioni centrali nella discussione sui "big data" e cioè la titolarità di tali dati, la interesezione con la disciplina dei dati personali, le responsabilità connesse all'uso dei dati, le decisioni pubbliche che su di esse si fondano, e gli effetti che questo nuovo contesto ha sul modo con cui il giurista conosce ed organizza il diritto.

The article analyses some of the most important issues surrounding the big data revolution: entitlement of data; the overlappings with data protection legislation; liability for damages arising from the use of data; public decision-making processes on the basis of data analytics; and the effects that this new scenario has on the ways through which jurists understand and organize the law.

Sommario

1. Premessa. – 2. La "proprietà" dei dati. – 3. I dati personali. – 4. La responsabilità connessa all'uso dei dati. – 5. Decisioni pubbliche basate sui dati. – 6. La mutante epistemologia del giurista.

Keywords: Big data, Titolarità dei dati, Dati personali, Responsabilità per dati, Amministrazione digitale

1. Premessa

Esiste un mondo reale, fatto da questo pianeta; dagli spazi, infiniti, extraterrestri; da tutto ciò che la Terra contiene di minerale, vegetale, animale, e dai suoi sette miliardi di abitanti. Ogni momento questo mondo reale cambia, da una foglia che cade ad un essere umano che muore o che nasce.

Ed esiste un mondo digitale in cui praticamente tutto il mondo reale è riprodotto attraverso strumenti che raccolgono, conservano, elaborano dati. La differenza è che questo mondo digitale è caratterizzato dal fattore "T". Mentre nel mondo reale esiste il passato, nel mondo digitale ogni elemento è sempre presente perché ne conserviamo una traccia, dalla pioggia che è caduta un giorno alla telefonata che una persona abbia fatto ad un'altra. Questo mondo – che possiamo chiamare "datasfera" – è al tempo stesso dinamico e immanente, nel senso che ne registriamo e conserviamo ogni mutamento (o non mutamento) nel tempo, che può essere sempre richiamato. Nel mondo reale ciò che non è presente lo possiamo ricreare attraverso il ricordo, il racconto, le statistiche. Nel mondo digitale possiamo in ogni momento ricostruire, anche visiva-

* L'articolo è stato inviato su richiesta della direzione e pertanto non è stato sottoposto a referaggio.

mente, quanto era e accadeva un'ora, un giorno, un anno fa.
Lungi dall'essere fantascientifica questa rappresentazione ha una concretezza fatta di miliardi di miliardi (attualmente l'unità di misura è lo zettabyte ovvero 10^7) di dati, ma soprattutto ha una sua interazione sociale: noi siamo, oltre ad esseri in carne ed ossa, milioni di dati; noi compiamo scelte sulla base di dati (banalmente la scelta di un percorso stradale o di un locale pubblico); le imprese e le istituzioni pubbliche prendono decisioni (anche immediate e contestuali) sulla base di dati.
Si tratta di un fenomeno in costante ed esponenziale crescita: secondo per secondo dati si accumulano ad altri dati; unendosi a quelli precedenti generano ulteriori dati. Esso è destinato ad aumentare in modo ancor più vertiginoso con la diffusione di quel che viene gergalmente chiamato "*Internet of the things*" (IOT) ovvero "Internet delle cose" in cui saranno gli oggetti – anche più minuti – a registrare il proprio utilizzo e l'ambiente circostante (già lo fanno gli autoveicoli) trasmettendo altri miliardi di dati ogni istante.
Il giurista, che osserva la società e studia le regole che la governano, non può restare indifferente a tale evoluzione, come non poteva restarlo quando si scoprivano nuovi mondi.
Quali sono i profili che maggiormente lo interessano, sia per la loro rilevanza pratica che per quella teorica? Qui di seguito cerco di fornire un elenco, nella consapevolezza che è solo parziale e provvisorio, anche perché il giurista ha una passione nel creare questioni da discutere e approfondire, talvolta puramente ipotetiche, talaltra estremamente concrete.

2. La "proprietà" dei dati

Miliardi di dati; ma "appartengono" a qualcuno? Il giurista formatosi nella tradizione romanistica è portato spontaneamente a farsi questa domanda perché dalla qualificazione della forma di appartenenza di un bene dipende la utilità – giuridicamente tutelata – che se ne può trarre.
Questi dati, dunque, "appartengono" a chi li genera? (*e.g.* il conducente del veicolo?) Al proprietario dell'oggetto che li genera (*e.g.* il proprietario del veicolo)? Al titolare della apparecchiatura che li registra (*e.g.* il produttore della "scatola nera" sul veicolo)?Oppure a chi li raccoglie e li elabora (*e.g.* la casa automobilistica verso la quale confluiscono i dati di tutti i veicoli da essa costruiti)? Gli esempi – tratti da una accesa contesa già in atto – evidenzia la molteplicità di possibili soluzioni. Ma, poi, come possiamo qualificare la forma di appartenenza? "Proprietà", nel senso romanistico del termine, appare difficile per ragioni concettuali e comparatistiche. Da un lato sono ben note le impervietà teoriche quando si cerchi di applicare la disciplina della proprietà ed entità non materiali (*ex multis*, la "proprietà del credito") con tutte le aporie riguardanti il modo di acquisto, di godimento, di trasmissione ed i relativi rimedi. Nel contempo, considerato che i "dati", per la loro immaterialità e il loro intrinseco legame con le reti di telecomunicazione, non possono essere radicati nel territorio (e dunque nel diritto) di un solo Stato, va tenuto presente che in taluni ordinamenti (primo fra tutti quello tedesco) il

concetto di bene è normativamente legato alla corporeità dell'oggetto.
Più plausibile la prospettazione di una generica "titolarità" la quale attribuisce al soggetto – sulla scia della consolidata tradizione dei beni immateriali – una serie di diritti, facoltà e correlativi limiti e rimedi. Ma proprio l'esperienza dei beni immateriali ci ammonisce quanto l'affermazione di pretese giuridiche su di essi dipende da espressi riconoscimenti normativi, che nel caso dei dati (e con la esclusione di quelli "personali" e delle basi di dati di cui alla Direttiva 9/1996) ancora difetta. I dati godono di una qualche tutela ma indirettamente attraverso la disciplina della concorrenza sleale, dei segreti d'impresa, della responsabilità civile, del patrimonio dell'azienda.
Peraltro anche la prospettiva della "titolarità sui dati" presente una serie di problematicità.
In primo luogo va ricordato che i dati presentano le caratteristiche che gli economisti definiscono come "beni pubblici" ovverosia la loro non consumabilità (il loro valore in generale è indipendente dall'uso che se ne fa: la data della scoperta dell'America può essere fruita da uno o da tutti, ma ciò non ne diminuisce il valore); la non-rivalità (la circostanza che uno sia "titolare" di un dato non impedisce – come invece per i beni corporali – che qualcun altro allo stesso tempo lo sia. Tali elementi ovviamente incidono sulla conformazione dei diritti che si vogliono affermare sul bene in funzione alle utilità che se ne intendono trarre. La esclusività, dunque, presenta profili peculiari.
In secondo luogo di fronte ai miliardi e miliardi di dati, i quali rappresentano l'intero mondo, e lo duplicano digitalmente, la pretesa appropriativa rischia di apparire presuntuosa e utopistica, come quella di chi volesse appropriarsi delle gocce che compongono il mare o delle particelle che compongono l'aria. In altri termini, di fronte a grandezze di difficile commensurabilità e ad entità la cui circolazione e duplicazione è naturale e praticamente senza costo schemi generali di titolarità risultano di scarsa utilità ai fini pratici, ovverosia quello di assicurare ad un soggetto – e solo a quel soggetto – il diritto di trarre un vantaggio economico dalla sua posizione.
Infine, e a tale ultimo riguardo, ci si può porre la domanda – ricorrente nel settore – se il valore non sia nei dati in sé, bensì sugli strumenti informatici (i c.d. *data analytics*) utilizzati per analizzare tali moli così grandi e variegate. In teoria tutti potrebbero avere accesso a tali dati, ma solo chi dispone degli algoritmi e dei programmi idonei. E' su questi ultimi che si afferma la privativa industriale.

3. I dati personali

Un indice del regime giuridico dei dati può essere dato dalla elefantiaca normativa europea, il Regolamento generale sulla protezione dei dati personali (679/16) composto di appena un paio di centinaia di "considerando" e di un centinaio di articoli, cui si aggiungono una corona di direttive (680/16 e 681/16), per altre centinaia di articoli, sul trattamento dei dati nelle indagini penali, dei dati nelle prenotazioni aeree e (in preparazione) sulle reti di telecomunicazioni. Da questo complesso è comunque chiaro che sui dati non si vanta un diritto dominicale. Senza scomodare Ulpiano *(dominus nemo membrorum suorum videtur)* il rapporto giuridico che si instaura è piuttosto di controllo

sull'uso che terzi possono fare di tali dati, assistito da uno *ius arcendi* che si concretizza nell'ordine di cancellazione dei dati illegittimamente trattati.
Peraltro proprio l'analisi della normativa e della prassi in materia di dati personali fa comprendere quanto la pretesa da parte del titolare di esercitare i diritti attribuitigli è veramente illusorio, giacché quei dati, una volta acquisiti sono utilizzati, trasferiti, elaborati, ceduti, duplicati infinite volte a sua insaputa, spesso in un'altra parte del globo, grazie alle ubique tecnologie c.d. *cloud*.
Un simulacro di titolarità, dunque, che è ancor più evidente con riferimento a dati non qualificabili soggettivamente o oggettivamente come "personali" per via o dell'ente cui si riferiscono ovvero di quanto in essi rappresentato.
Il rispetto, dunque, dei diritti individuali è rimesso non a istituti privatistici bensì a ben più penetrati controlli pubblicistici effettuati dai "Garanti per la protezione dei dati personali" i quali dispongono altresì delle armi della sanzione penale. Quello dei dati diventa uno, fra i tanti, "mercati regolamentati" cui è preposta una autorità e che opera secondo logiche di sistema. D'altronde, considerata la dimensione della "datasfera", è difficile immaginare che possa avvenire diversamente: la similitudine va al rapporto fra tutela privatistica della proprietà delle immissioni e disciplina pubblicistica dell'ambiente e di contrasto all'inquinamento.

4. La responsabilità connessa all'uso dei dati

Da quasi 40 anni ci si interroga sui profili di responsabilità civile connessi all'uso di dati: l'esempio archetipale era quello di un "sistema esperto" (si chiamavano così all'epoca) di assistenza al traffico aereo che, a causa di un errore di elaborazione, provocava un incidente. L'esperienza di questi decenni non fornisce elementi che ci consentano di affermare che tali sistemi (a partire dal più banale programma informatico, che assai semplicemente elabora i dati che immettiamo nel sistema, anche il più semplice, come quello del tasto "invio") siano privi di difetti e non provochino danni. Anzi, ripetutamente gli organi di informazione riportano, non si sa con quanta attendibilità, siffatti incidenti. Quel che però si constata è che, setacciando la giurisprudenza al di qua e al di là dell'Atlantico, e senza trascurare il Pacifico, il numero di casi nei quali l'universale istituto della responsabilità civile è stato chiamato in causa per raddrizzare i torti informatici è insignificante in confronto con altri settori. Il fenomeno va considerato attentamente: solitamente l'avvento di nuove tecnologie porta con se il verificarsi di incidenti (si pensi ai treni prima e agli autoveicoli poi). In questo caso, invece, nonostante la onnipresenza degli strumenti informatici e dell'uso dei dati, questo non è successo. Le ragioni possono essere legate alla dimensione delle imprese, alla generalizzata copertura assicurativa ma soprattutto, e più verosimilmente, alla immaterialità dei processi produttivi del danno, alla difficoltà di ricondurla ad una errata o insufficiente elaborazione dei dati, e alla circostanza che il danno sovente consiste nella interruzione di attività (come nei classici casi di interruzione della energia elettrica).
Poco di nuovo dunque? L'elemento che va oggi considerato e sul quale vi è un notevole dibattito è rappresentato dagli algoritmi – che riescono a scavare, selezionare e orga-

nizzare milioni e milioni di dati – sulla loro genesi e costruzione. Soprattutto quando essi siano utilizzati non per conoscere il passato, ma piuttosto per orientare scelte future e/o prevedere con ragionevole approssimazione comportamenti futuri, costituisce dato acquisito che essi riflettono scelte valoriali del soggetto che li realizza ovvero li commissiona. La prima esigenza che si pone è quella della trasparenza di tali opzioni, onde evitare discriminazioni digitalmente orientate, tipicamente quelle di genere, di età o di razza.

La seconda, connessa, è quella della individuazione di parametri professionali nella elaborazione degli algoritmi. Attualmente essi sono assenti e dunque difetta uno "stato dell'arte" su cui fondare un giudizio di diligenza/negligenza. In particolare va considerato che essi sono solitamente inclusi nell'interno di programmi più articolati, la cui realizzazione dipende da molteplici produttori e assemblatori (ad es. "app" che orientano le scelte del visitatore in una certa località; sistemi di ricerca di soluzioni di viaggio; navigatori per il traffico stradale). Anche in questi casi l'emersione di profili di responsabilità appare estremamente difficile in primo luogo perché esso deriverebbe da scelte volontarie – ancorché indirizzate – dell'utente; ed in secondo luogo dalla sfuggente prova del danno. Di qui l'esigenza di interventi di natura preventiva idonei a formulare giudizi di responsabilità oggettiva.

5. Decisioni pubbliche basate sui dati

L'ultima considerazione svolta nel paragrafo precedente porta ad analizzare il rilievo giuridico che hanno decisioni di soggetti pubblici effettuate sulla base di analisi di dati. Tali decisioni sono del genere più svariato e possono riguardare soggetti singoli, come gruppi di persone o comunità.

Nel primo caso – e si parla solitamente di "dati granulari" – l'esempio più ovvio sono le indagini informatiche per identificare soggetti che possono avere connessioni con il terrorismo o con altri gruppi criminali. Ma se ne trovano molteplici nel campo fiscale (di cui, per rimanere in Italia, gli "studi di settore" sono un esempio egregio). In taluni casi la analisi, anche predittiva, dei dati è regolamentata (Direttiva 680/16), in altri casi è coperta da una coltre di incertezza regolamentare, soprattutto laddove il soggetto pubblico, nell'esercizio della sua – doverosa – attività ispettiva, operi a campione.

Un altro settore di grandissima importanza pratica è quello della previdenza sociale nel quale piani contributivi e pensionistici vengono scelti, da lavoratori ma anche da imprese, sulla base di dati relativi al singolo individuo o alla singola impresa, ma anche dall'universo dei soggetti secondo previsioni fortemente influenzate dalla demografia e da politiche di spesa pubblica.

In tutti questi casi la verificabilità del processo di analisi appare indispensabile a tutela dell'indagato, del contribuente, del lavoratore, i quali possono subire gravissimi ed ingiustificati danni da qualche impostazione discrezionale che lo fa oggetto di indagine/ispezione (il soggetto cui viene negato l'imbarco in aeroporto perché rientrante in una categoria ipoteticamente rischiosa; l'impresa perfettamente in regola che viene tartassata da ispezioni fiscali o contributive).

Vi sono poi scelte pubbliche che riguardano interi gruppi (ad es. soggetti affetti da una certa patologia) o comunità (in particolare territoriale). Si pensi alla pianificazione urbanistica, alla rete dei trasporti, alla dislocazione dei servizi (scuole, ospedali): in una prospettiva di decisione informata è naturale che il soggetto pubblico si avvalga di sistemi di elaborazione di grandi moli di dati. Sarebbe, anzi, un vizio procedurale se non lo facesse. Ma è necessario comprendere quali dati e quali metodiche sono stati utilizzati. E' noto da quasi un secolo che le statistiche subiscono la influenza soggettiva di chi le raccoglie ed elabora. Lo stesso può dirsi della analisi dei dati i quali, ancora più facilmente, possono essere piegati per giustificare talune soluzioni.
La responsabilità dei soggetti pubblici si estende dunque ad una "*data accountability*" che richiede nuove forme di verifica ed accertamento. Di certo, in società democratiche evolute, non ci si può limitare – come una volta – a ritenere che la sanzione di scelte pubbliche errate sia esclusivamente politica, nel voto. Il procedimento partecipativo alla formazione delle decisioni e la loro sindacabilità passa, ora, inevitabilmente attraverso una verifica – che potrebbe anche consistere nell'opporre altri dati, altri algoritmi – digitale.

6. La mutante epistemologia del giurista

L'ultimo riferimento ci porta ad un tema di grande rilievo anche se di teoria generale del diritto e di lunga portata.
La circostanza che il giurista operi in un mondo ed in contesto dominato dai dati cambia il suo modo di conoscere il diritto, di crearlo, di interpretarlo.
L'ipotesi che si sottopone alla discussione che nel mondo dei Big Data cambia l'epistemologia del giurista, ovverosia il modo in cui egli organizza le regole, soprattutto nella tradizione dell'Europa continentale in cui è abituato a ragionare per categorie astratte e per norme di portata generale.
Il cambio di passo mentale consiste nel passaggio da una logica essenzialmente causale, in cui l'argomentazione – e dunque la concatenazione delle regole – segue un ragionamento consequenziale, ad una logica di tipo inferenziale.
Nel mondo dei grandi dati interessano non certezze bensì collegamenti probabilistici fra elementi fra di loro ontologicamente diversi. L'esempio più ovvio è quando scegliamo di acquistare un bene o un servizio sulla rete Internet ed immediatamente ci viene proposto l'acquisto di un bene o servizio che l'algoritmo governante inferisce poter essere di nostro interesse ("Coloro i quali hanno acquistato X hanno acquistato anche Y"). Come si applica questo procedimento al mondo del diritto? In primo luogo nella fase di produzione delle norme in cui si sostituisce ad un dato certo e apparentemente statico (le statistiche, appunto) la elaborazione dinamica di dati, anche in funzione predittiva, nella valutazione di impatto della nuova norma. Inferiamo – perché non siamo, né possiamo, essere certi – che una determinata norma porterà al conseguimento degli obiettivi che essa si prefigge, anche perché, sempre inferenzialmente, assumiamo che la condotta dei suoi destinatari sarà di un certo genere.
Ben inteso in questo non vi è nulla di intrinsecamente errato ed è anzi ben possibile che

il risultato sia ben più coerente rispetto a quello conseguito da una norma basata solo su assunzioni valoriali se non ideologici, anche non espressi.
Quel che va sottolineato è il diverso procedimento logico seguito che punta alla creazione di una norma che, probabilisticamente e predittivamente, coprirà il maggior numero di casi. Senza fare eccessivi sforzi di fantasia si pensi alla applicazione di questi criteri nel campo delle norme tributarie in cui il gettito è legato al grado di spontanea adesione dei contribuenti e alla difficoltà per questi di adottare strategie elusive.
Ma quel che colpisce di più è che la logica inferenziale non è utilizzata solo per comprendere ciò che è avvenuto, ma anche e soprattutto in funzione predittiva. La c.d. *predictive analytics* diventa dunque lo strumento attraverso il quale vengono prese decisioni che riguardano la collettività (legislative, regolamentari) o l'individuo (orientamento al lavoro, indagini penali). Gli esempi più evidenti sono l'uso che già ora viene fatto di tali strumenti nelle procedure di scelta di assunzione di un lavoratore o di una lavoratrice. Oppure nella stipula di un contratto di assicurazione e a quali condizioni. Con il che alcuni principi che sono fra i capisaldi del diritto contemporaneo, quello di eguaglianza e di non discriminazione, sono messi in crisi, e si torna ad un conflitto, le cui radici vanno ben oltre la filosofia e affondano nella religione, fra determinismo e libero arbitrio.

Tutela dei diritti fondamentali nell'era digitale e contesto valoriale: una indagine transatlantica*

Oreste Pollicino

Abstract

Il saggio esamina la rilevanza del cosiddetto "*judicial frame*" per definire la protezione giurisprudenziale della libertà di espressione nell'ambito di Internet. L'autore, in particolare, compara i differenti punti di vista dalla Corte europea dei diritti dell'uomo e della Corte suprema statunitense. In conclusione, il saggio spiega come l'adozione, da parte delle corti, di una prospettiva interna o esterna nell'ambito della protezione dei diritti fondamentali in Internet conduce di frequente a un diverso bilanciamento e, infine, a soluzione differenti per casi che da un punto di vista fattuale non paiono così dissimili.

The essay explores the relevance of the so-called "judicial frame" to define the judicial protection of freedom of speech on the Internet. The Author, in particular, compares the different points of view of the European Court of Human Rights and the Supreme Court of the United States of America. In conclusion, the work shows how the adoption of an internal or external point of view about the judicial protection of fundamental rights in Internet leads, very often, to a different balancing and, finally, to different results for cases which are not so different from a factual point of view.

Sommario

1. Introduzione. - 2. Metafore e *frame*: dalle scienze cognitive al diritto nell'era digitale. - 3. Il *frame in action*: libertà di espressione in Internet nella giurisprudenza della Corte europea dei diritti dell'uomo e nella Corte suprema degli Stati Uniti. - 4. Conclusioni.

Keywords: Internet, Diritti fondamentali, Creatività dei giudici, Metafore, Argomentazione giuridica

1. Introduzione

Per provare a fare emergere la connessione, solo apparentemente tenue, tra linguaggio metaforico, creatività giurisprudenziale e tutela dei diritti fondamentali in ambito digitale è utile mettere a confronto due brani che hanno apparentemente pochissimo in comune.

Il primo. «Osserva il Collegio che l'art. 1 della legge n. 47 del 1948 si limita a definire esplicitamente il concetto di stampa nella sua accezione tecnica di riproduzione tipo-

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio anonimo, in quanto riproduce la relazione presentata dall'A. al convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno" (Messina, 26-27 maggio 2017).

grafica o comunque ottenuta con mezzi meccanici o fisico-chimici. Il termine stampa, però, ha anche un significato figurato e, in tal senso, indica i giornali, che sono strumento elettivo dell'informazione e lo erano soprattutto all'epoca in cui entrarono in vigore la Carta Fondamentale e la richiamata legge n. 47 del 1948, quando cioè gli altri *mass media,* in particolare la televisione e i siti di informazione *on line,* non erano operativi. Questo concetto di stampa in senso figurato definisce il prodotto editoriale che presenta i requisiti ontologico (struttura) e teleologico (scopi della pubblicazione) propri di un giornale».

Il secondo. «*Now you can see the meaning of my title cyberspace and the Law of the Horse. When asked to talk about Property in Cyberspace, my reaction was, "Isn't this just the law of the horse?"*[...] *This leads directly to my principal conclusion: Develop around law of intellectual property, then just apply it to computer networks*».

Come si diceva, i due brani apparentemente hanno pochissimo in comune. Nel primo caso si tratta di giudici italiani (la Cassazione a Sezioni Unite)[1] che si pronunciano, nel gennaio 2015, su una specifica questione legata all'applicazione delle regole (in *bonam* e *malam partem*) previste per la carta stampata anche per Internet, ed in particolare per le riviste telematiche ed elettroniche.

Nel secondo caso, si tratta di un altro giudice, Frank Easterbrook[2], che però scrive nella sua "capacità accademica", in occasione di un Convegno a Chicago dedicato al nascente *cyberspace* (ritorneremo su questa metafora costitutiva) e si chiede ironicamente, nel 1995, alle origini del web, che senso abbia parlare di "diritto dei cavalli" quando basterebbe riferirsi al genere "diritto degli animali", e propone di non adottare alcun *novum* regolamentare per il mondo dei bit ma, semplicemente, di applicare, con buon senso, le regole giuridiche tradizionali del mondo degli atomi al nuovo ambiente tecnologico.

In realtà però, pur nella loro diversità, i due brani evidenziano il medesimo dilemma in cui si trovano operatori, interpreti, ma anche legislatori quando devono "trasferire" alcune categorie, non solo giuridiche, dal campo analogico a quello digitale. Traslazione e traduzione *sic et simpliciter* delle categorie tradizionali al nuovo contesto tecnologico oppure necessità di ripensare e rimodulare le stesse categorie per l'esigenza di adeguarle (manipolarle?) ad uno scenario tecnologico completamente differente?

Le opzioni adottate nei due passi sopra citati sembrano suggerire due risposte diametralmente opposte.

Nel primo caso, le Sezioni Unite della Cassazione propongono un ripensamento «in senso figurato» di quanto (la nozione di stampa) finora era stato definito in senso tecnico, in modo che tale nozione possa aprirsi all'evoluzione tecnologica ed, in particolare, all'impatto di Internet.

Nel secondo caso, invece, emerge nelle parole di Easterbrook una cornice valoriale o *frame* (ci ritorneremo) di resistenza alla tecnologia emergente che si concretizza nella proposta di una mera traslazione applicativa dello strumentario giuridico tradizionale allo scenario digitale. Ma, tanto in un caso, quanto nell'altro, sia quando si propone una rilettura (anche manipolativa) delle regole esistenti in forza del mutamento del fattore

[1] Cass. pen., sez. un., 17 luglio 2015, n. 31022.

[2] F.H. Easterbrook, *Cyberspace and the Law of the Horse*, University of Chicago Legal Forum 207, 1996.

tecnologico[3], sia invece quando si propende per una semplice traslazione di dette regole dal piano materiale a quello immateriale, l'interprete, e specialmente il giudice, non può fare a meno di esercitare la sua *legal immagination*, per dirla con James Boyd White[4]. Di più, qualsiasi sia la strada prescelta, elemento necessario di quell'operazione di trasferimento o traslazione cui si faceva prima riferimento delle categorie "classiche" dal mondo materiale a quello immateriale, è l'utilizzo del linguaggio metaforico.

In fondo, la metafora, quasi geneticamente, e sicuramente etimologicamente, ha in sé quel *meta-pherein*, trasferire "oltre", attraverso campi di esperienza diversi, e implica, per dirla con Winter[5], quel processo di «*carry over, transfer knowledge across domain*».

Da questo punto di vista, il riferimento alla metafora diviene uno strumento, se non necessario, sicuramente elettivo, nel percorso argomentativo dell'interprete che si interroghi sull'impatto dell'evoluzione tecnologica sulla "tenuta" delle categorie giuridiche tradizionali.

Ciò che mi piacerebbe provare in questa sede è come tali operazioni argomentative di trasferimento concettuale dal mondo degli atomi al mondo dei bit non siano neutrali ma, in base all'opzione assiologica o cornice valoriale che ne costituisce il fondamento, hanno un impatto sull'esito del bilanciamento in concreto operato dal giudice e, in ultima istanza, sul livello di protezione dei diritti in gioco.

In questo scenario, il giudice costituzionale o supremo sembra avere un ruolo ancora più delicato, perché deve scegliere, per dirla con Cass Sunstein[6], tra «*constitutional traslation and constitutional caution*», ovvero decidere se tradurre i valori costituzionali originari attraverso una interpretazione tecnologicamente orientata dei parametri rilevanti, in modo da consentirne una loro estensione alle nuove esigenze emerse con l'evolvere della evoluzione tecnologica o se, invece, esibire un approccio di *self-restraint*, lasciando questo compito al decisore politico.

2. Metafore e *frame*: dalle scienze cognitive al diritto nell'era digitale

L'*humus cruciale* che ha fatto da base a tali riflessioni va identificato negli studi degli scienziati cognitivi che attribuiscono alla metafora una valenza costitutiva nel linguaggio (e non, in contrapposizione con alcune tesi più tradizionali, solo accessoria o ornamentale). Il riferimento è ovviamente a George Lakoff ed alla sua convinzione in forza della quale: «*metaphor is not act of description is a way of conceptualization*»[7].

Secondo tale prospettiva, la metafora è una forma di pensiero che detiene il potere di

[3] P. Costanzo, *Il ruolo del fattore tecnologico e le trasformazioni del costituzionalismo*, Relazione al convegno annuale AIC, Salerno, 23-24 novembre 2012, in *Costituzionalismo e globalizzazione*, Atti del XXVII Convegno Annuale, Associazione Italiana Dei Costituzionalisti, Napoli, 2014, 43 ss.

[4] J. B. White, *The Legal Imagination*, Chicago, 1985,

[5] S. L. Winter, *A Clearing in the Forest: Law, Life, and Mind,* Chicago, 2001.

[6] C. R. Sunstein, *Constitutional Caution*, in *University of Chicago Legal Forum*, 1(11), 1996.

[7] G. Lakoff - M. Johnson, *Philosophy in the Flesh: the Embodied Mind & its Challenge to Western Thought*, New York, 1999.

strutturare la nostra percezione allo scopo di essere in grado di effettuare operazioni concettuali di trasferimento da un prototipo familiare ad uno meno familiare.
In questo quadro, è per noi assai utile il concetto di *frame* proposto da Lakoff, in cui si contestualizza un utilizzo costitutivo della metafora in forza del quale quest'ultima è il punto focale di un contesto che ne costituisce l'indispensabile cornice.
L'utilità ai nostri fini della nozione di *frame* è evidente: trasferendo tale concetto dall'ambito della teoria del linguaggio e delle scienze cognitive a quello delle teorie dell'interpretazione e dell'argomentazione, e quindi individuando come sottocategoria del *frame* il *judicial frame*, è possibile fare emergere quali opzioni valoriali di base facciano da cornice all'utilizzo di una specifica metafora da parte delle corti e costituiscano il fondamento di una determinata operazione di *judicial balancing*.
Rimandando ad un prossimo studio, già *in fieri*[8], un'analisi approfondita circa il ruolo (costitutivo) giocato dalla metafora nel linguaggio giuridico in generale e nello *ius dicere* in particolare, deve ora indagarsi quale linguaggio, non solo metaforico, caratterizzi il *frame* dei giudici quando si confrontano, nello specifico, con il fattore tecnologico.
Apparentemente, ma vedremo tra un momento come lo scenario sia molto più complesso, sembrerebbero esserci due sole opzioni argomentative: da una parte ricontestualizzare i parametri rilevanti, ricreare nuovi *frame*, alla luce del nuovo ambiente tecnologico o, dall'altra parte, esibire una *judicial deference* nei confronti del legislatore.
Di quest'ultimo avviso è Larry Lessig: «*My sense is that, knowing nothing, or at least not very much, terrified by the threats of which they don't know, these judges will defer to democratic authority*»[9].
Rimane però un piccolo problema: il giudice deve decidere il caso che gli è sottoposto, non ha molta scelta. Emblematico a questo proposito quanto Justice Kennedy scrive nella sua *dissenting opinion* nel caso *Denver Area Educational Telecommunications Consortium*[10], avente ad oggetto la regolamentazione della televisione via cavo e deciso nel 1996 dalla Corte suprema statunitense. Quest'ultima, nel caso di specie, è arrivata quasi a dire, con riferimento al (a quel tempo nuovo) fattore tecnologico, «*we don't know yet, but here's the best we can*». Kennedy incalza i giudici di maggioranza sostenendo che «*doubt and caution may be reasons for the Supreme Court not to take a case, but once taken, it is hard to accept the attitude of the Court to not decide. This is why metaphors and analogies to other areas of our First Amendment case law become a responsibility, rather than the luxury the plurality considers them to be*».
In altre parole il caso va deciso, in qualche modo il fattore tecnologico va affrontato, ed è qui che il *frame*, elaborato dagli scienziati del linguaggio quale struttura cognitiva designata per facilitare la comprensione diventa *judicial frame*e tecnica argomentativa grazie a cui, per l'appunto, argomentare attraverso metafore o applicazioni analogiche consente uno spostamento dal prototipo familiare ad un nuovo contesto tecnologico.
Ora la *summa divisio* che mi pare si possa applicare a tal riguardo, è tra un *frame* di resistenza alla tecnologia, da una parte, ed uno, alternativo, di apertura al fattore tecno-

[8] A. Morelli - O Pollicino, *Le metafore della rete. Linguaggio figurati,* judicial frame *e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto,* in *Rivista dell'Associazione dei Costituzionalisti Italiani*, 1, 2018.

[9] L. Lessig, *Reading the Constitution in Cyberspace*, in *Emory Law Journal* 45(3), 1996, 874 ss.

[10] *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, 518 U.S. 727 (1996).

logico dall'altra. Cornici valoriali che possono sintetizzarsi in ostilità o inclinazione a riconoscere per un verso o a negare per un altro il *novum* della tecnologia in oggetto rispetto al passato, quindi ragionare, rispettivamente, in termini di discontinuità o di continuità rispetto allo *status quo*.

In ogni caso, qualunque sia il *frame* prescelto, sia che vada nel senso del riconoscimento di una continuità o, invece, una discontinuità rispetto all'assetto tecnologico preesistente, l'operazione in esame non è mai neutrale, perché condizionata da un'altra importante alternativa spesso sottovalutata nella ricostruzione della rappresentazione del giudice di fronte al fattore tecnologico: la possibilità che egli adotti, per riprendere la contrapposizione tra punto di vista esterno ed interno di Hart[11], una prospettiva interna alla nuova tecnologia o invece una esterna a quest'ultima.

Una tale contrapposizione tra punto di vista esterno ed interno al *novum* tecnologico, emerge già, *ante litteram*, rispetto alla nascita di Internet, con riguardo al mezzo telefonico, nella decisione *Olmstead*[12], della Corte Suprema ed, in particolare nella *dissenting opinion* di Justice Brandeis. Secondo l'opinione di maggioranza, l'utilizzo di intercettazioni telefoniche ottenute da agenti federali senza alcuna autorizzazione da parte del giudice e poi utilizzate quali prove in dibattimento non violava il IV Emendamento in quanto «*listening to a private telephone conversation did not require a physical search or entry into a person's private space*».

Il *judicial frame* che caratterizza la *dissenting opinion* di Brandeis è invece di natura contraria e insiste per un riconoscimento della discontinuità tecnologica tra (l'allora) nuovo mezzo e lo *status quo* e quindi propende per una interpretazione tecnologicamente orientata di *seizure* e *search*, alla base, come è noto del IV Emendamento[13].

Perché un *frame* cosi diverso per giudici che siedono, nello stesso momento, nella stessa Corte? La differenza potrebbe spiegarsi, come si accennava, applicando una delle distinzioni più conosciute di Hart cui prima si faceva riferimento: la contrapposizione tra la prospettiva interna di chi fa parte del gioco rispetto alla prospettiva esterna dell'*outsider*.

In fondo, mentre la maggioranza della Corte in *Olmstead* si pone in una prospettiva esterna, anche spazialmente, rispetto a chi è coinvolto in una conversazione telefonica, Brandeis, al contrario, elabora, da *internal player* (e non da *outsider*) il suo *judicial frame* guardando al nuovo (allora) mezzo tecnologico da una prospettiva interna allo stesso, e concependo la rete telefonica come un mezzo privilegiato per creare un *virtual closet*, in cui i segreti utilizzando le stesse parole di Brandeis «possono essere sussurati». Sulla base di tale cornice valoriale, strutturalmente differente rispetto a quello che si è vista caratterizzare il *frame* dell'opinione di maggioranza, Brandeis non ha difficoltà a concludere che, se pur non *phisical*, vi è stata comunque una intrusione, se non nella proprietà, in ogni caso nella sfera privata dei soggetti intercettati che ha portato alla

[11] H.L.A. Hart, *Concept of Law,* Oxford, 1961.

[12] *Olmstead v. United States*, 277 U.S. 438 (1928).

[13] Il IV Emendamento della Costituzione degli Stati Uniti recita: «*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*».

violazione del IV Emendamento.
Se la possibile contrapposizione tra prospettiva esterna e interna, con riguardo alla identificazione del *novum* tecnologico emerge sicuramente prima di Internet, è con l'esplosione del web che tale contrapposizione trova il suo *habitat* tecnologico privilegiato per ulteriormente evidenziare la dialettica tra apertura e resistenza a detto *novum*.
Il che non può stupire. Non è un caso che Internet sia l'unico *medium* con sua metafora spaziale costitutiva: *cyberspace*. Questo perché, a differenza delle altre tecnologie, il contesto, la cornice di riferimento, ha una natura talmente costitutiva, talmente autosufficiente da poter competere con la realtà fisica e quindi consentire in capo al giudice una scelta tra quale prospettiva caratterizzare il suo *judicial frame*, quella interna o esterna, quando si trova ad applicare il diritto di Internet.
Pensando ai due passaggi con cui si sono aperte queste riflessioni, mentre la preferenza per il "senso figurato" rispetto a quello tecnico di stampa dimostrata dalle Sezioni Unite della Cassazione fa emergere una prospettiva interna che guarda alla realtà immateriale come luogo di elezione per la riconsiderazione di alcune categorie o istituti tradizionali, il riferimento ironico e provocatorio al "diritto dei cavalli" da parte di Easterbrook denota una prospettiva esterna rispetto all'oggetto di indagine, di chi guarda alla dimensione analogica quale punto di riferimento elettivo per l'applicazione di una certa disciplina e la dimensione digitale come mero accessorio a cui è possibile e financo consigliabile trasferire *sic e simpliciter* le categorie giuridiche tradizionali.

3. Il *frame in action*: libertà di espressione in Internet nella giurisprudenza della Corte europea dei diritti dell'uomo e nella Corte suprema degli Stati Uniti

Una volta fissate le coordinate di riferimento che fanno da substrato teorico all'analisi, si vuole adesso provare a testare come un differente *judicial frame* possa determinare una significativa differenza nell'esito finale cui può pervenire il bilanciamento operato dai giudici quando si trovano a tutelare diritti fondamentali esercitati in rete. Ci si concentrerà in particolare su come una cornice valoriale diversa adottata rispettivamente da Corte di Strasburgo e Corte Suprema degli Stati Uniti in relazione alla tutela della libertà espressione in internet online, possa essere determinante per l'identificazione del livello di protezione da accordare a tale libertà allorché si scontra con altri diritti fondamentali.
Iniziando l'esame partendo dall'art. 10 CEDU[14], si deve in primo luogo riconoscere

[14] L'art. 10 CEDU recita: «1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive. 2. L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario».

che il perimetro della protezione garantita da questa disposizione, è stato definito, nel mondo degli atomi, e quindi offline, in modo ampio dalla Corte di Strasburgo, che ha segnato, sin dai casi *Handyside c. Regno Unito*[15] e *Jersild c. Danimarca*[16], alcuni importanti punti fermi.

In *Handyside*, una storica sentenza del 1976, la Corte ha chiarito che la tutela racchiusa nell'art. 10 non si applica soltanto alle "informazioni" o alle "idee" che sono accolte in modo favorevole tra i consociati o che sono percepite come inoffensive o comunque con indifferenza. L'ambito di copertura offerto da questa norma, infatti, si estende anche alle espressioni offensive, scioccanti o disturbanti rispetto allo Stato o a qualsiasi parte della popolazione. In un passaggio successivo la Corte europea ha enfatizzato come l'ampiezza di questo ambito di tutela risponda alle esigenze di pluralismo, tolleranza e apertura mentale senza le quali non sarebbe possibile configurare una società democratica. Questa sentenza, invero, allarga di molto i confini della libertà di espressione, affermando che anche quei contenuti che faticherebbero a ottenere approvazione presso la generalità dei consociati in quanto scioccanti od offensivi non possono essere privati, per ciò solo, delle garanzie che accompagnano la libertà di espressione. Non è dunque il livello di accettazione o di gradimento sociale di un contenuto a giustificarne l'accesso alle garanzie della libertà di parola.

Queste affermazioni sembrerebbero tuttavia accreditare l'assunto per cui tanto più variegato è il panorama delle idee e delle opinioni, quanto più il carattere democratico di una democrazia ne gioverà. Si deve tuttavia misurare questo assunto con la varietà della fisionomia delle *fake news*, che non portano con sé uno specifico pregio dal punto di vista informativo, ma anzi realizzano effetti contrari alle finalità della libertà di espressione, diffondendo presso la collettività messaggi non veritieri. Il quesito che occorre porsi, dunque, è se quelle notizie che sono del tutto prive di un'utilità sociale, e che non racchiudono alcun contributo all'informazione degli individui, in quanto false o tendenziose, meritino egualmente di circolare alla stregua di quei contenuti che, al contrario, soddisfano un interesse informativo secondo il parametro convenzionale.

In *Jersild,* uno dei primi casi di *hate speech*, la Corte di Strasburgo ha dimostrato sensibilità per il contesto peculiare entro il quale le espressioni offensive sono formulate, ritenendo che lo stato contraente coinvolto (la Danimarca) avesse violato l'art. 10 CEDU nell'imporre una condanna a carico di un giornalista che aveva intervistato un gruppo di giovani appartenenti a frange politiche estremiste i quali, nel corso del colloquio radiofonico, avevano rilasciato dichiarazioni patentemente offensive e razziste.

Dal panorama giurisprudenziale prima richiamato emergono chiare indicazioni in favore di una portata espansiva della libertà di manifestazione del pensiero, il cui perimetro sembrerebbe giungere ad abbracciare, nell'interpretazione della Corte europea, anche quelle espressioni che non offrono un significativo contributo allo sviluppo democratico e alla formazione dell'opinione pubblica e che presentano un contenuto raccapricciante e disturbante.

Rispetto al *judicial frame* che si è descritto con riferimento alla protezione apprestata dalla Corte di Strasburgo alla protezione della libertà di espressione e di informazione

[15] CEDU, *Handyside c. Regno Unito*, ric. 5493/72 (1976).

[16] CEDU, *Jersild c. Danimarca*, ric. 15890/89 (1994).

nel mondo degli atomi, quale cornice valoriale sembra invece emergere nella giurisprudenza della stessa Corte quando la medesima libertà è al contrario esercitata nel mondo dei bit?

Guardando alle decisioni in cui la Corte di europea è stata chiamata pronunciarsi nell'ambito di ricorsi occasionati da presunte violazioni della libertà di espressione in Internet, si nota un'inclinazione a rimodulare quella portata espansiva che aveva contraddistinto la precedente giurisprudenza sulle applicazioni dell'art. 10 in ambiente analogico. Questa nuova modulazione dell'ambito e della portata della libertà di espressione in rete sembra radicarsi nel convincimento che l'utilizzo delle tecnologie digitali presenti un grado di offensività maggiore rispetto ad altri interessi con cui l'esercizio della libertà di parola deve coniugarsi[17]. Beninteso: il carattere "relativo" e "cedevole" rispetto a operazioni di bilanciamento dei diritti fondamentali tutelati dalla CEDU non costituisce certo una novità, ma questo carattere appare accentuato nel campo della casistica che ha a che vedere con Internet.

Questa lettura per così dire "restrittiva" conosce i suoi prodromi nella pronuncia *Editorial Board of Pravoye Delo* e *Shtekel c. Ucraina*[18] del 2011, in cui la Corte ebbe modo di argomentare che: «*The Internet is an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit information. The electronic network, serving billions of users worldwide, is not and potentially will never be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned*».

A differenza della Corte Suprema che, come si vedrà, nella sentenza *Reno v. ACLU*[19]del 1997 ha da subito messo in luce il potenziale per una espansione (definita "fenomenale") dello spazio di esercizio della libertà di pensiero, la Corte europea è parsa, in questa pronuncia, preoccupata soprattutto dalle criticità dell'uso del mezzo Internet e dei rischi connessi a una lesione più significativa di altri diritti fondamentali che potrebbero scontrarsi con la libertà di espressione e di informazione. Tutto questo quando, come si diceva, la partita si gioca non nel mondo degli atomi ma in quello dei bit.

Occorre poi ricordare che, come evidenziato in precedenza, la Corte europea ha da sempre indicato nella libertà di espressione, e, in particolare, nella libertà di stampa, una sorta di cartina di tornasole (il "cane da guardia") del livello di democrazia di un ordinamento. Sembra che anche questo portato consolidato nella giurisprudenza della Corte di Strasburgo sia stato rivisitato. Dapprima, nella sentenza *Stoll c. Svizzera*[20] del 2007, la Corte è parsa convalidare l'imposizione di obblighi più stringenti in capo ai

[17] O. Pollicino - M. Bassini, *Free speech, defamation and the limits to freedom of expression in the EU: a comparative analysis,* in A. Savin - J. Trzaskowski (a cura di), *Research Handbook On EU Internet Law*, Cheltenham-Northampton, 2014, 508 ss.

[18] CEDU, *Editorial Board of Pravoye Delo e Shtekel c. Ucraina,* ric. 33014/05 (2011).

[19] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

[20] CEDU (Grande Camera), *Stoll c. Svizzera*, ric. 69698/01 (2007).

giornalisti nel caso di utilizzo di Internet rispetto alla carta stampata: «*The safeguard afforded by Article 10 to journalists in relation to reporting on issues of general interest is subject to the provision that they are acting in good faith and on an accurate factual basis and provide "reliable and precise" information in accordance with the ethics of journalism* […] *These considerations play a particularly important role nowadays, given the influence wielded by the media in contemporary society: not only do they inform, they can also suggest by the way in which they present the information how it is to be assessed. In a world in which the individual is confronted with vast quantities of information circulated via traditional and electronic media and involving an ever-growing number of players, monitoring compliance with journalistic ethics takes on added importance*».

Inoltre, un indirizzo analogo trova conferma nella pronuncia *KU c. Finlandia*[21] del 2008: «*Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context. Such framework was not, however, in place at the material time, with the result that Finland's positive obligation with respect to the applicant could not be discharged*».

Non si deve, naturalmente, dimenticare che le decisioni della Corte europea riposano in larga parte sulla specificità delle singole situazioni che hanno occasionato, di volta in volta, i ricorsi.

Questi elementi consentono di ridimensionare o comunque di ponderare correttamente la portata di pronunciamenti all'apparenza radicali. Tale discorso vale, per esempio, per il caso Delfi AS c. Estonia[22], una decisione della Grande Camera del 2015 che pure conferma la linea di tendenza descritta finora, incline a validare con maggior favore possibili limitazioni della libertà di espressione online (basti, tra tutti, questo inciso: «*Defamatory and othertypes of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online*»).

La Corte ha stabilito che porre a carico del gestore di un portale di informazione online il pagamento di una somma, pur esigua (nel caso di specie, 320 Euro), a titolo di risarcimento del danno subito da un soggetto in conseguenza di alcuni commenti diffamatori rimasti accessibili per circa sei settimane a corredo di un articolo pubblicato sul sito non costituisce una restrizione sproporzionata alla libertà di espressione, in ragione della necessità di un suo bilanciamento con la tutela da assicurare ad altri diritti della personalità (quali l'onore e reputazione) del soggetto diffamato.

Va detto che la stessa vicenda sarebbe stata verosimilmente giudicata in altro modo dalla Corte di giustizia, il cui scrutinio però si sarebbe fondato su criteri diversi rispetto a quelli adottati da un giudice dei diritti fondamentali come la Corte di Strasburgo, appuntandosi all'opposto sul tema dell'eventuale responsabilità del gestore del portale

[21] CEDU, *KU c. Finlandia*, ric. 2872/02 (2008).

[22] CEDU (Grande Camera), *Delfi AS c. Estonia*, ric. 64569/09 (2015).

online e dunque sull'applicazione della Direttiva 2000/31/CE. La sentenza in parola è senz'altro problematica e difficile da riconciliare con il diritto dell'Unione europea: al netto della necessità di adottare una prospettiva d'indagine non fuorviante (il *thema decidendum* qui era se l'imposizione di un risarcimento in forma pecuniaria, di entità ridotta, potesse configurare una violazione ingiustificata dell'art. 10 CEDU, e non la compatibilità di tale opzione con la Direttiva 2000/31/CE), la sentenza apre uno spiraglio rispetto alla possibilità di imputare all'editore di un portale contenuti illeciti pubblicati da terzi al verificarsi di determinate circostanze.

Tali indicazioni emergono soprattutto se si confronta la portata della sentenza *Delfi* con quella, di alcuni mesi successiva, che ha visto la Corte di Strasburgo prendere nuovamente posizione su un caso analogo, seppure con esito differente, nella sentenza *MTE c. Ungheria*[23]. La vicenda non presentava sostanziali differenze, in quanto il ricorso era diretto a provocare uno scrutinio sulla compatibilità con l'art. 10 CEDU della condanna riportata dal gestore di un portale di informazione a causa dei commenti diffamatori riportati da terzi, in forma anonima, ossia tramite l'utilizzo di pseudonimi, in calce a una notizia pubblicata sul giornale. La Corte di Strasburgo è giunta, come precisato, a una pronuncia di segno opposto, nel senso della sussistenza di una violazione dell'art. 10, allontanandosi così dal suo precedente in *Delfi*. Secondo la Corte, i due casi si differenziano a causa della natura dei commenti offensivi e del loro diverso disvalore: in *Delfi,* infatti, i contenuti inseriti da terzi presentavano una particolare carica offensiva al punto di configurare una forma di *hate speech*, essendo connotati da toni incitanti alla violenza e all'odio razziale; tale connotazione, che per la Corte sembra provocare una maggiore attrazione di utenti, non si ritrova invece nel caso *MTE* ed è proprio la carenza di questo attributo di manifesta illiceità a giustificare un diverso atteggiamento nei confronti dell'*Internet service provider*.

La Corte di Strasburgo ha così rivisitato il proprio orientamento: peraltro, nella fattispecie non era in questione, come nel caso *Delfi,* la ritardata rimozione di commenti (giacché questa era stata invero eseguita tempestivamente) bensì proprio la responsabilità del gestore della piattaforma per i commenti di natura offensiva pubblicati da terzi. In questo senso, sembra apprezzarsi il tentativo da parte della Corte di avvicinarsi, rispetto al caso *Delfi,* al diritto dell'Unione europea e ai principi sulla responsabilità degli *Internet service provider*.

La stessa cornice valoriale di base che porta ad un'attenuazione, in Internet, della portata espansiva della libertà di espressione si rintraccia anche in due recenti decisioni della Corte europea in cui si è trattato di bilanciare quest'ultima con le istanze di protezione del diritto d'autore.

Anzitutto, nella decisione sul caso *Ashby Donald e altri c. Francia*[24] del 2013 era in discussione se la previsione di una sanzione pecuniaria in relazione alla pubblicazione in un sito Internet di alcune fotografie realizzate da alcuni fotografi professionisti in occasione di un evento, senza il consenso della casa di moda, integrasse o meno una violazione dell'art. 10 CEDU. La risposta del giudice di Strasburgo è stata negativa, dal momento che l'interferenza sull'esercizio della libertà di espressione è stata ritenuta giustificata,

[23] CEDU, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt c. Ungheria,* ric. 22947/13 (2016).

[24] CEDU, *Ashby Donald e altri c. Francia*, ric. 36769/08 (2014).

anche alla luce della natura commerciale delle forme di espressione in discorso, per la cui disciplina gli Stati contraenti dispongono di un margine di apprezzamento più ampio rispetto ad altri ambiti.

Altro caso significativo è quello che ha tratto origine dalla condanna dei gestori del portale The Pirate Bay per violazione delle norme svedesi sulla tutela del diritto d'autore[25]. Chiamata a pronunciarsi sul ricorso contro la condanna, la Corte ha rilevato che: «*Since the Swedish authorities were under an obligation to protect the plaintiffs' property rights in accordance with the Copyright Act and the Convention*, [...] *there were weighty reasons for the restriction of the applicants' freedom of expression*».

Se l'Europa, e in particolare la giurisprudenza della Corte europea dei diritti dell'uomo, si caratterizza per un *frame* di marcata ostilità rispetto all'estensione della libertà di espressione nel mondo dei bit, gli Stati Uniti si contraddistinguono all'opposto come il paese campione della libertà di manifestazione del pensiero anche nel nuovo ecosistema digitale.

Questo atteggiamento trova emersione nella cornice valoriale adottata dalla Corte suprema incline a esaltare fin dalla prima pronuncia in questa materia l'inedita dimensione libertaria del fenomeno Internet. Da subito, agli occhi della Corte suprema statunitense, Internet offre coordinate e spazi nuovi per l'esercizio della libertà di parola, ai quali occorre guardare attraverso lenti e categorie diverse da quelle che si applicano ai media tradizionali. Da qui la scelta, in *Reno*, di mutuare dalla celebre *dissenting opinion* di Justice Holmes l'utilizzo della metafora del *free marketplace of ideas*, la cui perdurante rilevanza, come si dirà oltre, potrebbe essere messa in discussione alla luce dei cambiamenti che hanno interessato Internet nel corso dei suoi primi anni di vita.

La sentenza, che risale al 1997, reagisce al primo tentativo del governo statunitense di limitare l'accesso a contenuti vietati ai minori in Internet, a fronte delle preoccupazioni legate all'impossibilità di replicare, in rete, come ben descritto da Lessig, quelle dinamiche di *zoning* e di *age verification* che prendono corpo nel mondo degli atomi, impedendo ai minori di ottenere la disponibilità di materiali vietati. A questo scopo nel 1996 fu approvato il Communication Decency Act (CDA), che mirava a colpire, in particolare, contenuti definiti come "indecenti" e "manifestamente offensivi". La Corte suprema, tuttavia, ne dichiarò l'incostituzionalità per contrasto con il Primo Emendamento, in quanto le restrizioni previste dal CDA risultavano troppo vaghe e indeterminate, non rispettose dello *strict scrutiny* cui ogni limitazione della libertà di parola dovrebbe essere soggetta secondo l'approccio della Corte suprema: in altri termini, la compressione della *free speech* non era contenuta entro i margini di stretta necessità per il raggiungimento dell'obiettivo perseguito, ossia la tutela dei minori. La Corte suprema svolge, nel suo ragionamento, alcuni interessanti passaggi, su cui si ritornerà in sede conclusiva, sul rapporto tra i media tradizionali e Internet: «*Radio and television, unlike the Internet, have, "as a matter of history* […] *received the mostlimited First Amendment protection*, […] *in large part because warnings could not adequately protect the listener from unexpected program content*. […] [On the Internet], *the risk of encountering indecent material by accident is remote because a series of affirmative steps is required to access specific material*».

La Corte suprema accoglie la metafora del libero mercato delle idee, anzi la esalta indi-

[25] CEDU, *Fredrik Neij e Peter Sunde Kolmisoppic. Svezia*, ric. 40397/12 (2012).

viduando in Internet un terreno elettivo peculiare dove questo libero scambio conosce una eccezionale espansione.

Guardando al *reasoning* della pronuncia è chiaramente individuabile la coppia assiologica riconoscimento della discontinuità tecnologica e del *novum* che la rete Internet porta con sé e prospettiva interna che nella prima parte di questo lavoro si è detto caratterizzare il punto di vista dell'*internal player* e non l'*outsider*. I nove giudici della Corte Suprema resistono alla tentazione di estendere al web la giurisprudenza in tema di attività radiotelevisiva, e quindi di fare prevalere un *frame* di resistenza alla (allora) nuova tecnologia e di conseguente continuità con l'assetto tecnologico precedente. A questo riguardo, gli stessi giudici sottolineano le ragioni specifiche per cui il regime regolatorio del mezzo audiovisivo non è trasferibile *sic et simpliciter* a Internet, a cominciare dal problema specifico delle risorse scarse, proprio (a quei tempi) del mezzo televisivo che necessita di una regolazione pubblicistica e della circostanza che, con specifico riferimento alla tutela dei minori, quest'ultimi, mentre su Internet devono (dovevano nel 1997) fare degli *affermative steps* per accedere a materiale osceno, sarebbero stati invece più esposti a detto materiale guardando, passivamente, la televisione.

Dopo la pronuncia della Corte suprema in *Reno,* altri tentativi si sono susseguiti da parte delle autorità statunitensi per regolare la circolazione di contenuti ritenuti dannosi per i minori. Nessuno di questi tentativi è però uscito indenne dallo scrutinio della Corte suprema. Al 1998 risale il Child Online Protection Act, che recepiva alcune indicazioni della sentenza *Reno*. Secondo la Corte Suprema, però, la definizione di "materiali nocivi per i minori", fondata su un generico rinvio agli standard della comunità di riferimento, non si conformava ai criteri necessari a circoscrivere le limitazioni su base legittima della libertà di espressione.

Analoga sorte ha caratterizzato il terzo e ultimo capitolo della battaglia tra governo statunitense e Corte Suprema per bandire da Internet i contenuti osceni dannosi per i minori, che aveva a oggetto il Child Pornography Prevention Act: anche in questo caso, secondo la Corte Suprema, le restrizioni introdotte per vietare la diffusione di immagini di minori illustrati nel compimento di condotte sessuali o di ogni forma evocativa di atti sessuali risultavano eccessive e prive del necessario carattere di proporzionalità. Si trattava, secondo la Corte Suprema, di norme la cui portata attingeva un ambito ben più ampio di quello che il legislatore avrebbe potuto legittimamente incidere per il raggiungimento dell'obiettivo di tutela dei minori.

Queste pronunce sono indicative di una chiara attitudine a salvaguardare l'esercizio del *free speech* tramite un mezzo ritenuto in grado di assicurare una straordinaria espansione del suo ambito di esercizio. La Corte Suprema, in altri termini, non si è premurata di ricalibrare la propria sensibilità sul punto "al ribasso", ossia dando risalto alle possibili implicazioni critiche dell'utilizzo di Internet, ma al contrario ha confermato la propria visione liberale, addirittura riconoscendo i margini per un accrescimento della libertà di parola alla luce delle caratteristiche di un mezzo del tutto inedito. È emblematico che i tre *strike* della Corte suprema siano caduti su norme previste a tutela di un interesse particolarmente sensibile, quale la protezione dei minori, tale da legittimare normalmente più di altri limitazioni particolarmente invasive della libertà di espressione.

Si coglie così un *judicial frame*, come si proverà ad articolare in modo meno approssi-

mativo in sede conclusiva, tendenzialmente opposto a quello che ha contraddistinto le corti europee, che anziché cavalcare Internet come volano della libertà di manifestazione del pensiero, ne hanno percepito e soppesato soprattutto la portata critica per l'esercizio di diritti concorrenti.

4. Conclusioni

A conclusione di un'analisi che non può che essere approssimativa, preliminare e destinata ad essere integrata quale *work in progress*, non può non confermarsi, guardando alla differenza tra i risultati cui perviene la giurisprudenza della Corte Suprema da una parte e quella della Corte di Strasburgo dall'altra in tema di tutela della libertà di espressione, che l'utilizzo di una determinata cornice valoriale è in grado non soltanto di influenzare l'apparato argomentativo di una decisione e il bilanciamento operato dalle Corti, ma anche, conseguentemente, di incidere sul livello di protezione dei diritti fondamentali in gioco.

Ritorniamo per un momento alla decisione *Reno* prima richiamata della Corte Suprema, in cui quest'ultima afferma che: «è tradizione della nostra giurisprudenza costituzionale presumere, in mancanza di prova contraria che la regolamentazione pubblica del contenuto delle manifestazioni del pensiero è più probabile che interferisca con il libero scambio delle idee piuttosto che incoraggiarlo. L'interesse a stimolare la libertà di espressione in una società democratica è superiore a qualunque preteso, non dimostrato, beneficio della censura». Come si accennava in precedenza, la Corte Suprema aggiunge riferendosi ad Internet che «*the dramatic expansion of this new marketplace of ideas*» contraddice l'idea alla base della proposta di regolazione dell'amministrazione Clinton per cui l'accessibilità di materiale indecente sul web avrebbe quale effetto quello di allontanare gli utenti dalla rete.

Confrontiamo questi passaggi con quanto emerge dalle decisioni che si sono richiamate in precedenza, sempre meno rare negli ultimi tempi, in cui la Corte di Strasburgo è stata chiamata a pronunciarsi sulla conformità al parametro convenzionale fornito dall'art. 10 CEDU dei limiti imposti, dallo Stato convenuto, all'esercizio, su Internet, della libertà di espressione del ricorrente. Dall'analisi, come si è cercato di dimostrare, è possibile identificare un *judicial frame* volto ad una rimodulazione ed un'attenuazione della portata espansiva della protezione accordata dall'art. 10 rispetto all'amplissimo ambito di tutela, prima ricordato, che la libertà di espressione si è vista riconoscere in ambiente analogico.

Rimodulazione e attenuazione la cui, forse, elaborazione più compiuta si trova, per la prima volta, nel 2011, allorché la Corte EDU ha avuto modo di affermare che «*the Internet is an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit information. The electronic network, serving billions of users worldwide, is not and potentially will never be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the*

Internet may differ. The latter undeniably have to be adjusted according to technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned»[26].

È evidente come la Corte di Strasburgo, nel passaggio considerato, abbia accentuato, più che i vantaggi di un'ulteriore amplificazione, sul web, dell'esercizio della libertà di espressione, come fa invece la Corte Suprema, i rischi che una tale amplificazione - attraverso uno strumento tecnologico che sfugge, almeno *prima facie*[27] al controllo degli Stati - possa avere nei confronti di una tutela effettiva di diritti e altre libertà che, sullo stesso *medium*, possono trovarsi, volta per volta, in contrasto.

Le due Corti sembrano animate da presunzioni di segno opposto: quella statunitense presume che una *content regulation* e dunque un controllo non sortisca maggiori benefici della libertà, quella europea, più sospettosa, ritiene verosimile che il mezzo generi pericolo per gli altri diritti e dunque assume la necessità, e quindi la legittimità di correttivi che possano limitare l'esercizio del *free speech*.

A differenza del *digital distrust*, della sfiducia nella nuova tecnologia che emerge dalla giurisprudenza rilevante della Corte europea, è evidente come il *frame* alla base della giurisprudenza richiamata della Corte Suprema sia di fiducia incondizionata nel mezzo che viene considerato in grado di ulteriormente amplificare il portato di libertà insito nel I Emendamento[28].

Interessante come la necessità di guardare al *novum* del mezzo tecnologico e la comparazione con i media tradizionali assume una valenza diversa a secondo del *frame* di riferimento. Nel caso della Corte Suprema, in nome di quella cornice valoriale di fiducia per "la novità" del web, è un argomento utilizzato per giustificare l'esigenza di una minore intrusività regolamentare nei confronti della rete rispetto all'assetto regolatorio caratterizzante il regime televisivo; nel secondo caso è, invece, un argomento utilizzato per giustificare esattamente il contrario, vale a dire una intrusione maggiore da parte degli stati nei confronti della libertà di espressione quando è esercitata su Internet rispetto a quando è esercitata, ad esempio, sulla carta stampata. Tutto questo in nome di quel *frame* di sfiducia nella nuova tecnologia e della potenziale amplificazione del rischio che su Internet altri diritti in contrasto con la libertà di espressione possano essere maggiormente lesi rispetto a quanto può capitare nel mondo degli atomi.

Insomma, per riprendere in chiave manipolativa la celebre esclamazione di Nanni Moretti in Palombella Rossa[29], metafore e *judicial frame* sono davvero importanti nel diritto dell'era digitale.

---

[26] *Editorial Board of Pravoye Delo e Shtekel c. Ucraina*, § 63.

[27] J. Goldsmith - T. Wu, *Who controls internet? Illusions of a Borderless World,* Oxford, 2006.

[28] Il I Emendamento della Costituzione degli Stati Uniti recita: «*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*».

[29] Nel film Palombella Rossa (1989) di Nanni Moretti che esclama in un dialogo surreale con una giornalista "alle prime armi": «le parole sono importanti!».

Lo spazio digitale come oggetto di un diritto reale?*

Attilio Gorassini

Abstract

Navigando tra i concetti di spazio e tempo nel Diritto e analizzando le categorie fondamentali proposte dalla teoria generale del diritto, si è cercato attraverso un esperimento mentale di collocare le nuove tecnologie digitali nella categoria dell'oggetto giuridico: più precisamente nella cosa (considerando il planisfero open source dei cavi, dei nodi, dei satelliti, dei NOC, delle parabole, dei modem) e nei beni (considerando l'energia dei bit e il loro funzionamento ai sensi degli artt. 813 e 814 c.c.).
Le nuove tecnologie digitali creano vero nuovo spazio (secondo i più accreditati risultati della attuale fisica teorica) e rispetto ad esso sembra necessario per il giurista ri-elaborare il concetto di "dominio" come fatto precursore del concetto di possesso e del diritto di proprietà in dimensione frattale.

Exploring the concepts of space and time in law and analyzing the fundamental categories proposed by the general theory of law, the article tries to put the new digital technologies in the category of the legal object through a mental experiment: precisely, partly in the things (considering open source cables, nodes, satellites, NOCs, parables, modems ....) and partly in the goods (considering the energy of the bits and their functioning in accordance with articles 813 and 814 of the Civil Code).
The new digital technologies create real new space in the universe (according to the most important results of the current theoretical physics) and thus it seems necessary for the jurist to re-elaborate the concepts of "domain" as a precursor of the concept of possession and property right in fractal dimension.

Sommario

1. Prolegomeni della relazione: il perché del suo titolo. – 2. Alla ricerca della fenomenologia giuridica rilevante nel settore osservato: tra spazio e tempo nel Diritto. – 3. La tecnologia nello spazio digitale come fenomeno giuridico rientrante nella categoria giuridica dell'oggetto. – 4. *Segue*. Lo spazio digitale come oggetto di diritto tra cosa e bene. – 5. Intuizione di un nuovo possibile paradigma del "dominio" in teoria generale.

Keywords: Tecnologia, Spazio digitale, Oggetto giuridico, Cosa/bene, Dominio

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio anonimo, in quanto riproduce la relazione presentata dall'A. al convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno" (Messina, 26-27 maggio 2017).

1. Prolegomeni della relazione: il perché del suo titolo

Gli organizzatori del convegno, essendo carissimi amici, mi hanno invitato, si sono fidati e si aspettano che non deluda l'uditorio. E, in questa direzione per prima cosa mi tocca spiegare il titolo che ho scelto per questo intervento e soprattutto il punto interrogativo (oggetto di specifica e reiterata richiesta di conferma).

Il titolo del convegno è «Nuove tecnologie e diritti umani»; seguono due punti con la esplicitazione di una specie di sotto scansione, «profili di diritto internazionale e di diritto interno», indicativa di direttive capaci di tenere unite le tre sezioni in cui si articola l'incontro e di cui l'ultima si manifesta come indagine su aspetti consoni a specifiche tipologie di settori giuridici (diritto penale, diritto costituzionale).

Nelle tre sezioni, il tema delle tecnologie è analizzato tenendo presenti molteplici prospettive. In alcune di queste direzioni prospettiche, con certezza risulta esplicita la scelta del punto di osservazione e del relativo orizzonte di analisi della fenomenologia legata alla tecnologia: protezione, tutela, difesa dei diritti umani e/o diritti fondamentali, con un'area dimensionale che degrada nel contenuto semantico di alcuni interventi sino al significato di rispetto. Dunque, prospettiva di confinamento di una realtà invadente (la Tecnologia).

In altre, il punto di osservazione sembra cambiare: la nuova tecnologia viene ad essere assunta come mezzo di realizzazione dei diritti umani o addirittura spazio di emersione di nuovi diritti. Dunque, in direzione diametralmente opposta all'altra.

In fondo, proprio in questa dicotomica dimensione, però, si manifesta la realtà collegata ai fondamenti teorici e dogmatici dei diritti fondamentali svolti nella dimensione giuridica contemporanea, per come evidenziata rispetto alle Carte Costituzionali vigenti da autorevoli Maestri del Diritto Civile[1] nelle cui analisi si rileva la dinamica collegata ai divieti di ingerenza, ai diritti di difesa, ai precetti di tutela che preludono ai c.d. diritti nativi (tra cui lo stesso diritto di accesso ad Internet)[2].

Con l'avvento della tecnologia digitale si assiste ad un sovraccarico cognitivo, anch'esso recentemente indagato con attenzione[3]: si rende manifesta la facilità dell'accesso al conoscere, ma si evidenzia nel suo eccesso di possibilità l'esigenza di forme di garanzia contro la falsa conoscenza o la notizia non vera o *alt-truth* (verità alternativa, come la chiamano in America) sino alla dialettica che innesca il tensore assiologico del c.d. diritto all'oblio rispetto al diritto di cronaca o alla conoscenza[4].

Tutti aspetti che hanno causato il proliferare di convegni di settore, specialmente in quest'ultimo anno in cui ricorre il trentennale del primo collegamento italiano a internet e si è analizzato con attenzione il Regolamento UE 679/2016 sulla protezione dei dati che si applicherà nel 2018; proprio in relazione al regolamento, i primi commentatori[5] evidenziano la distinzione – sia pure forse non pienamente realizzata – tra

[1] C.W. Canaris, *L'incidenza dei diritti fondamentali sul diritto privato tedesco*, in *Studium iuris*, 1999, 359 ss.

[2] Su cui A. Busacca, *Il diritto di accesso alla rete internet*, in *Rivista OIDU*, 3, 2017, 345 ss.

[3] D. Weinberger, *La stanza intelligente. La conoscenza come proprietà della rete*, Torino, 2017.

[4] Su cui M. Rizzuti, *Il diritto e l'oblio*, in *Il corriere giuridico*, 2016, 1077 ss.

[5] G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le nuove leggi civili commentate*, 1, 2017, 1 ss.

riservatezza e diritto alla protezione dei dati, introducendo così la libertà positiva del controllo del soggetto sulla sua stessa identità riflessa nel digitale (su cui altri parlerà).
Ma se guardo al Regolamento UE con i suoi 173 considerando, gli XI Capi divisi in Sezioni, per complessivi 99 articoli, quasi tutti complessi per la presenza stocastica di regole ed eccezioni, con intarsio sistematico variabile anche semplicemente alterando la sequenza progressiva di lettura, si potrà anche ritenere che sia tutto orientato a tentare di «creare un clima di fiducia per lo sviluppo economico negli ambienti *on line*»[6], ma certo io mi sento più di concordare con quanto da altri osservato: «La lettura complessiva del Regolamento non è agevole, né entusiasmante …..produce il risultato che è sotto gli occhi di tutti. Un codice europeo in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, fortemente specialistico (al punto da imporre il ricorso a vere e proprie nuove professionalità) e nel quale confluiscono norme a diverso livello di dettaglio»[7].
Tutto ciò rende quasi impossibile nella gente comune una conoscenza dei comportamenti dovuti prima del verificarsi dei fatti, impedendo quasi completamente la possibilità di un'attuazione spontanea del diritto in questo settore.
Occorre constatare che «di fatto, la coerenza sistematica non c'è, perché non c'è sistema. C'è soltanto un ammasso di regole disposte orizzontalmente, per così dire, non strutturate secondo la logica del generale, speciale, eccezionale»[8]; per cui il suggerimento più consono (se non addirittura percorso obbligato) è quello di utilizzare per l'ermeneutica del documento normativo la tipica logica del controllo computerizzato, la c.d. *fuzzy logic* (quella del bicchiere mezzo pieno e mezzo vuoto da gestire secondo quanti di maggiore o minore proporzionalità…).
Stante questo background, mi sono chiesto: possibile che in questa materia l'osservatore che voglia compiere una analisi scientifica non riesca a posizionarsi meglio rispetto alla globalità dei fenomeni? Posizionarsi in modo coerente, assumendo una dimensione più generale d'indagine, una posizione magari *pre-supposta* da cui partire, idonea ad osservare l'insieme e tale da poter far suggerire, non dico alla gente comune, ma a un comune giurista del nostro tempo, una strada per poter capire la normatività senza la necessità dello specialista, specializzando in eterno in tecnologia digitale?
È veramente possibile che non esista una via per venir fuori dalla pura dimensione normativa, quasi statistica, delle probabilità gestite tecnologicamente, collegate con il funzionamento della logica quasi paradossale e parossistica della proporzionalità contingente?
E se fossimo solo nella difficoltà dell'ovvio, tema cui ci ha introdotto, come giuristi, uno degli autorevoli rappresentanti della scuola di Messina[9]?
Mi sono così spinto a cercare una risposta, che però non so se esista: e ciò giustifica il punto interrogativo che ho voluto per il mio intervento.

---

[6] Così ancora G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., 6.

[7] M. Granieri, *Il trattamento di categorie particolari di dati personali nel REG. UE 2016/679*, in *Le nuove leggi civili commentate*, 1, 2017, 165-166.

[8] Sono ancora parole di M. Granieri, *Il trattamento di categorie particolari di dati personali nel REG. UE 2016/679*, cit.,188.

[9] D. Farias, *L'ermeneutica dell'ovvio, Studi sull'esplicitazione dei principi più evidenti*, Milano, 1990, vol I.

2. Alla ricerca della fenomenologia giuridica rilevante nel settore osservato: tra spazio e tempo nel Diritto

Alla ricerca di una risposta, in questo intervento si cercherà di realizzare brevemente un esperimento mentale[10]; si utilizzerà come punto di partenza la quadripartizione della fenomenologia giuridica proposta dalla scuola messinese[11], ritenendo peraltro di non poter fare altrimenti, sia perché questo Convegno si svolge all'Università di Messina[12], sia perché non credo esista una valida alternativa dogmatica (o almeno non è da me conosciuta) per procedere in coerenza scientifica nell'esperimento mentale.
Nella massima estensione semantica della nozione, parlando di "nuove tecnologie" a quale dimensione e categoria di fenomeno giuridico occorre rapportarsi: dimensione spaziale o dimensione temporale? Categoria del Soggetto o quella dell'Oggetto? Ovvero occorre riferirsi ai Fatti o ai Comportamenti?
Se si parlasse della Tecnologia come robotica[13] o della incidenza di essa sulla nascita o morte delle persone, bisognerebbe scegliere la categoria del Soggetto; ma certamente, pur essendo questi aspetti rilevanti, non riescono a coprire il tutto e soprattutto coprono un'area più di rilevanza etico-filosofica che giuridica, guardando al Soggetto *del* Diritto, più che al Soggetto *nel* Diritto (per come è possibile alla teoria generale[14]).
Se si parlasse della Tecnologia come nuovo mezzo delle relazioni umane, sarebbe d'uopo guardare alla categoria del comportamento, ma si tornerebbe nel bel mezzo del dilemma iniziale di quale sia il punto di osservazione (protezione o realizzazione) della fenomenologia rilevante, sia pure nella direzione del c.d. diritto di accesso alla Rifkin[15].
Forse potrebbe essere interessante guardare ai comportamenti di tutti i soggetti giuridici su internet come espressione di nuove tipologie di consuetudini globali, che inaugurano un nuovo *ius gentium* o anche solo una diversa *lex mercatoria*, ma certamente non è questa la sede per farlo né ne ho la competenza[16].
Trattandosi di Tecnologia (necessariamente attività umana[17]), la categoria del "Fatto in senso stretto" sarebbe certamente eccentrica, anche se i fenomeni potrebbero rilevare in sé come (fatti di) energia: questa energia sarebbe però sempre gestita e solo tale

[10] Un *Gedankenexperiment* su cui v. M. Burroni, *Esperimento e esperimento mentale*, Milano, 2004.

[11] A. Falzea, *Ricerche di teoria generale del diritto e di dogmatica giuridica. Vol. II. Dogmatica giuridica*, Milano, 1997.

[12] Peraltro esperimento proposto sulla suggestione di un pensiero del compianto prof. Domenico Farias.

[13] Relativa anche semplicemente ai droni o seguendo la suggestione di G. Teubiner in una *lectio magistralis* a Verona del 18 maggio 2017 su *Agenti elettronici e grandi scimmie*.

[14] Che incontra il limite degli assiomi non dimostrabili alla Gòdel: v. A. Gorassini, *Lezioni di biodiritto*, Torino, 2007.

[15] J. Rifkin, *L'era dell'accesso*, Milano, 2000.

[16] Qui rileverebbe il problema della confinazione del c.d. diritto all'oblio rispetto al diritto all'informazione tra identità, correttezza e proporzionalità, su cui v. R. Senigaglia, *Regolamento UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Le nuove leggi civili commentate*, 5, 2017, 1023 ss.

[17] Nel portato dell'etimologia greca indica un trattato sistematico anche se il termine sembra ormai limitato ad indicare una applicazione tecnica multidisciplinare: *Vocabolario lingua italiana, Enciclopedia Treccani*, Roma, 1994, 756.

gestione porterebbe alla obsolescenza programmata delle cose virtuali (diventando rilevante solo in questa direzione e riportandoci verso i comportamenti).
Ma questa osservazione eccentrica, indirizza, pur se in deviazione riflessa, verso la categoria dell'Oggetto (peraltro l'ultima rimasta). Ed è proprio questa, allora, che sembra forse quella idonea a fissare il punto di partenza dell'esperimento mentale che si vorrebbe tentare in questa sede: la categoria spaziale dell'oggetto nella sua dicotomica alternativa essenziale propria della dimensione giuridica del bene e/o del danno[18].
Il prof. A. Falzea, in un suo intervento del 2001[19], ponendo la tecnologia tra scienza e tecnica con la caratterizzazione consequenziale a questa appartenenza verso le regole generali di settore (libertà e responsabilità), aveva evidenziato la generalità della dimensione spaziale di questi fenomeni conseguente al fenomeno della globalizzazione, con l'indebolimento inevitabile della posizione dell'individuo tale da rendere indispensabile l'accelerazione delle comunicazioni per bilanciare l'allargamento dello spazio. Scriveva che «secondo una legge antropologica ineluttabile, quanto maggiore è l'ambito spaziale in cui l'uomo si trova ad operare, altrettanto maggiori sono le difficoltà della sua esistenza e le misure protettive di cui ha bisogno per fronteggiarle»[20].
Ciò sembra conforti la scelta della dimensione spaziale e in particolare della categoria dell'oggetto come punto di osservazione.

3. La tecnologia nello spazio digitale come fenomeno giuridico rientrante nella categoria giuridica dell'oggetto

Qual è la fenomenologia racchiusa nel sintagma "nuove tecnologie" percepibile nella sua più generale estensione dalla prospettiva dell'oggetto che appartiene ai fenomeni spaziali?
Assumiamo in questa direzione come prospettiva d'osservazione dei fenomeni lo spazio c.d. digitale. Può considerarsi l'intero "spazio" dei fenomeni digitali come "cosa"?
Qui inizia il vero esperimento mentale che propongo in questa sede e che spero giustifichi scientificamente (anche solo per renderla eventualmente falsificabile) la relazione ed il suo titolo.

[18] Del resto, M. Granieri, *Il trattamento di categorie particolari di dati personali nel REG. UE 2016/679*, cit., 185 s. ha rilevato in relazione al nuovo regolamento che i dati personali «come beni-oggetto esistono già in natura con gli individui ai quali appartengono…». Per cui «Purché legittimamente raccolto, il dato personale può confluire in un insieme strutturato, che nel suo complesso forma oggetto di un diritto di proprietà sui generis di diverso titolare, rappresentato da colui che si fa carico degli investimenti per la costituzione dell'insieme dei dati». Tutto ciò sembrerebbe essere rilevante per un conflitto tra il diritto del costitutore e quello del titolare del dato. Ma è anche quanto osservato da F. Mezzanotte, *L'appartenenza come tecnica di regolazione (a proposito di Regulatory Property Rights*), in *Rivista critica del diritto privato*, 2016, 635 ss. discettando in relazione ad una raccolta di scritti curata da C. Godt e considerando l'appartenenza come tecnica di regolazione che troverebbe il suo centro gravitazionale nei principi immanenti dell'ordinamento comunitario (e che prelude alle *new properties* ben oltre il modello reichiano classico di utilità reificate che rileverebbero anche come beni comuni).

[19] A. Falzea, *Nuove tecnologie e diritto*, in Id., *Ricerche di teoria generale del diritto e di dogmatica giuridica. Vol. III. Scritti d'occasione*, Milano, 2010, 267 ss.

[20] *Ibidem*, 276.

Cosa si intende per spazio? Cosa si intende per digitale?
Il sintagma "spazio digitale", spesso utilizzato, riferisce una mappa senza confini, in continua mutazione, senza regole, che procede a folle velocità: la semantica non è ancora consolidata. Spesso si usa il termine piattaforma, che in informatica indica una base software e/o hardware su cui sono sviluppate e/o eseguite applicazioni.
Con qualche approssimazione possiamo assumere come "spazio digitale" lo spazio in cui si manifesta il fenomeno Internet.
Di "spazio", in un qualsiasi vocabolario, troviamo almeno otto diversi significati[21]: di essi almeno tre sembrano rilevanti in questa sede.
a) spazio, in termini filosofici, è inteso come entità intuitivamente collegata ai concetti di estensione e di posizione dei corpi che vi sono collocati, così come vengono percepiti e che porta, nel linguaggio corrente, a luogo di estensione a due o tre dimensioni in cui si collocano gli oggetti e le persone (da cui poi nel diritto deriva ad es. il concetto di spazio pubblico). Ma anche luogo come struttura dotata di precise proprietà, come ad es. in matematica il c.d. spazio vettoriale o nel diritto il c.d. mercato.
b) spazio inteso come ambiente, il luogo entro il quale si trovano anche i corpi celesti (da cui poi in diritto deriva ad es. spazio aereo, parte dell'atmosfera definita dal prolungamento verticale dei confini di uno stato e che è soggetta alla sua sovranità).
c) spazio come estensione in senso temporale (da cui l'espressione "un breve spazio di tempo"), in musica ciascuno dei quattro intervalli compresi tra le cinque righe del pentagramma, ma in questo significato si spinge sino al figurativo ambito di influenza, campo d'azione (ad es. spazio politico, culturale, giuridico).
Torniamo all'esperimento. Lo spazio in cui si manifesta internet è senz'altro anche e soprattutto un luogo fisico (secondo la prima accezione): basta digitare su un motore di ricerca "*submarine cable-map*" per trovare i planisferi che individuano il complesso delle linee fisiche globali di cavi in fibra ottica interconnessi che si incrociano e intrecciano tra loro; e in cui centrale è il ruolo dei nodi, luoghi fisici, in genere vicini alle coste oceaniche, dove si collegano le reti internet del mondo (*rete*, termine che assume così il suo significato materiale originario). Sono solo queste migliaia di chilometri di cavi che rendono possibile il c.d. spazio digitale.
Come da altri osservato[22]: «È un planisfero *open source* costantemente aggiornato che monitora e traccia i cavi sottomarini, cavi lunghi 4,6, 12 mila chilometri entro cui la luce corre veloce da una *landing station* all'altra […] Analogo sviluppo delle tecnologie sulla terraferma, dove le dorsali si stanno moltiplicando a vista d'occhio».
La fisicità del c.d. spazio digitale la possiamo percepire del resto più direttamente solo se pensiamo alle applicazioni della domotica che utilizziamo a casa nostra, per garantire con gli impianti sicurezza, confort, risparmio sino agli estremi della gestione intelligente degli elettrodomestici magari con un controllo integrato da remoto, che guarda caso spesso avviene attraverso una applicazione della *fuzzy logic*. Ma tutto ciò presuppone una rete materiali di cavi o di cose con funzioni wireless.

[21] *Vocabolario lingua italiana, Enciclopedia Treccani*, Roma, 1994, 476 ss.

[22] Come osservato da M. Del Barba, *Migliaia di chilometri di cavi. È' l'internet (invisibile) da toccare*, in *Corriere Innovazione*, 6 aprile 2017, 8.

Altri ha già evidenziato[23] come le iperconnessioni hanno fatto nascere una iper-nazione i cui confini sono innanzitutto commerciali, ma anche fisici vista la penetrazione della fibra ottica sin dentro le case delle famiglie - almeno dell'unione europea.
E a cui deve aggiungersi la connessione degli oggetti attraverso i satelliti, sia da casa che da fuori.
L'intera infrastruttura che garantisce la connettività a Internet via satellite si basa, infatti, su tre elementi, tutti materiali: il satellite (ovviamente); le stazioni terrestri chiamate NOC (acronimo di Network Operations Center), una specie di grosso *router* il cui compito è collegare l'infrastruttura spaziale a Internet; la parabola e un modem ad essa collegato, necessari per catturare le onde inviate dal satellite e tramutarle in informazioni digitali. Sempre realtà fisica presupposta rispetto al collegamento dei soggetti.
Certamente, dunque, c'è uno spazio fisico nel quale viaggiano algoritmi di bit; ma come qualificare i bit fisicamente dentro questo spazio? Sono "cose"?
Da privatista cultore del diritto interno, sarei portato a dire con una qualche certezza che si tratta di beni: anche se fossero solo espressione di energia, in Italia esiste l'art. 814 c.c. («si considerano beni mobili le energie naturali che hanno valore economico»); e anche se si potessero avere dubbi sulla naturalità dell'energia dei bit, essendo essi senz'altro possibile oggetto di diritti, sarei comunque coperto dal portato normativo dell'ultimo inciso dell'art. 813 c.c. («le disposizioni concernenti i beni mobili si applicano a tutti gli altri diritti»).
Ma, vista la sede dell'intervento, in un convegno anche di diritto internazionale, una tale constatazione non basta (anche perché questa relazione non si colloca nella terza sezione, quella dei profili interni).
Assunto il livello di teoria generale del fenomeno che si sta cercando di indagare, occorre proseguire l'esperimento mentale sforzandosi di trovare una soluzione più consona a ogni settore di giuridicità.
L'energia che attraversa la rete fisica costituita dalla fibra ottica o dalle onde elettromagnetiche satellitari può trasformarsi in cosa, intendendola come comunemente viene percepita questa realtà in ogni settore?
Sperimentalmente in questo tempo, da giuristi abbiamo un indice di emersione fattuale per dire di sì: il *bitcoin* e la possibilità dei *blockchain* con cui si realizzano i c.d. *smart contract*, realtà su cui non posso in questa sede soffermarmi e su cui rinvio alle riflessioni svolte di recente da altri[24].
In questi fenomeni, l'energia crea nella dimensione spaziale digitale una realtà che diventa moneta, ma con materialità finita incorporata in quello spazio, secondo quanto programmato dalla enigmatica figura di Satoshi Nakamoto. Tutto è reale almeno come la moneta e il valore incorporato nella moneta che conosciamo e utilizziamo nello spazio reale, e di cui come oggetto mi sono occupato in altra sede, quella delle obbli-

[23] C. Seganfreddo, *Dieci miliardi di like ogni giorno della vita*, in *Corriere Innovazione*, cit., 22 s.

[24] Cfr. P. Cuccuru, *Blockchain da automazione contrattuale. Riflessioni sugli smart contract*, in *La Nuova giurisprudenza civile commentata,* 1, 2017, 107 ss. Ma lo stesso può farsi sulla piattaforma *Ethereum* che garantisce la stipula di accordi che prescindono da ogni competenza legislativa di ogni Paese e sono interamente gestiti secondo gli accordi raggiunti in rete e impossibili da modificare anche nella esecuzione.

gazioni pecuniarie, e alla quale in questa sede rinvio[25].
L'assunto sperimentale sembra avvalorato - pur non avendo approfondito - dalla evoluzione del modo di essere dei dati granulari sul rischio del credito di cui al regolamento UE 2016/867 della Banca Centrale Europea[26]. Ma anche i Big Data come tracce delle informazioni personali rilasciate nell'ambiente mediante l'uso di tecnologie informatiche, di cui ha trattato in un recente parere il Comitato nazionale di Bioetica[27].
E questa osservazione mi permette velocemente di generalizzare.
"Velocemente": l'avverbio o l'aggettivo con funzione avverbiale mi riporta a quella fenomenologia rilevante collegata con i comportamenti che abbiamo messo tra parentesi, pur riconoscendone l'appartenenza alla realtà indagata.
La mediazione delle nuove tecnologie ha permesso una globalizzazione delle relazioni umane prima inimmaginabile: ha permesso l'incontro di soggetti/persone alterando il luogo dell'incontro stesso; l'incontro avviene in un *luogo nuovo* creato dalla tecnologia che annulla le distanze reali e velocizza il tempo della possibile relazione facendo diminuire lo spazio da percorrere: i possibili contatti aumentano in modo esponenziale, sono accelerati, secondo la previsione di A. Falzea…
Avvengono sempre più *velocemente*!!

4. *Segue*. Lo spazio digitale come oggetto di diritto tra cosa e bene

Ancora questo termine: *velocemente*; che però come radice di sostantivo ci porta direttamente alla scienza fisica e alla famosa formula di Einstein $E = mc^2$, nella sua versione originaria[28].
Ma arrivati alla fisica come scienza, da qui in poi l'esperimento mentale dovrebbe diventare anche metodo di prova scientifica, ma non ho la competenza e pur impegnandomi non ho avuto neppure il tempo per approfondire, neppure cavalcando l'onda di luce nell'esperimento mentale di Einstein sulla relatività…[29]
Ma come posso e come so, in questa sede cercherò di dire qualcosa utilizzando un libro divulgativo di un fisico di Berkeley[30], mettendo in evidenza una realtà fenomenica: la relatività del tempo è facilmente sperimentabile per un fisico sperimentale, attraverso il rilevamento dell'emivita di un pione, 26 nanosecondi, che potrebbe apparire troppo breve, ma in quei 26 nanosecondi il mio iPhone può eseguire 36 operazioni elementari; per un non fisico è ancor più facile pensare alla dilatazione del tempo che ha rilevanza

[25] A. Gorassini - R. Siclari, *Di alcune specie di obbligazioni*, in *Trattato di diritto civile del Consiglio nazionale del notariato* diretto da P. Perlingieri, Napoli, 2013, vol. III, 14, 13 ss.

[26] Sul concetto v. M. Zani, *Granularità: un percorso di analisi*, in *Digitalia*, 2, 2006, 60 ss.

[27] CNB, *Tecnologie dell'informazione e della comunicazione e Big Data: profili bioetici*, 25 novembre 2016.

[28] Non nella più simpatica mutazione semantica suggerita dagli studenti universitari come formula universale dell'esame universitario perfetto, che credo tutti voi credo conosciate: Esame = memoria + capacità al quadrato !!!

[29] Per un divertente anche se rigoroso approccio alla tematica v. H. Nitta, M. Yacamamoto, K. Takatsu, *Relatività*, in *I manga della scienza*, Roma, 2016.

[30] R. A. Muller, *Adesso. La nuova fisica del tempo*, Milano, 2016.

sullo spazio, considerando la velocità orbitale dei satelliti GPS che è di 4Km al secondo e rallenta il tempo di 7200 nanosecondi al giorno e di cui il sistema di localizzazione sempre utilizzato dal mio iPhone tiene conto per determinare la mia posizione sulla terra, perché altrimenti le onde radio (che viaggiano a circa un terzo di metro al nanosecondo) ignorando i 7200 nanosecondi di dilatazione del tempo, calcolerebbero erroneamente la posizione GPS con una deformazione di oltre 2 Km, con le conseguenze facilmente immaginabili[31], per me e anche per voi se e quando utilizzate il GPS.

Questo però significa che la formula della covarianza relativistica di Einstein funziona anche in periodi discreti; anche la gravità ha effetti sul tempo; ma per il principio di equivalenza, il tempo ha incidenza discreta sullo spazio[32].

Lo spazio non è più entità semplice pre-supposta: si può espandere e contrarre. E lo spazio può anche crescere e comunque cresce nel tempo per la c.d. inflazione dell'Universo: come all'inizio del tempo le particelle acquisirono massa, anche adesso acquisiscono massa attraverso il c.d. meccanismo di Higgs (la famosa particella di Dio, di cui di recente si è avuta la prova).

E, sia che il flusso temporale sia guidato dall'entropia e dalla sua legge (secondo la teoria standard), sia che sia conseguenza nella teoria quantistica dell'ampiezza della funzione d'onda per effetto dell'*entanglement* (non spiegato ancora se non con il principio di indeterminazione di Heisenberg, ma che ha qualcosa di mistico che porta alla sovrapposizione del gatto sia vivo che morto di Schrődingher[33] considerata assurda da Einstein ma che è comunque vera, perché quei risultati della fisica quantistica «vengono oggi usati per progettare l'elettronica che fa funzionare gli smartphone, i tablet, i computer»[34]) si crea spazio. E la tecnologia applicata sta portando nel gergo informatico al quantum bit o "qubit", per aumentare spazio e velocizzare il tempo delle operazioni senza generare calore nel sistema se non alla fine (in un normale computer, ogni volta che un bit passa da 0 a 1 o viceversa si genera un minimo di calore e il calore incide sulla deformazione dello spazio/tempo).

Adesso però il discorso è diventato troppo tecnico e complesso, ma possiamo ritenere sufficientemente certo un dato: ormai tutti i fisici sono convinti che nell'Universo vi sia una continua espansione e creazione dello spazio/tempo.

Nella realtà umana della fenomenologia attenzionata in questa sede, la tecnologia oltre che occupare spazio ne crea, scaricando altrove l'entropia della sua creazione, in gran parte delocalizzandola nello spazio siderale, realtà possibile proprio per una sovrapposizione di stati dell'energia.

Dunque, questa realtà giuridica rilevante, guardata dalla prospettiva dell'oggetto indicata dall'esperimento mentale seguito in questa sede risulta complessa (e mi torna in mente la complessità indagata dal prof. Falzea in uno dei suoi scritti[35]).

---

[31] R. A. Muller, *Adesso. La nuova fisica del tempo*, cit., 41.

[32] C. Rovelli, *L'ordine del tempo*, Torino, 2017.

[33] Per una interpretazione semplificata v. J. Baker, *Il gatto di Schròdinger*, in *50 grandi idee di Fisica*, Bari, 2011, 122 ss.

[34] R.A. Muller, *Adesso. La nuova fisica del tempo*, cit., 256.

[35] A. Falzea, *Complessità giuridica*, in Id., *Ricerche di teoria generale del diritto e di dogmatica giuridica. Vol. III. Scritti d'occasione*, cit., 595 ss.

5. Intuizione di un nuovo possibile paradigma del "dominio" in teoria generale

Ma cerchiamo di tirare per quanto possibile le somme del presente esperimento mentale sulla Tecnologia come oggetto nel Diritto.
Se guardo lo spazio occupato nel mondo reale conosciuto e percepito, dal punto di vista della fenomenologia giuridica ho un bene transnazionale sostanzialmente immobile (nodi, reti e quant'altro perché incorporati al suolo) da qualificare.
Se guardo alla potenza e contenuto temporale, anche sotto il profilo del calore, del bit, trovo la struttura un bene mobile posto tra energia e cosa che incorpora valore, da definire per l'appropriazione.
Se guardo alla dimensione unitaria spazio/tempo, l'entropia creata dalla tecnologia (ma essa stessa per la funzione d'onda e il suo collassare) diventa spazio siderale (anche se ancora non è chiaro se nella dimensione di vero e proprio danno/rifiuto, conseguenza dell'entropia causata dall'attività dell'uomo); comunque, certo, per definire in questa direzione lo sfondo del suo regime giuridico occorre guardare ai trattati che pongono i principi sull'esplorazione e l'uso dei corpi esterni alla Terra, che per quanto ne so sono stati tendenzialmente elaborati tra il 1966 e il 1979.
Forse, dal punto di vista della teoria generale, si potrebbe e dovrebbe ragionare attraverso la elaborazione di un sistema frattale multilivello che riposizioni alla luce del post-moderno la teoria giuridica dell'oggetto: ma non è questa la sede per farlo.
Si può solo in accenno evidenziare come il sistema ha la necessità di riqualificare il concetto giuridico di "dominio" proprio partendo o comunque tenendo conto nella sua ri-elaborazione della peculiarità di esso nella realtà spazio/temporale di Internet; e da esso verificare e riposizionare la situazione di fatto che identifica il possesso.
Certo operazione non facile, ma non certo impossibile ricordando che la sovrapposizione di situazioni giuridiche proprietarie non è una novità nel diritto: le cose mobili sono sempre esistite su terreni beni immobili; i territori degli Stati si stagliano nella realtà geo-fisica globale (chiamata Ambiente) e si sovrappongono ai territori delle regioni, dei comuni e dei privati (evidenziando un sistema frattale le cui potenzialità attuative del valore della sussidiarietà sono ancora in gran parte non utilizzate o anche solo esplorate). E, del resto, nel tempo della evoluzione del pensiero giuridico i beni sono divenuti essenzialmente proiezioni di utilità di cose; e in genere gli oggetti dei diritti non sono che proiezioni di beni nei rapporti anche c.d. pubblici…[36]
Del resto, negli aspetti di limite e confinamento, molte di queste cose tecnologiche possono essere incorporate e divenire inerenti il Soggetto (come ad es. accade nella c.d. medicina potenziativa, ma lo stesso può valere per alcune manifestazioni di PMA). E con ciò si evidenzia il problema generale di dove finisce l'oggetto come categoria logica

[36] Dal bene immobile si può distinguere ogni cosa che richieda un suo "spazio" e si distacchi, anche solo geo-politicamente (Stati, regioni, Città …): necessaria è solo la presenza di un soggetto alternativo di riferimento: e se nessun soggetto nel mondo del diritto esiste, esiste almeno la Stato come soggetto d'appartenenza. Certo, forse accorrerebbe rimeditare in questa chiave i concetti di sussidiarietà verticale e/o orizzontale per come elaborati dalla pubblicistica e rivalutare l'obbligo di solidarietà di cui all'art. 2 Cost. (anche nella logica della c.d. trasparenza amministrativa della PA) come formante necessitato della giuridicità d'origine (assioma di sistema, spesso dimenticato).

e di dove inizia il soggetto: il vecchio problema della qualificazione delle parti del corpo umano sembra riproporsi per i dati digitali che definiscono l'identità ….

In realtà, occorrerebbe preliminarmente definire lo spazio di rilevanza della persona come Soggetto del Diritto: e questo come detto appartiene a un altro livello di analisi (necessariamente meta-giuridica).

In modalità di narrazione di fatti, si pensi che il Soggetto produce comunque informazione che vale come Bene o come Rifiuto nel mondo spaziale in cui si svolge la sua vita; ma se è Bene, è possibile che l'Altro tragga beneficio dal suo sfruttamento come cosa, non sempre riproducibile (si pensi alla divulgazione del segreto), venendosi a creare così un momento di conflitto da gestire mediante il diritto. Ma nella complessità delle informazioni prodotte da tutti i Soggetti nello spazio del mondo digitale, si rende evanescente la parte che è riconducibile in appartenenza all'Essere da quella che si colloca nel Tempo in dimensione dell'Avere (perché spesso le mie stesse informazioni personali le uso come cose esposte al mondo) e la ricerca di una differenziazione esasperata di piani porta all'indifferenziazione di una realtà globale non gestibile se non informaticamente come cosa nello spazio digitale.

Nel Diritto ci troviamo in una dimensione frattale che ormai da molto tempo crea complessità, ma che presenta, proprio per queste sue caratteristiche, semplicità di possibili strutture invarianti e semplificanti, evidenziate senza grosse contraddizioni fin quando i giuristi si sono impegnati a costruire categorie e figure dogmatiche.

Comunque l'esperimento mentale almeno in questa sede si chiude qui, e sembra suggerisca per il diritto digitale un nuovo paradigma che possa ancora ricondurre alla scienza giuridica, certo scienza pratica come è il Diritto predicato in questa terra da Salvatore Pugliatti, ma purché resti realtà praticamente predicabile in dimensione dogmatica e di sistema, magari chiedendo aiuto anche ad altre scienze.

Certo – magari – senza arrivare agli eccessi di voler applicare la formula dell'equazione dell'interpretazione perfetta attraverso un vero e proprio sistema di disequazioni per arrivare alla prevedibilità dell'esito giudiziale, come pur suggerito da alcuni studi di avanguardia, recentemente presentati presso la Camera dei Deputati[37]; queste metodiche sarebbero capaci di far predire la convenienza o meno di una azione giudiziaria civile rispetto alla attuale alta imprevedibilità dei giudizi strettamente dipendenti da un bilanciamento *ex post* dei fatti e valori da parte dei giudicanti, e che forse peraltro sarebbe l'ultima estrema possibilità per una anomala attuazione spontanea del diritto altrimenti neppure più immaginabile, anche se con evidente deformazione del concetto di Giustizia ….

Ma non solo il tempo dell'esperimento è finito, è finito anche il tempo di questo intervento[38], proiettato verso un futuro in cui spero esistano ancora dogmatica e Diritto non solo nella c.d. realtà virtuale.

[37] G. Spina, *Prevedibilità dell'esito giudiziale con sistemi matematici: primi spunti operativi*, in *La nuova procedura civile*, 3, 2017.

[38] E prima che l'uditorio inizi ad auspicarsi la presenza nell'Universo come singolarità di un anti-Gorassini che faccia annichilare il relatore per *entenglament* chiudo questo intervento.

Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*

Giandonato Caggiano

Abstract

La conservazione e l'accesso ai dati di traffico delle comunicazioni da parte delle autorità pubbliche è un ambito di complesso bilanciamento tra diritti fondamentali: esigenze di sicurezza da un lato si contemperano con quelle di riservatezza e correttezza del trattamento dei dati, in un contesto di flussi informativi che travalica molto spesso i confini della sovranità nazionale. Il contributo della giurisprudenza, anche sovranazionale, alla definizione del corretto bilanciamento si dimostra come essenziale alla individuazione del corretto bilanciamento, specie di fronte alle esitazioni del legislatore europeo ad armonizzare la materia della *data retention* e alle difficoltà ad applicarla negli scambi con paesi terzi.

Data retention requires balancing a variety of fundamental rights. While States, one one hand, aim at protecting national security, on the other one, public authorities must respect privacy and ensure fairness of data processing, often across national jurisdictions. Courts, especially at the EU level, have a prominent role in balancing the different perspectives and rights at stake, given the reluctance to harmonize the matter of data retention by EU legislation and to apply it to third countries.

Sommario

1. Introduzione. - 2. La conservazione dei dati delle comunicazioni elettroniche e i rischi di sorveglianza di massa. - 3. Le sentenze *Digital Rights* e *Google* sul bilanciamento tra diritti fondamentali e sicurezza. - 4. La sentenza *Schrems* e l'invalidità della dichiarazione di adeguatezza della Commissione. - 5. L'interpretazione conforme alla Carta delle legislazioni nazionali nella sentenza *Tele2/Watson*. - 6. La proposta della Commissione di direttiva *e-privacy* che rinuncia all'armonizzazione legislativa in materia e rinvia ai principi generali del Regolamento generale sulla protezione dei dati. - 7. La legge comunitaria 2017 prolunga il termine di conservazione dei dati.

Keyword: Data retention, Conservazione dati, Privacy, Dati personali, Sorveglianza

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio anonimo, in quanto riproduce la relazione presentata dall'A. al convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno" (Messina, 26-27 maggio 2017).

1. Introduzione

La conservazione e l'accesso delle autorità pubbliche per finalità di sicurezza ai dati di traffico delle comunicazioni (d'ora in poi: *data retention*) si segnalano tra gli aspetti più controversi della tutela multilivello dei diritti fondamentali, sottoposta a crescenti esigenze di bilanciamento con le finalità di sicurezza nel settore della prevenzione e contrasto del terrorismo.

La materia della *data retention* appare particolarmente emblematica della complessità di interazione tra giudici e legislatore sia nell'Unione che negli Stati-membri. Proprio in questo ambito, la Corte di giustizia dimostra di voler consolidare la propria funzione costituzionale nell'ordinamento dell'Unione[1] e le corti costituzionali di vari Stati membri intervengono sulle legislazioni nazionali[2] mentre il legislatore europeo esita ancora ad adottare una nuova normativa europea di armonizzazione dopo la dichiarazione di invalidità della precedente[3] e il legislatore italiano ha adottato una norma incompatibile con la Carta dei diritti fondamentali, così come interpretata dalla Corte di giustizia[4].

Un quadro ricco di spunti generali sull'evoluzione dell'ordinamento dell'Unione che cercheremo di svolgere nel presente lavoro.

2. La conservazione dei dati delle comunicazioni elettroniche e i rischi di sorveglianza di massa

Sino all'avvento delle comunicazioni digitali, un controllo generalizzato di massa era stato concepito solo da qualche governo dittatoriale[5]. L'ascolto e la visione degli individui in qualsiasi momento della vita sono invece una potenzialità attuale per effetto delle

[1] V. *infra*, paragrafi 3, 4 e 5.

[2] Non è possibile in questa sede occuparsi della prospettiva di diritto pubblico comparato, ma appare utile accennare all'entità della tutela costituzionale multilivello in materia. Particolarmente interessante la sentenza del Tribunale costituzionale tedesco (sentenza del 2 marzo 2010, n. 11 (1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08) che ha dichiarato l'illegittimità delle norme nazionali che prevedevano l'obbligo di conservazione dei dati per un periodo di sei mesi, in assenza di una richiesta originata da indagini preliminari. Secondo molti commentatori, l'argomentazione del Tribunale avrebbe ispirato la sentenza *Digital Rights Ireland* della Corte di giustizia. Già prima della sentenza della Corte di giustizia varie corti costituzionali avevano dichiarato incostituzionali le legislazioni nazionali di attuazione della direttiva *data retention* (Bulgaria, Romania, Repubblica ceca, Cipro), v. T. Konstadinides, *Destroying Democracy on the Ground of Defending It? The Data Retention Directive*, *the Surveillance State and Our Constitutional Ecosystem*, in *European law review*, 2011, 722 ss.

Dopo la sentenza della Corte di giustizia, altre corti costituzionali di vari Stati membri sono intervenute sulle leggi nazionali di conservazione dei dati (Austria, Slovenia, Romania, Slovacchia, Irlanda, Paesi Bassi e Bulgaria, Polonia) o sulle nuove leggi in materia (Belgio). Il quadro della situazione nei vari ordinamenti è descritta da N. Vainio, *Fundamental rights compliance and the politics of interpretation: Explaining Member State and court reactions to* Digital Rights Ireland, in T. Bräutigam - S. Miettinen (eds.), *Data Protection, Privacy and European Regulation in the Digital Age*, Helsinki, December 2016, 229 ss.

[3] V. *infra*, par. 6.

[4] V. *infra*, par. 7.

[5] Sul controllo di massa nella DDR realizzato con varie modalità, ivi comprese le tracce dei vestiti dei fuggitivi da lasciare al fiuto dei cani molecolari, basti richiamare il film *Le vite degli altri*, Regista Henckel von Donnersmarck, Germania, 2006. Tra gli autori di fantascienza, l'Oscar delle citazioni va a G. Orwell, *1984*, 1949 reperibile *on line* in inglese e nella traduzione italiana.

informazioni raccolte nei "centri informatici" dei *service provider* e delle piattaforme di servizi su internet OTT (dai social network ai motori di ricerca)[6]; nonché per il possibile uso di "virus infettanti" di computer e smartphone che li trasformano in strumenti di intercettazione ambientale[7].

Gli operatori privati, spesso localizzati fuori dall'Unione, entrano in contatto con un'enorme quantità di dati personali, che possono riguardare il contenuto oppure l'"involucro" (d'ora in poi: metadati) delle comunicazioni elettroniche[8].

La conoscenza/consapevolezza dell'esistenza di pratiche legali e illegali, in base alle quali possono essere registrati per anni i dati di persone che non sono sospettati di gravi reati, ha determinato una crescente richiesta di stringenti criteri di (ri)equilibrio tra diritti fondamentali e finalità di sicurezza.

Il fenomeno della registrazione dei dati digitali era però già regolamentato, come vedremo in seguito, sia a livello europeo che nazionale. In linea di principio, la registrazione del contenuto delle comunicazioni deve essere determinata *ex ante* su autorizzazione delle autorità giudiziarie. La registrazione e conservazione di metadati appaiono utili solo *ex-post*, quando subentrino ragioni investigative su una determinata persona, a determinate condizioni fissate dalla legge. In entrambe le fattispecie, la questione giuridica consiste nel bilanciamento degli interessi in gioco da parte del giudice e del legislatore a livello dell'Unione e degli Stati membri. Le due tipologie di dati sono sottoposte dal Trattato di Lisbona alla medesima base giuridica (art. 16 TFUE)[9], ma continuano ad essere oggetto di strumenti diversi di diritto derivato.

Nel settore delle comunicazioni, il riconoscimento della Carta dei diritti quale fonte di

[6] *Over-the-top* è la categoria di servizi di comunicazione di audio, video e altri media su Internet senza il coinvolgimento dell'operatore di rete nel controllo o distribuzione del contenuto (chat, come WhatsApp, Facebook Messenger, WeChat; chiamate in video o in audio, come Skype, Gmail, Viber; servizi di video-streaming, come Netflix, Amazon Prime, YouTube). I servizi sono forniti sotto forma di applicazioni che eseguono il servizio di accesso a Internet. Tali servizi sostituiscono sempre di più la tradizionale telefonia vocale, SMS e posta elettronica con servizi *online* funzionalmente equivalenti

[7] EP STUDY, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, PE 583.137, disponibile *online*.

[8] Nell'uso degli apparati telefonici fissi o mobili e/o su internet si generano tecnicamente i metadati delle comunicazioni, quali l'origine, la destinazione, la data, l'ora, la durata, la tipologia, gli apparati utilizzati, ecc. Per le comunicazione mobili, si registra l'ubicazione dell'utente tramite la scia delle cellule agganciate lungo il percorso. Così, la nostra "scia o impronta digitale" contiene una grande quantità di informazioni personali, gestibile tramite l'analisi e la profilazione automatizzata delle comunicazioni. Alla definizione di servizio di comunicazioni elettroniche, si aggiungono quelle di "servizi di comunicazione interpersonali", basate sul numero o indipendente dal numero, v. COM(2016) 590 final, 12 ottobre 2016, proposta di direttiva per l'istituzione di un Codice Europeo delle Comunicazioni Elettroniche del 12 ottobre 2016, art. 2.

[9] Per un'analisi, v. B. Cortese, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Il Diritto dell'Unione europea*, 2013, 313 ss.

diritto primario[10] ha prodotto importanti sviluppi giurisprudenziali che suggeriscono riflessioni generali sul consolidamento del ruolo costituzionale della Corte di giustizia. Oltre che il rispetto del "nucleo essenziale" del diritto alla *privacy* e alla tutela dei dati personali, la Carta impone i principi di necessità e proporzionalità. Il principio del primato e l'idoneità di disposizioni della Carta a produrre un effetto diretto determinano l'obbligo di disapplicare la normativa interna incompatibile.

In premessa, vale la pena di ricordare che le disposizioni contenute nella Carta si applicano a istituzioni, organi e organismi dell'Unione «nel rispetto del principio di sussidiarietà», come pure agli Stati membri «esclusivamente nell'attuazione del diritto dell'Unione» (art. 51, par. 1) «secondo le rispettive competenze e nel rispetto dei limiti delle competenze conferite all'Unione nei trattati»[11]. Tale criterio definisce l'ambito applicativo della Carta e delimita conseguentemente la competenza interpretativa della Corte. Anche nell'ordinamento dell'Unione, lo "stato di diritto" richiede una corretta dinamica tra giudice e legislatore. In questa sede ci interessa approfondire l'incidenza della Carta rispetto alle due varianti dell'interpretazione pregiudiziale di validità delle disposizioni del diritto derivato[12] e dell'interpretazione pregiudiziale delle fonti derivate e nazionali. Nell'interpretazione pregiudiziale di validità, il monopolio interpretativo spetta alla Corte di giustizia che può dichiarare anche la totale invalidità dell'atto sottoposto al suo giudizio, quando l'incompatibilità con il Trattato, e in particolare con la Carta, ne vizia la legittimità nel suo insieme. Nell'interpretazione pregiudiziale il dialogo tra giudice nazionale e Corte di giustizia si indirizza al giudizio *a quo* ma resta al legislatore nazionale eliminare la norma eventualmente giudicata incompatibile con il diritto

[10] Sul valore e sugli effetti della Carta, dopo l'entrata in vigore del Trattato di Lisbona, la bibliografia è molto ampia. Tra i tanti, G. Di Federico (ed.), *The EU Charter of Fundamental Rights, From Declaration to Binding Instrument*, Dordrecht, 2011; S.I. Sánchez, *The Court and the Charter: The impact of the entry into force of the Lisbon Treaty on the ECJ's approach to fundamental rights*, in *Common Market Law Review*, 2012, 1564 ss.; K. Lenaerts, *The Court's Outer and Inner Selves: Exploring the External and Internal Legitimacy of the European Court of Justice*, in M. Adams–H. De Waele–J. Meeusen–G. Straetmans, *Judging Europe's Judges. The Legitimacy of the Case Law of the European Court of Justice*, Oxford-Portland, 2013, 13 ss.; D. Sarmiento, *Who's Afraid of the Charter? The Court of Justice, National courts, and the new framework of fundamental rights protection in Europe*, in *Common Market Law Review*, 2013, 1267 ss.; K. Ł. Bojarski - D. Schindlauer - K. Wladasch, *The European Charter of Fundamental Rights as a Living Instrument*, Rome-Warsaw-Vienna, 2014; G. Palmisano (a cura di), *Making the Charter of Fundamental Rights a Living Instrument*, Leiden, 2014; K. Lenaerts–J.A. Gutiérrez-Fons, *The place of the Charter in the EU constitutional edifice*, in S. Peers–T. Hervey–J. Kenner–A. Ward (a cura di), *The EU Charter of fundamental Rights*, Oxford e Portland (OR) 2014, 1559 ss. ; S. de Vries - U. Bernitz - S. Weatherill (eds), *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old*, Oxford, 2015; P. Mori, *Autonomia e primato della Carta dei diritti fondamentali dell'Unione europea, in* G. Nesi - P. Gargiulo (a cura di), *Luigi Ferrari Bravo il diritto internazionale come professione*, Trento, 2015, 169 ss.; L.S. Rossi, *"Stesso valore giuridico dei Trattati"? Rango, primato ed effetti diretti della Carta dei diritti fondamentali dell'Unione europea*, in E. Falletti - V. Piccone (a cura di), *Il filo delle tutele nel dedalo d'Europa*, Napoli, 2016, 73 ss.; L. D'Andrea – G. Moschella – A. Ruggeri – A. Saitta (a cura di), *La Carta dei diritti dell'Unione Europea e le altre Carte (ascendenze culturali e mutue implicazioni)*, Torino, 2016.

[11] La Corte ha chiarito che «i diritti fondamentali garantiti nell'ordinamento giuridico dell'Unione si applicano in tutte le situazioni disciplinate dal diritto dell'Unione, ma non al di fuori di esse»: v. sentenza del 26 febbraio 2013, causa C-617/10, *Åklagaren/Hans Åkerberg Fransson*. Sull'obbligo di interpretazione del diritto interno in conformità alla Carta e ai principi generali da parte del giudice nazionale, v. P. Mori, *La "qualità" della legge e la clausola generale di limitazione dell'art. 52, par. 1, della Carta dei diritti fondamentali dell'UE*, in *Il diritto dell'Unione europea*, 2014, 243 ss.; R. Baratta, *Il telos dell'interpretazione conforme all'*acquis *dell'Unione*, in *Rivista di diritto internazionale*, 2015, 28 ss., e 41 ss.

[12] In materia, v. lo studio di A. Adinolfi, *L'accertamento in via pregiudiziale della validità di atti comunitari*, Milano, 1997. I principi della giurisprudenza in materia sono riportati nella *Nota informativa della Corte di giustizia*, *GUUE* C 160/2 28 maggio 2011, paragrafi 15, 16 e 17.

dell'Unione.

Il presente lavoro ha per oggetto gli sviluppi più recenti della giurisprudenza della Corte, che hanno rilanciato, tramite decisioni coraggiose e radicali, il processo costituzionale dell'Unione in una materia così sensibile per i diritti fondamentali. Nella nostra analisi ci limiteremo a richiamare gli aspetti istituzionali rilevanti delle sentenze *Digital Rights Ireland* e *Google Spain*, già adeguatamente approfondite in dottrina, per concentrarci invece sulle più recenti sentenze e sulla (in)attività del legislatore dell'Unione in materia[13].

Il presente contributo si concentra sulla tutela dei dati personali nelle comunicazioni elettroniche, escludendo la normativa del settore penale[14] e, pertanto, la direttiva 2017/541 sulla lotta contro il terrorismo. Vedremo però in seguito come il legislatore italiano abbia già richiamato tale direttiva per giustificare, in contrasto con le decisioni della Corte di giustizia, la conservazione generalizzata dei metadati delle comunicazioni per un periodo di sei anni[15].

Peraltro, non è possibile in questa sede occuparci di altre categorie di dati personali, quali il PRR dei viaggiatori aerei, i dati finanziari e fiscali e quelli delle agenzie dell'Unione. Così, esula dall'ambito di questo lavoro, l'approfondimento della giurisprudenza della Corte di Strasburgo[16]. Pur non sottovalutando l'importanza del suo contributo, occorre ricordare che, per la Corte di giustizia, «l'esame sulla validità delle disposizioni

[13] Una riflessione specifica sulle due sentenze in parola, come esempi di interpretazione di validità e interpretazione conforme, corredata di opportuni riferimenti ai precedenti giurisprudenziali, è svolta da F. Bestagno, *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali*, in *Diritto dell'Unione europea*, 2015, 21 ss. In un successivo articolo, lo stesso Autore (*I rapporti tra la Carta e le fonti secondarie di diritto dell'UE nella giurisprudenza della Corte di giustizia*, in *Diritti umani e diritto internazionale*, 2015) riflessioni ricostruttive che abbiamo tenuto in considerazione nel corso di questo scritto.

[14] A livello dell'ex-terzo pilastro, v. direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio**,** *GUUE* L 119, 4 maggio 2016, 89 ss. La conservazione dei dati su ordine giudiziario è uno strumento investigativo previsto e utilizzato dagli Stati firmatari della convenzione del Consiglio d'Europa sulla criminalità informatica, v. art. 16 della Convenzione sulla criminalità informatica - "Convention on Cybercrime" Budapest, 23 November 2001, ETS No.185.

[15] Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio, *GUUE* L 88, 31 marzo 2017, 6 ss., considerando 21.

[16] Per un'analisi della giurisprudenza della Corte di Strasburgo, v. *Opinion 1/2014 of the Article 29 Working Party on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 27 febbraio 2014. Successivamente, *Zakharov v. Russia*, ric. 47143/06 (2015); *Szabo and Vissy v. Hungary*, ric. 37138/14 (2016). Per un commento, v. L. Woods, *Zakharov v Russia: Mass Surveillance and the European Court of Human Rights*, in *EU Law Analysis*, 16 December 2015.
I limiti posti dagli articoli 8, par. 2 CEDU e 52, par. 1 Carta sono equivalenti: l'art. 8, par. 2 CEDU esplicita rispetto alla Carta che la limitazione deve essere «necessaria in una società democratica». La condizione dalla CEDU per giustificare la misura e la legittimità delle limitazioni sembra ulteriormente qualificabile con l'esistenza un «bisogno sociale imperioso», idoneo a mettere in crisi il funzionamento stesso della società. Sul dialogo tra le corti sovranazionali europee, v. M. D. Cole - A. Vandendriessche, *From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabb/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance*, in *Eur. Data Prot. L. Rev.*, 2, 2016, 127 ss.; A. Terrasi, *Il rapporto tra diritto alla privacy e protezione dei dati personali tra Corte di giustizia dell'Unione europea e Corte europea dei diritti dell'uomo*, in M. Distefano (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, 2017, 127 ss.

legislative devono essere effettuate alla sola luce della Carta»[17].

3. Le sentenze *Digital Rights* e *Google* sul bilanciamento tra diritti fondamentali e sicurezza

Nel 1990 Internet non esisteva ancora quando la Commissione propose il primo testo sulla tutela dei dati personali[18], adottato come direttiva 95/46 (in vigore sino al maggio 2018)[19]. La specificità delle comunicazioni elettroniche, rispetto a tale normativa generale, venne disciplinata per la prima volta dalla direttiva 97/66/CE per la salvaguardia della pubblica sicurezza, della difesa o dell'ordine pubblico (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato), e per l'applicazione del diritto penale, che consentiva la conservazione e l'uso di dati a fini di contrasto[20]. La questione della necessità di bilanciamento tra diritti fondamentali ed esigenze di sicurezza era ben presente al momento dell'adozione della prima disciplina generale delle comunicazioni elettroniche dell'Unione (pacchetto di direttive del 2002), dopo la distruzione delle Torri gemelle[21].

L'adozione della direttiva c.d. *data retention* del 2006[22] apparve necessaria al legislatore europeo dopo gli attacchi terroristici di Madrid e Londra. Essa legittimava la raccolta di metadati da parte dei *service provider* senza alcun collegamento con indagini in corso ma solo nell'eventualità (in nessun modo pronosticabile al momento della raccolta) di

[17] C 199/11, *Otis and Others*, par. 47, case C 398/13 P, *Inuit Tapiriit Kanatami*, par. 46 and case C-601/15 PPU, par. 46.

[18] Per la originaria proposta, v. COM/90/314 def, 24 settembre 1990, Proposta di direttiva del Consiglio sulla protezione dei dati personali e della vita privata nell'ambito delle reti digitali pubbliche di telecomunicazione, con particolare riferimento all'ISDN (rete digitale integrata nei servizi) e alle reti digitali per servizi pubblici di radiotelefonia mobile.

[19] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, *GUUE* n. L 281 del 23 novembre 1995, 31 ss.

[20] V. direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, *GUUE* L 24 del 30 gennaio 1998, p. 1 ss. (art. 14, par. 1).

[21] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva *e-privacy*), *GUUE* L 201 del 31 luglio 2002. La direttiva *e-privacy* è stata rivista dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica (…) della direttiva 2002/58/CE (…), *GUUE* L 337, 18.12.2009, 11 ss. Per alcuni aspetti della riforma del pacchetto sulle comunicazioni elettroniche del 2019, v. G. Caggiano, *La riforma del regime delle radiofrequenze nel quadro delle comunicazioni elettroniche*, in *Studi sull'integrazione europea*, 2010, 79 ss.; Id, *La regolazione delle reti delle comunicazioni e dell'energia nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2011, 41 ss.

[22] La direttiva 2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, del 15 marzo 2006, *GUUE* L 105/54 del 13 aprile 2006, ha previsto l'obbligo degli Stati membri di provvedere affinché determinate categorie di dati (elencati nell'art. 5), siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione. L'attacco terroristico di Londra è esplicitamente richiamato nel decimo considerando della direttiva 2006/24/CE.

"sopravvenienti indagini" collegate alla commissione di gravi reati[23].

Nella storica sentenza *Digital Rights Ireland*[24], la Corte di giustizia sottolinea l'estrema sensibilità dei metadati: «Questi dati, presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati»[25].

La Corte ha dichiarato invalida l'intera direttiva 2006/24 per violazione dei diritti al rispetto della vita privata e alla protezione dei dati personali[26]. La sentenza presuppone il rango di diritto primario della Carta senza un esplicito richiamo all'art. 6, par. 1 TUE. La Corte applica il test di necessità in senso stretto a tutte le misure che prevedano limitazioni all'esercizio del diritto alla protezione dei dati personali e al rispetto della vita privata: «derogazioni e limitazioni in relazione alla protezione di dati personali devono essere applicate solamente qualora ciò si riveli strettamente necessario»[27]. La Corte ha sottolineato che «non importa che le informazioni in questione, relative alla vita privata siano dati sensibili o se le persone interessate siano state colpite direttamente»[28].

Secondo la sentenza in parola, «l'obbligo di conservare per un certo periodo dati relativi alla vita privata di una persona e alle sue comunicazioni" e l'accesso delle autorità nazionali competenti ai dati costituiscono di per sé un'ingerenza nei diritti garantiti dalla Carta[29]. Dal punto di vista del *test di necessità in senso stretto*, i criteri di accesso ai dati da parte delle autorità pubbliche (persone autorizzate, uso strettamente necessario, ecc.) devono essere oggetto di scrutinio e analisi approfondita. Inoltre, il *test di proporzionalità* richiede che la misura limitativa sia, da un lato, essenziale al raggiungimento della finalità d'interesse generale; e, dall'altro, il più possibile "meno intrusiva" di altre

---

[23] La direttiva *data retention*, ancorchè "di fatto" complementare all'indagine e alla prevenzione del crimine, venne giudicata nel 2009 dalla Corte di giustizia come correttamente adottata sulla base giuridica della realizzazione del mercato (art. 95 TCE, divenuto oggi art. 114 TFUE) perché riferita alle attività dei provider (e non al terzo pilastro), v. sentenza 10 febbraio 2009, C-301/06, *Irlanda c. Parlamento e Consiglio*, sulla scelta della base giuridica della direttiva 2006/24. Per un commento, v. F. Fabbrini, *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quad. cost.*, 2009, 419 ss.

[24] S. Peers, *Data Retention: A Landmark Court of Justice's Ruling (4) Will this saga continue and how?*, 8 Aprile 2014, in *EU Law Analysis*, 2014: «*The CJEU has seized the chance to give an iconic judgment on the protection of human rights in the EU legal order. Time will deal whether the Digital Rights judgment is seen as the EU's equivalent of classic civil rights judgments of the US Supreme Court, on the desegregation of schools (Brown) or criminal suspects' rights (Miranda). If the Charter ultimately contributes to the development of a 'constitutional patriotism' in the European Union, this judgment will be one of its foundations*».

[25] Corte di giustizia, sentenza *Digital Rights Ireland*, punto 27.

[26] Sulla sentenza della Corte, v. M. P. Granger - K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, in *Eur. L. Rev.*, 2014, 835 ss.; O. Lynskey, *The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland*, in *Comm. Mark. L. Rev.*, 2014, 1789 ss.; M. Nino, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia Ue: prospettive ed evoluzioni future del sistema europeo di data retention*, in *Diritto dell'Unione europea*, 2014, 803 ss.; E. Rossi, *Il diritto alla "privacy" nel quadro giuridico europeo ed internazionale alla luce delle recenti vicende sulla sorveglianza di massa*, in *Dir. com. scambi internaz.*, 2014, 331 ss.; M. Messina, *La Corte di giustizia Ue si pronuncia sulla proporzionalità delle misure in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica e ne dichiara la loro invalidità*, in *Rivista OIDU*, 2014, 396 ss.

[27] *Digital Rights Ireland*, punto 47.

[28] *Digital Rights Ireland*, punto 33.

[29] *Digital Rights Ireland*, punti 34 e 35.

alternative, quali, ad esempio, controllo sui dati solo di una parte della popolazione o di una zona geografica.

La Corte osserva che la direttiva *data retention* prevede ingerenze nei diritti fondamentali «di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione» e non appresta adeguate garanzie[30]. La Corte pondera le finalità di interesse generale cui risponde la disciplina sottoposta al suo esame (principalmente la lotta al terrorismo e alla criminalità), ma all'esito del giudizio di bilanciamento con i diritti fondamentali giudica che tali ingerenze non rispondano al principio di proporzionalità (art. 52. par. 1 della Carta).

La decisione accerta le ingerenze nei diritti protetti dalla Carta, la loro prevalenza rispetto ad altri interessi in gioco e il superamento dei limiti imposti dal rispetto del principio di proporzionalità per l'assenza delle necessarie garanzie (art. 52, par. 1)[31]. Considerata l'ampiezza e pervasività dei profili di contrasto con i diritti in discussione[32], la Corte dichiara l'invalidità totale della direttiva con effetti *ex tunc*[33]. Anche l'Avvocato Generale Cruz Villalón era giunto al medesimo risultato ma sulla base delle carenze del requisito della "previsione legislativa" che difettava, a suo avviso, di sufficiente precisione sulle condizioni di accesso e impiego dei dati conservati[34]. La sentenza, anticipando i temi della giurisprudenza successiva, evoca la necessità di analoghi strumenti di salvaguardia nell'ipotesi in cui la raccolta e la conservazione dei dati siano disposti per motivi di sicurezza da parte di autorità straniere[35].

Nella quasi parallela sentenza *Google*, meno rilevante per la prospettiva del presente lavoro, il riferimento alla Carta nello specifico del diritto all'identità personale (o diritto all'oblio), si riferisce al ruolo dei motori di ricerca nei confronti degli utenti europei, conferendo loro una funzione di cancellazione di alcuni dati personali non più attuali ma conservando un giudizio di seconda istanza alle autorità nazionali indipendenti. La scelta di non richiamare i principi generali dell'ordinamento dell'Unione, né la CEDU, sottolinea il ruolo costituzionale che la Corte di giustizia riconosce alla Carta. La sentenza in parola ribadisce più volte che dei diritti "derivanti" o "risultanti" dalla Carta si deve tener conto nella «ponderazione dei contrapposti diritti e interessi in gioco»[36].

Tuttavia, nella sentenza in parola vale la pena di sottolineare l'ampliamento dell'ambito

---

[30] Sentenza *Digital Rights*, cit., punto 37. Per l'affermazione secondo la quale la direttiva 2006/24 «non prevede garanzie sufficienti, come richieste dall'articolo 8 della Carta», v. *ibidem*, punto 66; v. anche il punto 68, ai sensi del quale «non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, paragrafo 3 della Carta, del rispetto dei requisiti di protezione e sicurezza» dei dati medesimi.

[31] L. Woods, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)*, in *EU Law Analysis*, 21 December 2016

[32] La Corte non si è neppure posta la questione di una dichiarazione di invalidità parziale (o di annullamento parziale) per parti "separabili" dell'atto che potrebbe costituire una questione di ricevibilità della domanda pregiudiziale, v. conclusioni dell'AG Juliane Kokott presentate il 23 dicembre 2015, causa C-477/14, *Pillbox 38 (UK) Limited*, paragrafi 13-16 e giurisprudenza ivi citata.

[33] Si noti che la Corte non ha limitato gli effetti nel tempo della dichiarazione di invalidità, come invece aveva chiesto l'avvocato generale.

[34] V. le conclusioni dell'avvocato generale P. Cruz Villalón, presentate il 12 dicembre 2013 in causa *Digital Rights*, spec. al punto 153.

[35] V. *Digital Rights*, punto. 68 che ricorda che «tale direttiva non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione».

[36] Sentenza *Google*, cit., punti 74, 81 e 97 della motivazione e punto 4) del dispositivo.

di applicazione territoriale della direttiva 95/46 sulla tutela dei dati personali. L'interpretazione estensiva è finalizzata ad assicurare garanzie equivalenti ai dati trattati/trasferiti fuori dai confini dell'Unione[37]. Secondo la disciplina in vigore[38], il trasferimento di dati personali da Stati membri dell'Unione verso Paesi-terzi è vietato, a meno che non sia garantito un livello di protezione "adeguato", accertato e validato dalla Commissione attraverso una specifica decisione[39]. In deroga a tale divieto, il trasferimento verso Paesi-terzi è consentito anche nel caso di consenso della persona interessata, interesse pubblico preminente, ecc., nonché sulla base di adeguati strumenti contrattuali.

4. La sentenza *Schrems* e l'invalidità della dichiarazione di adeguatezza della Commissione

Proprio rispetto al trasferimento dei dati personali dall'Unione europea alle piattaforme di servizi su internet (*social network*), localizzate negli Stati Uniti, il "cammino costituzionale" della Corte di giustizia si perfeziona ulteriormente[40].

[37] A tal fine, la Corte ritiene rilevante non tanto il luogo in cui il trattamento dei dati viene fisicamente effettuato, quanto il luogo in cui il motore di ricerca esercita la propria attività, ove apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro. L'interpretazione della Corte anticipa così il Regolamento generale sulla protezione dei dati del 2016 che valorizza il criterio di applicabilità della normativa europea al destinatario del servizio e non del criterio della localizzazione del prestatore del servizio, v. art. 3, Campo di applicazione territoriale: «Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento nell'Unione. Il presente regolamento si applica al trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento che non è stabilito nell'Unione […]».

[38] Nel nuovo Regolamento generale del 2016, *cfr.* gli articoli 45 (trasferimento sulla base di una decisione di adeguatezza); 46 (altre garanzie adeguate, comprese le norme vincolanti d'impresa); art. 49 (deroghe in specifiche situazioni).

[39] L'Accordo sull'approdo sicuro è un accordo concluso nel 2000 tra Unione europea e Stati Uniti per garantire la protezione dei dati dei cittadini europei, anche quando i dati sono in possesso di imprese americane, fuori dal territorio europeo. Il funzionamento dell'accordo si basava sulla richiesta di autocertificazione alle aziende americane circa il rispetto delle regole sulla protezione dei dati. La Commissione aveva in precedenza valutato che tutte le autorità americane competenti avevano accesso libero ai dati conservati e trattati negli Stati Uniti, v. COM(2013) 847 final sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite.

[40] In argomento v. M. Nino, *Terrorismo internazionale, privacy e protezione dei dati personali*, Napoli, 2012, 147 ss.; D. Bigo et al., *Open Season for Data Fishing in the Web: The Challenges of the US PRISM Programme for the EU*, *Policy Brief*, CEPS, Brussels, June 2013; v. anche Id., *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*, *Paper in Liberty and Security in Europe*, CEPS, Brussels, November 2013. Per un'ampia disamina delle differenze tra UE e USA in materia di trattamento dei dati per finalità di contrasto della criminalità, si veda F. Bohem, *A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes, Study for the LIBE Committee*, PE 2015; P. M. Schwartz - D. J. Solove, *Reconciling Personal Information in the United States and European Union*, in *California L. Rev.*, 2014, 877; F. Bignami - G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, in *LCP*, 2015, 101 ss. Sul sistema statunitense si veda anche F. Bignami, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*, Study for the LIBE Committee, PE 519.215, May 2015.

Secondo la sentenza *Schrems*[41], i dati personali devono essere improntati all'effettiva osservanza della Carta negli atti dell'Unione, che devono tener conto dell'adeguatezza della tutela di altri ordinamenti giuridici coinvolti nella conservazione dei dati. Secondo la disciplina in vigore (confermata sostanzialmente dal Regolamento generale del 2016), il trasferimento di dati personali da Stati membri dell'Unione verso Paesi-terzi è vietato, a meno che non sia garantito un livello di protezione "adeguato", accertato e validato dalla Commissione attraverso una specifica decisione[42]. In deroga a tale divieto, il trasferimento verso Paesi-terzi è consentito anche nel caso di consenso della persona interessata, interesse pubblico preminente, ecc., nonché sulla base di adeguati strumenti contrattuali.

Con la sentenza *Schrems*, la Corte di giustizia statuisce l'invalidità della decisione della Commissione classificabile come atto esecutivo di terzo livello dell'ordinamento dell'Unione[43]. I motivi di invalidità si ritrovano, al di là delle assicurazioni offerte a suo tempo dalle autorità statunitensi, nelle modalità effettive di interpretazione e gestione dei dati. In tale ordinamento di destinazione dei dati personali, non erano previste regole idonee a limitare le ingerenze allo "stretto necessario" per conseguire l'obiettivo della protezione della sicurezza nazionale, né specifici rimedi di natura giurisdizionale o amministrativa a tutela dei soggetti interessati. Le deroghe ammissibili avrebbero dovuto essere munite di un meccanismo di controllo indipendente e di mezzi di ricorso adeguati[44]. Pertanto, le ingerenze riscontrate superano di gran lunga quanto strettamente necessario e, nel caso specifico, intaccano il contenuto essenziale del diritto al rispetto della vita privata in un quadro giuridico "affievolito" di tutela. In conclusione, la sorveglianza di massa dei cittadini dell'Unione non è conforme alla Carta[45].

La Corte riafferma solennemente il proprio cammino costituzionale: «[…] secondo la quale l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono

[41] Sentenza 6 ottobre 2015, causa C-362/14, *Schrems*. Per un'analisi, v. S. Carrera - E. Guild, *Safe Harbour or into the Storm? EU-US Data Transfers after the Schrems Judgment*, in *CEPS Liberty and Security in Europe Papers*, November 2015. Sulla sentenza e i suoi seguiti, v. V. Zeno-Zencovich - G. Resta (a cura di), *La protezione transnazionale dei dati personali Dai "safe harbour principles" al "privacy shield"*, Roma, 2016, in particolare i contributi di V. Zeno-Zencovich, G. Resta, C. Comella, O. Pollicino-M. Bassini, G. Finocchiaro, P. Piroddi.

[42] L'Accordo sull'approdo sicuro è un accordo concluso nel 2000 tra Unione europea e Stati Uniti per garantire la protezione dei dati dei cittadini europei, anche quando i dati sono in possesso di imprese americane, fuori dal territorio europeo. Il funzionamento dell'accordo si basava sulla richiesta di autocertificazione alle aziende americane circa il rispetto delle regole sulla protezione dei dati. La Commissione ha valutato che le autorità americane avevano accesso libero ai dati conservati e trattati negli Stati Uniti, v. COM(2013) 847 final sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite.

[43] Tale decisione veniva impropriamente chiamata "Accordo UE-Usa Safe Harbor" mentre, in realtà, si trattava in sostanza di un atto unilaterale della Commissione a seguito di documentazione presentata dall'Amministrazione Usa.

[44] Le difficoltà derivano dall'impiego che le autorità americane fanno delle deroghe previste dalla disposizione dell'Allegato I, quarto comma.

[45] Sentenza 6 ottobre 2015, cit., par. 93, 94 e 95. In particolare, viene giudicata incompatibile con la Carta (articoli 7 e 8) «che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta».

soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali[46][…]. La Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione […] e la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione[47] […]. Per quanto i giudici nazionali siano effettivamente legittimati ad esaminare la validità di un atto dell'Unione […], essi non sono tuttavia competenti a constatare essi stessi l'invalidità di un siffatto atto[48]. *A fortiori*, in sede di esame di una domanda, […] le autorità nazionali di controllo non sono competenti a constatare esse stesse l'invalidità di una siffatta decisione»[49].

Si tratta della riconferma della giurisprudenza *Foto-Frost*, il cui obbligo di rinvio è parte integrante dell'*acquis* comunitario, nonostante il mancato inserimento nelle varie modifiche dei Trattati istitutivi. In tale giurisprudenza in materia, la Corte aveva più ampiamente motivato che i giudici nazionali non sono competenti a dichiarare l'invalidità degli atti delle istituzioni dell'Unione perché il rinvio pregiudiziale di validità deve garantire l'uniforme applicazione del diritto comunitario da parte dei giudici nazionali, soprattutto quando viene messa in dubbio la validità del diritto dell'Unione. Infatti, le divergenze fra i giudici nazionali su tale validità potrebbero compromettere la stessa unità dell'ordinamento giuridico comunitario e ledere il principio fondamentale della certezza del diritto.

E' importante sottolineare che nella sentenza *Schrems*, la Corte di giustizia dichiara l'invalidità dell'atto in parola, in sede di interpretazione pregiudiziale, senza esserne richiesta esplicitamente dal ricorrente nel procedimento principale né dal giudice di rinvio. Quando una persona si rivolge a un'autorità nazionale di controllo, essa esamina la compatibilità della decisione alla base del trasferimento dei dati con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona: «[…]tali giudici devono sospendere la decisione e investire la Corte di un procedimento pregiudiziale per accertamento di validità, allorché essi ritengono che uno o più motivi di invalidità formulati dalle parti o, eventualmente, sollevati d'ufficio siano fondati »[50]. Come richiamato dall'Avvocato generale[51], «nell'ambito del ricorso per annullamento, la legittimità di un atto deve essere valutata in base alla situazione di fatto e di diritto esistente al momento in cui l'atto è stato adottato, e la valutazione della Commissione può essere criticata solo se essa risulta manifestamente erronea alla luce degli elementi di cui la

[46] Nel testo della sentenza *Schrems*, la Corte cita le sue precedenti sentenze *Commissione e a./Kadi*, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 66; *Inuit Tapiriit Kanatami e a./Parlamento e Consiglio*, C-583/11 P, EU:C:2013:625, punto 91, nonché *Telefónica/Commissione*, C-274/12 P, EU:C:2013:852, punto 56.

[47] Tra le più recenti vengono citate le sentenze *Melki e Abdeli*, C-188/10 e C-189/10, punto 54, nonché *CIVAD*, C-533/10, punto 40.

[48] La Corte cita in tal senso le sentenze *Foto-Frost*, 314/85, EU:C:1987:452, punti da 15 a 20, nonché *IATA e ELFAA*, C-344/04, EU:C:2006:10, punto 27. Su quest'ultima v. G. Gattinara, *La questione pregiudiziale di validità rispetto al diritto internazionale pattizio secondo la sentenza IATA*, in *SIE*, 2006, 343 ss.

[49] V. paragrafi 60-62.

[50] Al riguardo la Corte cita la sentenza *T & L Sugars e Sidul Açúcares/Commissione*, C-456/13 P, EU:C:2015:284, punto 48 e la giurisprudenza ivi citata.

[51] *Ivi*, paragrafi 131 e 132.

stessa disponeva al momento dell'adozione dell'atto in questione»[52].

La Corte ha altresì rilevato che garantire l'accesso a rimedi efficaci e un controllo giurisdizionale indipendente costituiscono condizioni essenziali per garantire lo Stato di diritto[53]: «l'esigenza di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto»[54]. Al riguardo, condizione essenziale è il diritto ad ottenere una tutela giurisdizionale (art. 19 TUE ai sensi del quale gli Stati membri hanno l'obbligo di assicurare la tutela giurisdizionale effettiva «nei settori disciplinati dal diritto dell'Unione») e dell'art. 47 della Carta (che influisce sulla interpretazione di molte regole nazionali processuali, ad esempio in materia di diritto alla difesa e al patrocinio legale a spese dello Stato, purché strumentali alla tutela di diritti conferiti da norme dell'Unione).

Decisiva è anche la giurisprudenza sul giusto processo che è applicabile nei procedimenti dinanzi ai giudici dell'Unione e nei procedimenti che si svolgono davanti ai giudici nazionali quando gli Stati attuano le norme dell'Unione. Secondo la giurisprudenza *Kadi*, [55], tale controllo di legittimità alla luce dei diritti fondamentali assume il valore di "garanzia costituzionale"[56] e riguarda qualsiasi atto dell'Unione. Il sistema di tutela giurisdizionale dei trattati si regge infatti sui due pilastri dei giudici dell'Unione e di quelli nazionali[57]. Quest'ultimi «stabiliscono i rimedi giurisdizionali necessari per assicurare una tutela giurisdizionale effettiva nei settori disciplinati dal diritto dell'Unione, secondo e l'art 47 della Carta»[58].

Una nuova decisione di adeguatezza del trattamento dei dati trasferiti negli Stati è stata adottata da parte della Commissione dopo l'invalidità della precedente decisione, perché era urgente ripristinare le comunicazioni a livello transatlantico[59].

---

[52] V., segnatamente, sentenza *BVGD/Commissione* (T-104/07 e T-339/08, EU:T:2013:366, punto 291), che richiama la sentenza *IECC/Commissione* (C-449/98 P, EU:C:2001:275, punto 87). Sentenza 1° ottobre 2009, C-247/08, *Gaz de France – Berliner Investissement*, EU:C:2009:600, punto 49 e la giurisprudenza ivi citata.

[53] *Schrems*, par. 95.

[54] V, in tal senso, la Corte richiama la propria giurisprudenza al riguardo: sentenze *Les Verts/Parlamento*, 294/83, EU:C:1986:166, punto 23; *Johnston*, 222/84, EU:C:1986:206, punti 18 e 19; *Heylens e a.*, 222/86, EU:C:1987:442, punto 14, nonché *UGTRioja e a.*, da C428/06 a C434/06, EU:C:2008:488, punto 80.

[55] In tal senso, sentenze *Commissione e a./Kadi*, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 66; *Inuit Tapiriit Kanatami e a./Parlamento e Consiglio*, C-583/11 P, EU:C:2013:625, punto 91, nonché *Telefónica/Commissione*, C-274/12 P, EU:C:2013:852, punto 56.

[56] V. sentenze del 29 giugno 2010, *E e F*, C-550/09, Racc. pag. I-6213, punto 44, nonché 26 giugno 2012, *Polonia/Commissione*, C-335/09 P, punto 48.

[57] *Cfr.* sentenza del 3 ottobre 2013, in causa C-583/11 P, *Inuit Tapiriit Kanatami*, cit., punto 90.

[58] *Ivi*, punto 101.

[59] Per il nuovo atto della Commissione, v. Decisione di esecuzione (Ue) 2016/1250 della Commissione del 12 luglio 2016 a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy [notificata con il numero C(2016) 4176] C(2016) 4176 final, Allegati da 1 a 7, in *GURI* 29-9-2016 2a Serie speciale - n. 74, 1-112. Sulla decisione, v. WP 238, Opinion 1/2016 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016. Per un commento, v. S. Crespi, *La nuova proposta di decisione di adeguatezza della commissione europea riguardo agli Usa: lo scudo Ue/Usa per la privacy*, in *Eurojus.it*, 2016. Nei confronti della nuova decisione è stato già proposto ricorso dal medesimo ricorrente, v. causa T-670/16, ricorso proposto il 16 settembre 2016, *Digital Rights Ireland/Commissione*.

5. L'interpretazione conforme alla Carta delle legislazioni nazionali nella sentenza *Tele2/Watson*

Rispetto all'interpretazione delle disposizioni in materia di *data retention*, la Corte di giustizia è ritornata in argomento nella sentenza *Tele2/Watson* del 21 dicembre 2016[60]. Le controversie *a quo* vertevano sull'obbligo generale imposto in Svezia e nel Regno Unito ai fornitori di servizi di comunicazioni elettroniche sulla base della direttiva *e-privacy* 2002/58 (art.15, par.1), una normativa antecedente alla direttiva *data retention* ma non "travolta" dal giudizio di invalidità di quest'ultima.

Nella sentenza, la Corte di giustizia ha dichiarato che tale disposizione alla luce della Carta (artt. 7, 8, 11 e art. 52, n. 1) osta ad una normativa nazionale che, ai fini della lotta contro la criminalità, prevede la conservazione generale e indiscriminata di tutti i dati di traffico e di localizzazione di tutti gli abbonati e degli utenti registrati relativi a tutti i mezzi di comunicazione elettronica. Sono giudicati incompatibili con gli obblighi di attuazione della Carta, le legislazioni nazionali che prevedano l'obbligo degli operatori di conservazione generalizzata e indifferenziata dei dati personali e consentano, senza specifici meccanismi di trasparenza, l'accesso da parte delle autorità nazionali. La conservazione di tali dati deve essere comunque rispettosa del principio di proporzionalità e l'accesso deve essere sottoposto ad un preventivo controllo da parte dei giudici e/o dell'autorità indipendente competente. Si tratta di un'indicazione significativa dell'obbligo di interpretazione conforme alla Carta da parte delle disposizioni nazionali nell'attuazione del diritto dell'Unione.

La direttiva e-*privacy* consente la memorizzazione dei dati soltanto nella misura e per la durata necessaria per la fatturazione dei servizi, per la loro commercializzazione e per la fornitura di servizi a valore aggiunto. Al contrario ne fa divieto senza il consenso dell'utilizzatore interessato, salvo che si verifichino determinate condizioni previste dalla legge (art. 15, n. 1)[61]. La Corte afferma che l'interpretazione di tale deroga relativa a un diritto fondamentale non può che essere restrittiva. L'elencazione degli obiettivi ha carattere esaustivo e non può essere travisata dagli Stati membri: «(…) una disposizione siffatta non può giustificare che la deroga al suddetto obbligo di principio e, in particolare, al divieto di memorizzare tali dati (…), divenga la regola, a pena di privare quest'ultima norma di gran parte della sua portata»[62].

---

[60] Sentenza del 21 dicembre 2016 nelle cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB e Tom Watson*. Per un commento, v. I. Cameron, *'A. Court of Justice Balancing data protection and law enforcement needs: Tele2 Sverige and Watson',* in *Common Market Law Review,* 2017, 1467 ss.

[61] L'art. 15, par. 1, prima frase, della direttiva 2002/58 stabilisce che le misure legislative restrittive devono avere come obiettivo «la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica». La medesima disposizione deve essere integrata e interpretata alla luce del rinvio alla direttiva 95/46: «Deroghe e restrizioni: […] una misura necessaria alla salvaguardia: a) della sicurezza dello Stato; b) della difesa; c) della pubblica sicurezza; d) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate; e) di un rilevante interesse economico o finanziario di uno Stato membro o dell'Unione europea, anche in materia monetaria, di bilancio e tributaria; f) di un compito di controllo, ispezione o disciplina connesso, anche occasionalmente, con l'esercizio dei pubblici poteri nei casi di cui alle lettere c), d) ed e); g) della protezione della persona interessata o dei diritti e delle libertà altrui (art. 13, par. 1)».

[62] Par. 89.

Più in particolare, la sentenza *Tele2/Watson* afferma che è necessario un bilanciamento con i livelli di tutela e l'adozione di modalità operative proporzionate. Il livello di proporzionalità viene applicato al margine di discrezionalità degli Stati membri per la conservazione dei dati e l'accesso da parte delle autorità nazionali competenti. E' incompatibile con il diritto dell'Unione la legislazione nazionale che: non limiti l'accesso ai dati alle sole finalità di lotta contro la criminalità grave, non sottoponga l'accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente[63]; non esiga che i dati siano conservati nel territorio dell'Unione; non imponga di comunicare appena possibile all'interessato l'avvenuto accesso; non fondi su elementi oggettivi le circostanze in presenza delle quali l'accesso è ammesso[64].
L'Avvocato generale esplicita nuovamente l'ulteriore condizione di ricerca di una misura meno intrusiva che possa offrire la medesima efficacia nella lotta contro i reati gravi[65].
La disposizione dichiarata invalida invece non richiede alcuna correlazione tra la conservazione dei dati e l'esistenza di una minaccia per la sicurezza pubblica. La limitazione della conservazione non è prevista «per un periodo di tempo e/o a una zona geografica e/o una cerchia di persone suscettibili di essere implicate in una maniera o in un'altra in una violazione grave, oppure persone che potrebbero, per altri motivi, contribuire, mediante la conservazione dei loro dati, alla lotta contro la criminalità»[66].
Secondo la Corte, l'obiettivo di interesse generale non vale di per sé solo a giustificare una normativa nazionale[67].

6. La proposta della Commissione di direttiva *e-privacy* che rinuncia all'armonizzazione legislativa in materia e rinvia ai principi generali del Regolamento generale sulla protezione dei dati

Le implicazioni della giurisprudenza della Corte di giustizia si prevedono particolarmente interessanti in sede di attuazione delle decisioni a livello dell'Unione e degli ordinamenti nazionali nazionale.
Al riguardo, occorre premettere che la direttiva *data retention*, dichiarata invalida dalla Corte di giustizia nel 2014, non è stata a oggi ancora sostituita.
A seguito delle decisioni della Corte di giustizia, il legislatore dell'Unione e i legislatori

63 CEDU, *Szabó e Vissy c. Ungheria,* ric. 37138/14 (2016), § 77 e 80.

64 CEDU, *Zakharov c. Russia,* ric. 47143/06 (2015), § 260.

65 Conclusioni dell'Avvocato generale nella causa *Tele2 Sverige AB* (C-203/15 e C-698/15), punti 209 e 211.

66 *Schrems*, punto 106. Nello stesso senso la sentenza *Digital Rights*, punto 59.

67 *Schrems*, punto 103. Nello stesso senso sentenza *Digital Rights*, punto 51. Ne consegue il giudizio su tale disposizione: «Una normativa nazionale come quella in discussione nei procedimenti principali travalica dunque i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, così come richiede l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta» (*Scherms*, punto 108).

nazionali dovranno correggere gli elementi di incompatibilità con la Carta[68]. Le sentenze *Schrems* e *Tele2/Watson* consentono di riconoscere effetti diretti alla regola generale di divieto di conservazione indiscriminata dei dati, salvo che per esigenze specifiche di contrasto ai reati gravi e con il supporto di specifiche garanzie processuali. Ne consegue l'obbligo per i giudici nazionali e la pubblica amministrazione di procedere alla disapplicazione delle norme nazionali contrastanti.

Al riguardo, le eventuali incertezze applicative della dichiarazione di invalidità della direttiva *data retention* sulle norme nazionali (che pure, ex art. 51 della Carta, poteva considerarsi "strettamente collegate" anche se non di trasposizione in senso tecnico) sono da ritenersi superate dalla successiva interpretazione restrittiva svolta direttamente dalla Corte sulle deroghe previste dalla direttiva *e-privacy* tuttora vigente.

Da parte degli Stati-membri, si manifesta una forte "resistenza" a seguire le indicazioni della Corte nel senso di ridimensionare, tramite un'armonizzazione normativa più stringente, uno strumento di contrasto. ritenuto strategico per la sicurezza nazional[69]. E' indiscutibile che la conservazione dei metadati è ritenuta da molti Stati membri un "paracadute" importante per la propria sicurezza, consentendo accertamenti *ex-post* sui comportamenti di individui sospettati per reati gravi (comprensivi di quelli di pericolo)[70]. Dal punto di vista dell'interesse pubblico alla sicurezza dello Stato, qualsiasi modalità di conservazione per ordine giudiziario non potrebbe sostituire, in modo altrettanto efficace, la conservazione generalizzata dei "dati storici" in discussione. La conservazione per ordine giudiziario, infatti, non garantisce la possibilità di individuare "tracce precedenti" del reato e ovviamente non fornisce aiuto alle indagini prima che vi sia un soggetto sospettato.

Nella riforma in atto delle comunicazioni elettroniche si manifesta la rinuncia a sostituire la direttiva *data retention* con un altro atto di armonizzazione delle legislazioni

[68] Il Regolamento generale sulla protezione dei dati (GDPR), regolamento UE n. 2016/679) del 24 maggio 2016, mira a rendere maggiormente efficace il livello di tutela dei dati personali trattati nelle comunicazioni elettroniche in accordo con gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. In primo luogo, i nuovi servizi offerti mediante Internet e utilizzati da un numero crescente di consumatori, come ad esempio le chiamate VoIP (*Voice over IP*), o la sempre più diffusa messaggistica istantanea non rientrerebbero nel campo di applicazione della direttiva *ePrivacy* né del regolamento 679/2016.

[69] Sull'evoluzione del quadro legislativo negli Stati membri, v. FRA, *Data retention across the EU*, disponibile *online*: «*Member States made only limited progress in adopting new legal frameworks for data retention to incorporate the requirements and safeguards set out in the CJEU's case law. Most seem reluctant to amend their national laws to conform to the Digital Rights Ireland and Tele2 judgments. In the meantime, challenges against domestic data retention laws in Member States generally abated, though three characteristic cases challenging data retention were brought in Germany, the Netherlands and the United Kingdom in 2016*».

[70] COM(2011) 225 definitivo, 18 aprile 2011, Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24/CE).

nazionali[71]. In discussione, come abbiamo già detto nel corso di questo lavoro, non è però la legittimità dell'obiettivo ma la durata del periodo di conservazione, la necessità e stretta proporzionalità della raccolta, la trasparenza dell'accesso da parte delle Autorità pubbliche, l'esistenza di ricorsi giurisdizionali e amministrativi da parte delle persone coinvolte.

La proposta di aggiornamento della direttiva *e-privacy*, attualmente in discussione al Consiglio e al Parlamento europeo, è incentrata principalmente sull'attività dei *service provider* e non sulla sorveglianza e accesso ai metadati da parte delle Autorità pubbliche. La proposta dovrebbe contenere soltanto un generico rinvio alle limitazioni ammissibili al principio di riservatezza, secondo il Regolamento generale sulla protezione dei dati del 2016 (art. 23). La decisione di non procedere all'armonizzazione aumenta il margine di discrezionalità degli Stati membri e rende più difficile la verifica giurisdizionale dei principi affermati dalla Corte di giustizia.

Secondo le norme proposte, sia il contenuto delle comunicazioni sia i metadati dovranno essere anonimizzati o eliminati in caso di mancato consenso degli utenti, purché non siano necessari per specifiche finalità (*cfr.* art. 6 della proposta di Regolamento). Competente per la violazione delle norme sulle comunicazioni elettroniche saranno le Autorità nazionali per la protezione dei dati personali. Per quanto riguarda l'ambito territoriale, la proposta si applica ai servizi forniti agli utenti finali nell'Unione, indipendentemente dal fatto che il fornitore sia stabilito nell'Unione.

Quanto al rispetto dei limiti per la conservazione dei dati nelle legislazioni nazionali non contiene disposizioni di armonizzazione ma contiene una clausola generale che rinvia agli Stati membri di legiferare sulle restrizioni della portata dei diritti e degli obblighi previsti purchè «siffatta limitazione rispetta l'essenza dei diritti e delle libertà fondamentali e costituisce una misura necessaria, appropriata e proporzionata in una società democratica intesa a salvaguardare uno o più interessi pubblici» in conformità al Regolamento generale del 2016[72].

Infatti, anche se la direttiva *data retention* è stata dichiarata invalida dalla Corte di giustizia, molti Stati membri continuano ad applicare le normative nazionali adottate in attuazione di tale direttiva o comunque ispirate da principi e meccanismi dichiarati illegittimi. Gli Stati membri sono pertanto liberi di mantenere o creare quadri di riferi-

[71] Le implicazioni della sentenza Tele2/Watson sono state analizzate dal servizio giuridico del Consiglio, Doc. Council 5884/11, 1 February 2017 (document partially accessible to the public 29.03.2017), Legal Service to Permanent Representatives Committee, Judgment of the Court of 21 December 2016 in joined Cases C-203/15 and C-698/15 (*Tele2 and Watson*) (Parte III. *Consequences of the judgement for the Council (deleted*). Sulle difficoltà degli Stati-membri a seguire le indicazioni della Corte di giustizia, v. doc. Council 6713/17, 1 March 2017, *Retention of electronic communication data, next steps*, par. 3: «*Many delegations expressed their concerns on the implications of the judgement, which might hinder the effectiveness of the investigations and prosecutions of crimes*». Sul dibattito in seno al Consiglio, Doc. 8798/17, 4 May 2017, Access criteria for competent authorities to retained communication data, Exchange of views; doc. 11107/17, 12 July 2017, Processing and storage of data in the context of the draft ePrivacy Regulation, Introduction and preliminary exchange of views; doc 11110/17, 12 July 2017, Requirements of the Tele 2 judgement regarding data retention, Continuation of discussion;

[72] Proposta di art. 11, che rinvia alle definizioni dell'art. 23, par. 1, lett. da *a)* a *e)*, del regolamento (UE) 2016/679, in relazione al monitoraggio, ispezione o funzione regolamentare. In base a procedure che saranno stabilite dalla legislazione degli Stati membri, i fornitori di servizi di comunicazione elettronica forniranno alla competente autorità di controllo informazioni sulle procedure di accesso, sul numero di richieste ricevute, sui motivi legali addotti e sulla loro risposta.

mento nazionali in materia di conservazione dei dati che prevedano fra l'altro misure di conservazione mirate, purché essi siano conformi al diritto dell'Unione e tengano conto della giurisprudenza della Corte di giustizia sull'interpretazione della direttiva sulla vita privata elettronica e della carta dei diritti fondamentali[73]. Non ci appare che questa formula di salvaguardia sia efficace quanto potrebbe essere l'adozione di un atto di armonizzazione delle legislazioni nazionali che fissi il periodo massimo ammissibile di conservazione dei dati, le procedure di accesso delle autorità pubbliche, le garanzie di controllo, ecc.

E' evidente che se il legislatore europeo si limitasse alla semplice indicazione dei criteri in parola segnerebbe un regresso nella tutela sostanziale dei diritti fondamentali. Soprattutto ci sembra che la scelta del legislatore dell'Unione di non sostituire la direttiva *data retention* manifesti la volontà degli Stati membri di ridurre il preteso "attivismo giudiziario" della Corte di giustizia.

Quest'ultima potrà certo continuare a reiterare le proprie indicazioni nel contesto del rinvio pregiudiziale sulla compatibilità con il diritto dell'Unione delle singole legislazioni nazionali, come ha fatto nella sentenza *Tele2* nei confronti di Svezia e Regno Unito, chiedendo al giudice nazionale di verificarne i presupposti nel procedimento principale a livello nazionale.

La materia della *data retention* continuerà infatti a far parte del «campo di applicazione del diritto dell'Unione», anche in assenza di un'articolata armonizzazione legislativa.

In ogni caso, i giudici nazionali saranno tenuti a disapplicare quegli aspetti delle legislazioni nazionali che appaiono loro incompatibili con i criteri previsti dal Regolamento del 2016 e ribaditi nella proposta di nuova direttiva *e-privacy* .Tuttavia, a nostro avviso, i giudici nazionali saranno piuttosto propensi a rivolgersi alla propria Corte costituzionale, creando occasioni di divergenza interpretativa delle disposizioni in materia di *data retention.*

7. La legge comunitaria 2017 prolunga il termine di conservazione dei dati

Da ultimo merita un accenno il caso dell'ordinamento italiano in cui è in vigore un obbligo generale di conservazione all'art. 132 del Codice della privacy, rivisto nel 2008 a seguito dell'adozione della direttiva *data retention*[74]. Tale disposizione resta in vigore in quanto non è stata rimossa dal legislatore italiano e i giudici italiani in questo perio-

[73] V. considerando 26.

[74] Sui possibili effetti delle sentenze della Corte di giustizia nell'ordinamento italiano, v. F. Iovene, *"Data retention" tra passato e futuro. Ma quale presente?,* in *Cass. penale*, 2014, 4274 ss.; A. Arena, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quad. cost.*, 2014, 722 ss.; R. Flor, *Dalla "data retention" al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive "de jure condendo"?*, in *Dir. informaz. informatica*, 2014, 775 ss.; S. Crespi, *Diritti fondamentali, Corte di Giustizia e riforma del sistema UE di protezione dei dati*, in *Riv. it. dir. pubbl. com.*, 2015, 819 ss., spec. par. 6.

do sono rimasti "sordi" alle indicazioni della Corte di giustizia[75]. In senso contrario, i termini di conservazione vengono progressivamente prolungati dal legislatore italiano. In deroga alla disposizione in parola, la legge comunitaria del 2017 prevede che i gestori del traffico telefonico e telematico conservino per settantadue mesi, senza meccanismi di consenso o regole di accesso delle Autorità pubbliche, i dati di traffico telefonico e telematico, nonché i dati relativi alle chiamate senza risposta (art. 24)[76]. La finalità dichiarata è quella di garantire strumenti di indagine efficaci in considerazione delle straordinarie esigenze di contrasto del terrorismo e degli altri gravi reati indicati, specificando che in tal modo si darebbe attuazione alla direttiva 2017/541/UE sulla lotta contro il terrorismo[77], in particolare all'obbligo di adottare misure necessarie affinché le autorità competenti dispongano di "strumenti di indagine efficaci" (art. 20)[78]. Più che di un anticipo sui termini di attuazione della direttiva 2017/541 si tratta del prolungamento della normativa italiana antiterrorismo che imponeva l'obbligo di conservazione dei dati relativi al traffico telefonico o telematico conservati dagli operatori dei servizi di telecomunicazione[79].

La nuova previsione sembra in evidente contrasto con le sentenze della Corte di giustizia, indicate nel presente lavoro, che restringono i margini di conservazione di questi dati, ancorandoli al principio di necessarietà e proporzionalità in senso stretto, e che certamente non consentono un periodo così lungo di conservazione dei metadati.

[75] R. Flor, *Data retention ed art. 132 cod. privacy: vexata quaestio (?)*, in *Dir. pen. cont.* (www.penalecontemporaneo.it), 9 marzo 2017 (Nota a Trib. Padova, ord. 15 marzo 2017). Secondo l'Autore, che critica fortemente tale sentenza, si tratta di uno dei rari casi conosciuti nella giurisprudenza italiana.

[76] V. Legislatura 17ª, Aula, Resoconto stenografico della seduta n. 894 del 10 ottobre 2017, discussione e approvazione del disegno di legge n. 2886.

[77] La direttiva prevede una normativa complessa e articolata il cui termine di recepimento scade l'8 settembre 2018. Nessun'altra disposizione della direttiva è fatta oggetto di attuazione.

[78] L'A.S. 2886 è stato esaminato dalla 14a Commissione permanente del Senato della Repubblica tra il 14 edil 27 settembre 2017 e approvato senza modifiche rispetto al testo trasmesso dalla Camera dei deputati (A.S. 2886-A).

[79] L'art. 4-*bis* della l. 17 aprile 2015, n. 43, che disciplina la conservazione dei dati di traffico telefonico o telematico. Tale norma è stata modificato dal d. l. 30 dicembre 2015, n. 210, conv. con modif. dalla l. 25 febbraio 2016, n. 21, che ha prorogato al 30 giugno 2017 il termine di conservazione dei dati relativi al traffico telefonico o telematico per le finalità di accertamento e di repressione di alcuni reati. Solo una norma si riferisce al terrorismo (art. 51, c. 3-*quater*, c.p.p), mentre le altre fattispecie richiamate riguardano altri reati gravi (art. 407, c. 2, lett. *a)*, c.p.p).

Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*

Marco Orofino

Abstract

L'articolo si propone di analizzare il mutevole quadro dei rapporti tra *privacy* (protezione dei dati personali) e sicurezza: in particolare, esso mira soprattutto a porre in evidenza come queste categorie – grazie anche al Regolamento 2016/679 e ad importanti pronunce della Corte di giustizia e della Corte CEDU – non devono più essere lette in contrapposizione tra loro, dovendosene invece fornire un'interpretazione complementare, che legga l'una in relazione all'altra.
Da un lato, infatti, la protezione dei dati personali ha assunto anche una connotazione di interesse pubblico, necessaria per il corretto funzionamento di qualsiasi ordinamento giuridico e democratico; dall'altro, il principio di sicurezza ha acquistato altresì i caratteri di diritto individuale, in un'ottica di garanzia delle libertà fondamentali del singolo quale componente del contesto sociale in cui egli vive.
Mantenendo dunque fermo il loro nucleo essenziale, *privacy* e sicurezza rappresentano due facce della stessa medaglia, ovverosia quella della protezione dei diritti essenziali dell'individuo nel più ampio quadro dei bisogni di tutela di una società globale interessata da gravi minacce alla sua stessa esistenza: minacce che impongono, quindi, di riconsiderare ragionevolmente i confini e i contenuti delle stesse libertà del singolo e delle esigenze di protezione della sicurezza collettiva.

This article aims to analyse the relations between privacy (i.e. protection of personal data) and security: in particular, it tries to underline that these categories should not be read as opposed to one another but have to be considered as complementary, especially looking at the EU Regulation 2016/679 and some important judgments of the European Court of Justice and the European Court of Human Rights.
In fact, on one side privacy has been read as a category of public interest as far as a correct development of legal and democratic systems is concerned whereas, on the other side, security has to be seen also as an individual right, necessary for the protection of fundamental rights of every single person.
Privacy and security, therefore, are two sides of the same coin, that of the guarantee of essential individual rights while trying to protect, at the same time, the broader context of a global society threatened in its own existence. For this reason, those threats impose a balanced reconsideration of the borders and contents of individual freedom and public security, always avoiding to damage their essential core.

Sommario

1. Introduzione. – 2. I bisogni ancestrali dell'uomo e la loro traduzione giuridica. – 3.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio anonimo, in quanto riproduce la relazione presentata dall'A. al convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno" (Messina, 26-27 maggio 2017).

Diritto individuale alla sicurezza e interesse costituzionale alla sicurezza. – 4. La lunga marcia del diritto alla riservatezza e il riconoscimento del *Right to privacy*. – 5. La declinazione europea della protezione dei dati personali. – 6. La sicurezza nazionale e la sicurezza pubblica come fini legittimi per la restrizione del diritto alla protezione dei dati personali. – 7. Sicurezza individuale e protezione dei dati personali – 8. Brevi osservazioni conclusive.

Keywords: Privacy, Sicurezza, Interesse pubblico, Libertà fondamentali, Limitazioni

1. Introduzione

Il tema del rapporto tra *privacy* e sicurezza ha assunto, negli ultimi anni, una particolare rilevanza[1].

Tra i molti fattori che hanno determinato questo crescente interesse, il più evidente è ovviamente quello tecnologico. Come è ormai talmente noto da apparire quasi superfluo rammentare, lo sviluppo tumultuoso ed inarrestabile delle tecnologie della comunicazione e dell'informazione sono il tratto più caratteristico dell'epoca attuale. Internet, il web 2.0, i servizi *overthetop* e le tecnologie connesse hanno fatto emergere, accanto a straordinarie potenzialità, nuove questioni legate alla protezione dell'intimità, della riservatezza e della capacità auto determinativa dei singoli individui[2].

L'enorme quantità di dati personali generati e diffusi tramite tali strumenti, unita all'accresciuta capacità di "archiviarli", "organizzarli" e "correlarli", traendo dai medesimi, anche attraverso l'intelligenza artificiale, nuovi dati e nuove informazioni, consente, infatti, una profilazione assai precisa tanto dei singoli individui quanto dei gruppi sociali[3]. Profilare significa ricostruire l'altrui identità, conoscere una persona, le sue abitudini, le sue opinioni e i suoi desideri. Come è intuitivo, questa conoscenza dettagliata è certamente un valore che può essere utilizzato per svolgere una pluralità di attività di tipo economico, sociale e politico. Inoltre, il trattamento dati e la profilazione può essere utilizzata dai pubblici poteri per la prevenzione, l'accertamento e la persecuzione di

[1] Si v. nella dottrina italiana, L. Califano, *Privacy e sicurezza,* in *Democrazia e sicurezza*, 3, 2013; F. Clementi – G. Tiberi, *Sicurezza interna, diritti e cooperazione internazionale nella lotta al terrorismo: i casi PNR e Swift*, in www.astrid-online.it, 1, 2013; P. Costanzo, *Videosorveglianza e Internet*, in M. Manetti - R. Borrello (a cura di), *Videosorveglianza e privacy*, Firenze, 2010; M. Rubechi, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze e vecchie questioni* (*a un anno dagli attacchi di Parigi*), in www.federalismi.it, 23, 2016; L. Scaffardi, *Nuove tecnologie, prevenzione del crimine e privacy, alla ricerca di un difficile bilanciamento* e A. Pace, *Libertà e sicurezza. Cinquant'anni dopo*, entrambi in A. Torre (a cura di), *Costituzioni e sicurezza dello Stato*, Rimini, 2013, rispettivamente 425 ss. e 547 ss.

[2] P. Passaglia, *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in *Consulta OnLine*, 3, 2016, 332 ss.

[3] L'evoluzione dell'Intelligenza Artificiale (IA) pone tutta una serie di questioni nuove in materia di protezione dei dati. V. in proposito il recente volume di F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018 ed ivi in particolare la prima parte dell'A. e nella seconda parte i contributi di G. D'Acquisto, *Qualità dei dati e Intelligenza artificiale: intelligenza dai dati e intelligenza dei dati*, 265 ss.; M. Bassini - L. Liguori - O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi*, 333 ss.; R. Bifulco, *Intelligenza artificiale e ordine spontaneo*, 383 ss.

reati.

Allo stesso tempo la disponibilità di una tale mole di dati riguardanti singoli individui rappresenta un rischio perché essi si prestano anche ad essere utilizzati per molte attività illecite, se non addirittura criminali.

Gli esempi che possono farsi sono innumerevoli e tra di loro molto differenti.

Si può pensare alla profilazione del consumatore per la vendita di prodotti a distanza partendo dal tracciamento dei siti Internet visitati o dalle ricerche effettuate tramite i motori di ricerca, alla diffusione delle *app* per la videosorveglianza via web, alla videosorveglianza professionale arricchita da tecniche di riconoscimento e di allerta, ai programmi di captazione informatica ormai facilmente installabili senza alcuna particolare capacità informatica, ai *software* per perpetrare frodi informatiche o anche ad attività molto più complesse quali l'analisi su larga scala di dati (e comportamenti) – come avveniva nel programma PRISM dell'*intelligence* americana – per attività di sorveglianza globale finalizzate a minimizzare i rischi per la sicurezza pubblica e nazionale.

Proprio le polemiche seguite alla rivelazione del programma PRISM, ma identiche osservazioni possono farsi per tante altre attività molto meno sofisticate seppur aventi un impatto quotidiano sulla vita delle persone, hanno spinto alcuni studiosi a leggere la contrapposizione tra *privacy* – da intendersi per ora nel senso molto ampio di protezione dell'intimità, della riservatezza e dell'autodeterminazione – e sicurezza come la spia di una nuova stagione di contrapposizione tra libertà ed autorità, capace di rimettere in discussione gli equilibri su cui si fondano le società liberal-democratiche e di cui le Costituzioni contemporanee sono, al tempo stesso, specchio e garanzia[4].

Un secondo fattore, più contingente, ma altrettanto rilevante, che ha contribuito a polarizzare il dibattito e, in questo caso, a semplificarlo nella opposizione "sicurezza vs. *privacy*", è legato evidentemente alla generalizzata percezione individuale di un aumentato rischio per la propria sicurezza individuale. Questo è il risultato inevitabile del terrorismo internazione e, in particolare, dei ripetuti attacchi di matrice islamista verificatisi in diversi Paesi europei[5]. Anche gli ingenti fenomeni migratori legati alle guerre all'ISIS in Nord-Africa, in Siria ed in Iraq e la paura che tra i migranti vi siano *foreign fighters* di ritorno dalle zone di guerra contribuiscono a diffondere nella società paura e preoccupazione per la propria sicurezza. Come conseguenza dei diversi attacchi terroristici, tutti i Paesi europei hanno progressivamente aumentato il livello di controllo e

[4] Cfr. F. Pizzetti, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in www.federalismi.it, 13, 2013 A. Rinella, *Walls and Fences. Muri e barriere tra sicurezza nazionale e libertà*, in A. Torre (a cura di), *Costituzioni e sicurezza dello Stato. Profili di diritto costituzionale comparato*, cit., 357 ss.

[5] Il tema del bilanciamento tra libertà e sicurezza, con particolare riferimento alle emergenze terroristiche, è stato ampiamente studiato nella dottrina italiana. Sia consentito ricordare, tra i molti, gli atti del Convegno AIC, *Liberta' e sicurezza nelle democrazie contemporanee: atti del 18. Convegno annuale, Bari, 17-18 ottobre 2003: annuario 2003*, Padova, 2007 i volumi collettanei di M. Dogliani - S. Sicardi (a cura di), *Diritti umani e uso della forza*, Torino, 1999, P. Carnevale (a cura di), *Guerra e Costituzione*, Torino, 2004; T. Groppi (a cura di), *Democrazia e terrorismo*, Napoli, 2006; M. Cavino - M.G. Losano - C. Tripodina (a cura di), *Lotta al terrorismo e tutela dei diritti fondamentali*, Torino, 2009; nonché i lavori monografici di G. De Vergottini, *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, Bologna, 2004; V. Baldini, *Sicurezza e libertà nello Stato di diritto in trasformazione. Problematiche costituzionali delle discipline di lotta al terrorismo internazionale*, Torino, 2004; P, Bonetti, *Terrorismo, emergenza e costituzioni democratiche*, Bologna, 2006; C. Bassu, *Terrorismo e costituzionalismo. Percorsi comparati*, Torino, 2010. V. recentemente G. De Minico, *Costituzione. Emergenza e terrorismo*, Napoli, 2016, spec. 205 ss.

di monitoraggio, facendo ormai largo ricorso a tecniche investigative sul web[6].

Alcune forze politiche, nei diversi Paesi europei, cercando di interpretare la richiesta sociale di maggiore sicurezza hanno utilizzato accenti talvolta così forti nella richiesta di controlli capillari, da far apparire la protezione dei dati come un orpello e il sacrificio della *privacy* come un prezzo davvero minimo per garantire sicurezza.

Questo approccio, indipendentemente da ogni giudizio politico che può darsi su questa strategia, dimostra una conoscenza assai parziale di quale sia il contenuto dei diritti di protezione dati e, più ampiamente, di quali obiettivi intendano perseguire le norme in materia.

Il titolo di questo contributo rende manifesto lo scopo dell'indagine, ossia dimostrare che la contrapposizione tra diritto alla protezione dei dati personali e sicurezza è assai sovrastimata e che la scelta, talvolta presentata come ineludibile, tra il soddisfacimento del diritto individuale alla protezione dei propri dati personali o della sicurezza dello Stato e degli individui è, in realtà, una semplificazione che non tiene conto dell'ampiezza delle possibili declinazioni tanto della protezione dati quanto della sicurezza[7].

Infatti, come si vedrà nei paragrafi che seguiranno, la stessa qualificazione dell'una, la protezione dei dati, come diritto individuale e dell'altra, la sicurezza, come interesse collettivo, coglie infatti solo uno dei possibili profili di riflessione.

Occorre infatti considerare che la protezione dei dati personali è espressamente qualificata, nel recente Regolamento 2016/679, non solo più come un diritto individuale, ma pure come un interesse pubblico rilevante per le società contemporanee, una garanzia per la loro democraticità e per il loro buon funzionamento[8].

D'altra parte, anche la sicurezza può essere letta non solo come interesse collettivo ma pure come valore superprimario e come diritto individuale. Una prospettiva questa, propria del contrattualismo, che alcuni studiosi hanno riportato a galla, riaprendo così

[6] V. A. Spataro *Sicurezza e politiche antiterrorismo*, in G. Cocco (a cura di), *I diversi volti della sicurezza. Atti del Convegno (Milano, 4 giugno 2009)*, Milano, 2012, 87 ss. nonché recentemente M. Rubechi, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze e vecchie questioni (a un anno dagli attacchi di Parigi*), cit. V. anche, G. de Minico, *Antiche libertà e nuove frontiere digitali*, Torino, 2016, 131 ss.

[7] In proposito v. L. Califano, *Privacy e sicurezza*, cit. 19. V. inoltre sull'ampiezza del significato di sicurezza K. Mavrias, *La sicurezza: un concetto polisemico*, in A. Torre (a cura di), *Costituzioni e sicurezza dello Stato*, cit, 457 ss.; sulla pluralità di usi del termine sicurezza nella Costituzione italiana M. Dogliani, *Il volto costituzionale della sicurezza*, in G. Cocco (a cura di), *I diversi volti della sicurezza. Atti del Convegno (Milano, 4 giugno 2009)*, Milano, 2012, 1 ss.

[8] Molto interessante è anche la tesi di chi guarda alla non diffusione di dati relativi alla persona dal punto di vista dei doveri. V. sul punto le osservazioni di A. Ruggeri, *Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni*), in *Consulta OnLine*, 3, 2016, 371 ss. spec. 372

un dibattito storico e suscitando un nuovo proficuo confronto tra le diverse posizioni[9].

2. I bisogni ancestrali dell'uomo e la loro traduzione giuridica

Secondo la nota classificazione dello studioso Abraham Maslow, iniziatore della psicologia umanistica, ogni uomo ha esigenze psico-biologiche irrinunciabili che vanno soddisfatte al fine di sopravvivere, crescere, esprimere la propria personalità, realizzare le proprie scelte[10].

Tali bisogni sono raggruppati da Maslow in cinque categorie e disposti come in una piramide, secondo una gerarchia biologica ed esistenziale. Occorre avvertire che i bisogni individuati non sono però isolati o a sé stanti, ma al contrario pur potendosi disporre secondo una gerarchia di dominanza e di importanza, essi sono interdipendenti.

Il punto di partenza è che ogni persona ha un potenziale, un principio di autorealizzazione da cui promanano le motivazioni interiori e i desideri profondi. I bisogni "superiori", quelli collocati sulla punta della piramide possono realizzarsi solo se la realtà consente di soddisfare i bisogni "inferiori". D'altra parte, il pieno soddisfacimento e appagamento di un bisogno "inferiore" non fa venir meno la tensione naturale dell'uomo verso la soddisfazione di tutti i bisogni "superiori".

I bisogni inferiori o primari sono dunque quelli propriamente fisiologici, alla cui base c'è l'istinto di sopravvivenza, e i bisogni di sicurezza legati al desiderio di protezione e di tranquillità. Salendo la piramide si incontrano i bisogni di appartenenza ad un gruppo e i bisogni di stima da intendersi nel duplice senso di stima da parte degli altri e di autostima. Infine, all'ultimo gradino, vi sono i bisogni di autorealizzazione, legati al desiderio di "voler essere" in base alle proprie aspirazioni e ai propri talenti.

---

[9] V. nel senso di considerare la sicurezza come un valore superprimario G. Cerrina Feroni - G. Morbidelli, *La sicurezza: un valore superprimario*, in *Percorsi costituzionali*, 1, 2008 17; T.E. Frosini, *Il diritto costituzionale alla sicurezza*, in www.forumcostituzionale.it. Di diritto individuale dei cittadini parlano, con sfumature differenti, G. De Vergottini, *Il bilanciamento tra sicurezza e libertà civili nella stagione del terrorismo*, in AA.VV., *Sicurezza: le nuove frontiere*, 2005, 110; P. Torretta, *"Diritto alla sicurezza" e altri diritti e libertà della persona: un complesso bilanciamento costituzionale*, in A. D'Aloia (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Milano, 2003, 451 ss.; S. Raimondi, *Per l'affermazione della sicurezza pubblica come diritto*, in *Diritto amministrativo.*, 4, 2006, 747 ss. Tra gli A. decisamente contrari all'impostazione della sicurezza come diritto individuale, v. M. Ruotolo, *La sicurezza nel gioco del bilanciamento*, in G. Cocco (a cura di), *I diversi volti della sicurezza*, cit., 18 ss., nonché, Id., *Diritto alla sicurezza e sicurezza dei diritti*, in *Democrazia e Sicurezza*, 2, 2013; T.F. Giupponi, *Contro il "diritto alla sicurezza". Immigrazione, sicurezza e autonomie territoriali nella più recente giurisprudenza della Corte costituzionale*, in AA.VV., *Studi in onore di Giuseppe de Vergottini*, I, Padova, 2015, 719 ss. Per una definizione di sicurezza di carattere restrittivo, vale a dire limitata solo al suo tradizionale profilo preventivo e repressivo e, dunque, intesa nel senso di garanzia dell'ordine pubblico e come una ragione di limiti ai diritti cfr., M. Rubechi, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze e vecchie questioni (a un anno dagli attacchi di Parigi)*, cit. Per l'inesistenza di un diritto individuale alla sicurezza si esprime anche T. Fenucci, *Quanto spazio c'è per un diritto individuale alla sicurezza nell'ordinamento costituzionale italiano? Brevi osservazioni*, in www.federalismi.it, 22, 2015.

[10] Nella psicologia il bisogno è la mancanza totale o parziale di uno o più elementi che costituiscono il benessere della persona. Cfr. A. Marlow, *Motivation and Personality,* 1954, trad. it., *Motivazione e Personalità*, 1954.

Non ad ogni bisogno umano può dirsi automaticamente corrispondere un diritto[11]. Persino i diritti umani che corrispondono spesso a "bisogni primari" dell'uomo sono nella loro configurazione giuridica "diritti storici cioè nati in certe circostanze". Questo significa che il loro riconoscimento e la loro ampiezza non è immutabile posto che i diversi fattori storici, politici, sociali ed economici sono capaci di rinnovarli continuamente[12].

3. Diritto individuale alla sicurezza e interesse costituzionale alla sicurezza

Il desiderio di sicurezza quale riflesso dell'istinto vitale e quale aspirazione ad una vita protetta dalle intemperie, dai nemici e dai pericoli è certamente un bisogno primario o "inferiore" dell'uomo che egli tende naturalmente a soddisfare in parte unendosi ad altri uomini, formando cioè comunità e, in parte, nascondendosi, per proteggersi da qualcosa o da qualcuno che lo porrebbe in una situazione di rischio[13].
Se è permesso l'ardire di transitare dalla psicologia al diritto, l'istinto di sopravvivenza ed il bisogno di sicurezza di cui parla Maslow non sono cosa diversa dalla *ratio naturalis*, la ragione naturale, che nel pensiero di Hobbes suggerisce a ciascuno il modo migliore

[11] Anche se sul piano ideale si concorda con A. Ruggeri, *Cosa sono i diritti fondamentali e da chi e come se ne può avere il riconoscimento e la tutela*, 2016, p. 2, laddove l'A. afferma che sono innanzitutto i bisogni elementari di ciascun essere umano senza il cui riconoscimento e l'effettiva tutela non potrebbe aversi un'esistenza libera e dignitosa.

[12] V. sul punto N. Bobbio, *L'età dei diritti*, Einaudi, Torino, 1990.

[13] In questo senso I. Kant (*Idea per una storia universale dal punto di vista cosmopolitico*, 1784, in *Scritti politici e di filosofia della storia e del diritto*, Torino, 1956, 127) per cui «l'uomo ha un'inclinazione ad associarsi perché egli in tale stato si sente maggiormente uomo, cioè sente di poter meglio sviluppare le sue naturali disposizioni. Ma egli ha anche una forte tendenza a dissociarsi, perché ha del pari in sé la qualità antisociale di voler tutto rivolgere solo al proprio interesse, per cui si aspetta resistenza da ogni parte e sa che egli deve da parte sua tendere a resistere contro gli altri».
Il dibattito sulla socialità dell'uomo e sulla questione se essa sia un istinto primario o il risultato di altre esigenze è tanto antico quanto ancora attuale. Come non ricordare Aristotele nella *Politica* (libro I) in cui l'uomo è definito «essere sociale-politico per natura» incapace di vivere isolato dagli altri. La necessità di associarsi non è determinata solo da bisogni materiali (come la difesa personale, il procurarsi nutrimento e garantire la procreazione ecc.), ma soprattutto, dal fatto che fuori dalla comunità l'uomo non potrebbe sviluppare ed esercitare la ragione ossia realizzare la sua più intima natura. Di questa impostazione si trovano i segni nel 'cosmopolitismo' (inteso come la comunità dell'intero genere umano) stoico e in Cicerone (*De finibus*, IV, 2, 4) che pure dissocia l'aspetto sociale da quello statuale. L'impostazione aristotelica prosegue nel pensiero di Grozio (*De iure belli ac pacis,* 1625*, Prolegomeni)* per cui l'uomo è «per natura» un essere razionale e sociale, cioè atto a vivere in società purché essa sia organizzata, in modo razionale. La critica più forte a tale impostazione è stata storicamente quella di Hobbes che nel *De cive* (1641) confuta la tesi dell'uomo socievole per natura, affermando che egli lo diventa solo in seguito a un ragionamento e a un calcolo di vantaggi. Anche per Rousseau (*Discorso sull'origine della disuguaglianza*, 1754) l'uomo naturale è una creatura solitaria e solo il bisogno lo spinge a cercare gli altri e a diventare un essere socievole e razionale, capace di linguaggio. Un secolo più tardi gli studi di Darwin (*L'origine dell'uomo*, 1871) sembrano offrire un punto che sembra essere di convergenza (se è lecito l'ardire) tra l'ipotesi aristotelica della socialità naturale e quelle della socialità derivata laddove il padre dell'evoluzionismo sostiene che vi sia un sentimento di "simpatia" degli animali (e dunque dell'uomo) nei confronti della propria specie, una sorta di disposizione generale alla socievolezza che però evolve sulla base dei condizionamenti della società sull'individuo.

per evitare la morte e sopravvivere[14].

Non può dunque stupire che la dottrina dello Stato di Hobbes sia tutta fondata sulla ricerca della sopravvivenza e sul valore intrinseco della sicurezza. Nel Leviatano, gli uomini escono, infatti, dallo stato di natura grazie alla *ratio naturalis*, e per far cessare l'aggressione reciproca si accordano per limitare la loro *cupiditas naturalis*, quel naturale desiderio di fruire dei beni del mondo anche attraverso la violenza.

Il patto associativo non è, tuttavia, sufficiente perché i contraenti non sono in grado di garantirsi reciprocamente. Per questo interviene il *pactum subiectionis* con cui gli individui si assoggettano a un potere sovrano, attraverso la costituzione di un ordinamento statale capace di obbligare le condotte già concordate e pattuite.

Gli individui trasferiscono i propri diritti naturali a un soggetto che abbia la forza necessaria per contrastare chiunque voglia infrangere la pace dello Stato. Questo soggetto è, nella ricostruzione di Hobbes, il sovrano che è titolare di un potere assoluto al di sopra delle parti, e che non avendo stipulato il patto non è, quindi, nemmeno limitato da esso. L'unico diritto che però gli uomini non trasferiscono è il diritto alla vita. L'unico obbligo che il potere sovrano ha nei confronti dei sudditi è proprio quello di garantire loro la vita e la sicurezza.

Come è evidente, la sicurezza degli individui è da principio un diritto individuale.

Esso può essere considerato un interesse collettivo nella misura in cui dalla sicurezza dello Stato, inteso come ordine costituito, dipenda la pace e il non precipitare, citando nuovamente Hobbes, nello stato di natura e, quindi, nel regno della *cupiditas naturalis*.

Pur con tutte le differenze legate alla diversa prospettiva, l'idea che esista ontologicamente prima un diritto individuale alla sicurezza e solo poi, in sua funzione, un interesse collettivo alla sicurezza dello Stato è condivisa tanto da Locke quanto, con accenti un poco diversi, da Montesquieu.

Il primo, Locke, condivide con Hobbes, l'idea che il sovrano (che per Locke è lo Stato) sia garante della pace e della sicurezza dei cittadini, ma aggiunge che il medesimo costituisce anche un pericolo per le libertà del cittadino, che, come noto, nella ricostruzione del filosofo inglese non si annullano né si trasferiscono ma che, invece, esistono prima dello Stato, permangono in capo ai cittadini e sono garantite dal contratto sociale[15].

Per Montesquieu, invece, la sicurezza coincide con la libertà politica. Quest'ultima libertà intesa come sicurezza psicologica esiste solo laddove non c'è abuso di potere. Per questo essa diviene anche sicurezza giuridica ossia osservanza dei principi fondamentali dello stato di diritto, con particolare riferimento alle garanzie procedimentali per l'applicazione delle leggi[16]. In altri termini, la sicurezza individuale è il prerequisito per il godimento degli altri diritti.

Non può stupire, date queste premesse, che le prime codificazioni dei diritti fondamentali collocassero tutte il diritto alla sicurezza tra i diritti innati dell'uomo. Tra di esse merita citare, da un lato, la Dichiarazione dei diritti dell'uomo e del cittadino del 1789 che nell'art. 2 perentoriamente afferma che «Il fine di ogni associazione politica è la conservazione dei diritti naturali ed imprescrittibili dell'uomo. Questi diritti sono la

[14] T. Hobbes, *Leviatano*, 1651.

[15] J. Locke, *Secondo trattato sul governo*, 1689.

[16] Montesquieu, *Lo spirito delle leggi*, 1748, spec. libro XI e libro XII.

libertà, la sicurezza e la resistenza»; e dall'altro la Dichiarazione dei diritti della Virginia che tra i diritti inalienabili dell'uomo pone accanto alla ricerca ed al conseguimento della felicità proprio la sicurezza[17].

Negli ordinamenti costituzionali contemporanei la qualificazione della sicurezza come diritto individuale è divenuta residuale. Nonostante alcune carte costituzionali ed anche la Carta dei diritti fondamentali dell'Unione europea contengano riferimenti espliciti al diritto alla sicurezza[18], ragioni di realismo politico connesse sia con la constatazione che gli ordinamenti liberal-democratici garantiscano standard di sicurezza personale ben più elevati rispetto agli ordinamenti ottocenteschi in cui il diritto individuale era stato affermato, sia con la difficoltà di immaginare la giustiziabilità di tale diritto[19], hanno portato a ritenere che la sicurezza individuale consista nella contestuale e complessiva tutela dei beni costituzionali o, con formula maggiormente evocativa, con la sicurezza dei diritti[20].

Questo naturalmente rompe il nesso tra sicurezza e coercizione (sicurezza come fine idoneo a limitare i diritti fondamentali) ed apre alla garanzia della sicurezza individuale attraverso azioni a sostegno del godimento effettivo dei diritti costituzionalmente protetti[21].

Tale impostazione, tuttavia, può reggere, per le medesime ragioni di realismo politico, da cui essa genera, fin tanto che la percezione di insicurezza non si diffonde al punto da mettere a rischio la tenuta della comunità[22]. La percezione soggettiva di sicurezza è dunque, da un lato, residuale rispetto agli altri beni costituzionalmente tutelati[23], da un altro lato, però è la ragion d'essere che tiene insieme una comunità[24]. Se la percezione soggettiva di sicurezza dei consociati crolla nel senso che lo Stato è percepito come non in grado di garantirla, riemerge naturalmente il bisogno individuale di sicurezza che è autonomo, e potenzialmente anche in contraddizione, rispetto ai bisogni corrispondenti ad altri beni costituzionalmente tutelati.

A fronte dell'affievolimento del diritto alla sicurezza come diritto individuale, nel co-

[17] V. anche l'accento fortissimo posto sulla sicurezza posto dalla Dichiarazione d'indipendenza americana, proprio laddove si afferma «che ogni qualvolta una forma di governo diviene antagonistica al conseguimento di questi scopi, il popolo ha diritto di modificarla e abolirla, e di creare un governo nuovo, ponendo a base di esso quei principi, e regolando i poteri di esso in quelle forme che offrono la maggiore probabilità di condurre alla sicurezza ed alla felicità del popolo medesimo».

[18] V. in questo senso l'art. 5 della CEDU, l'art. 6 della Carta dei diritti fondamentali dell'UE che afferma in modo perentorio, ma senza provvedere a definire gli ambiti della prescrizione che «ogni persona ha diritto alla libertà e alla sicurezza», l'art. 27 della Costituzione portoghese, l'art. 17 della Cost. spagnola. Sulla portata di tali norme nel senso che esse non definirebbero un diritto individuale v. A. Pace, *Libertà e sicurezza. Cinquant'anni dopo*, in A. Torre (a cura di), *Costituzioni e sicurezza dello Stato*, cit., 544.

[19] A. Pace, *Libertà e sicurezza. Cinquant'anni dopo*, cit., 547-548.

[20] In questo senso v. M. Ruotolo, *Diritto alla sicurezza e sicurezza dei diritti,* cit., 4 s.; di complessiva tutela dei beni costituzionali parla M. Dogliani, *Il volto costituzionale della sicurezza*, in G. Cocco (a cura di), *I diversi volti della sicurezza*, Milano, 2012, 1 ss.

[21] M. Dogliani, *Il volto costituzionale della sicurezza,* cit., 5.

[22] In questo senso, essa potrebbe essere considerato un "valore superprimario", cfr. G. Cerrina Feroni – G. Morbidelli, *La sicurezza: un valore superprimario*, cit. V. sulla questione anche T.E. Frosini, *Il diritto costituzionale alla sicurezza*, in www.forumcostituzionale.it.

[23] M. Dogliani, *Il volto costituzionale della sicurezza*, cit., 6.

[24] *Ibidem*, 8 ss."

stituzionalismo contemporaneo di matrice liberal-democratica si è molto rafforzato il profilo della sicurezza come interesse collettivo alla tenuta complessiva dello Stato di diritto. Per cui, nelle Costituzioni attuali si riconosce il valore costituzionale della sicurezza dello Stato, della sicurezza nazionale, dell'incolumità pubblica, dell'ordine pubblico[25]. Tali interessi e fini costituzionalmente rilevanti si affermano nella giurisprudenza costituzionale – e in quella delle Corti internazionali dei diritti – come cause legittime di restrizione dei diritti individuali[26].

Questo naturalmente nel rispetto di rigide regole formali, tra cui, spesso a tutela dei diritti inviolabili, la riserva di legge, la riserva di giurisdizione, l'obbligo di motivazione, e di regole sostanziali consistenti, a seconda della diversa terminologia e concettualità utilizzata dalle Corti nazionali ed europee, nel principio del bilanciamento o di contestuale tutela dei beni costituzionalmente rilevanti, nel limite del contenuto minimo o essenziale del diritto fondamentale, nel principio di proporzionalità o di ragionevolezza.

4. La lunga marcia del diritto alla riservatezza e il riconoscimento del *Right to privacy*

Anche l'esigenza di riservatezza intesa come riserbo nel palesare i propri sentimenti, il proprio pensiero, la propria intimità fisica rappresenta un bisogno dell'essere umano. Pur non potendo essere probabilmente collocata, riprendendo la piramide di Marlow, tra i bisogni fisiologici dell'uomo, se non in chiave servente rispetto all'esigenza di nascondersi per soddisfare l'istinto di sopravvivenza laddove si ravvisi una situazione di rischio, essa informa di sé i bisogni di sicurezza, di appartenenza, di stima e di autorealizzazione.

Essa è, infatti, connaturata alla consapevolezza che l'uomo ha di sé stesso e della propria storicità, alla sua socialità ed alla capacità di reagire ai fatti naturali che si susseguono, in modo non solo istintivo, ma esaminando le conseguenze delle diverse possibili azioni e reazioni.

La contezza di sé e la propria storicità sono *mutatis mutandis* l'albero della conoscenza e la conoscenza del bene e del male del passo della Genesi in cui, Adamo ed Eva, mangiato il frutto proibito aprirono gli occhi e si accorsero di essere nudi. Per questo intrecciarono foglie di fico e se ne fecero cinture. Udito, però, il passo di Dio si nascosero ed alla sua chiamata risposero che si erano nascosti avendo avuto paura in quanto

[25] Le espressioni utilizzate non sono sinonimi. Nella Costituzione italiana esse vengono utilizzate in contesti diversi e con diversa portata. Sui diversi usi del termine sicurezza, per tutti, M. Dogliani, *Il volto costituzionale della sicurezza*, cit., *passim*; M. Ruotolo, *La sicurezza nel gioco del bilanciamento*, cit.; T.F. Giupponi, *La sicurezza e le sue "dimensioni" costituzionali* in AA.VV., *Diritti umani: trasformazioni e reazioni*, Bologna, 2008, 275 ss.

[26] V. ad esempio le sentenze della Corte costituzionale 14 aprile 1976, n. 82 e 13 aprile 1977, n. 82 in cui la sicurezza nazionale è qualificata «come interesse preminente tra quelli previsti in Costituzione» e in cui «i problemi di sicurezza nazionale sono al vertice delle attività di carattere pubblico».

nudi[27].

Conoscenza del bene e del male, nudità e paura sono, dunque, il fondamento del bisogno di celarsi e di proteggere la propria intimità sia di fronte al Signore, come nel passo biblico, sia di fronte a chiunque altro, come dimostra il fatto che Adamo ed Eva cacciati dal giardino terrestre ricevettero tuniche di pelle per coprirsi.

Se il bisogno di proteggere la propria intimità è antico come l'uomo, i suoi confini, la sua intensità, il suo impatto sui bisogni superiori di appartenenza, di autostima e di autorealizzazione variano nel tempo, mutando a seconda del contesto storico e sociale in cui l'essere umano si colloca nonché a seconda degli strumenti e delle tecnologie disponibili per scoprire ciò che si vorrebbe celare.

Nell'antica Grecia, per fare un esempio, l'esigenza di una sfera privata era riconosciuta in un ambito strettamente limitato ai propri bisogni e alle proprie necessità. La sfera pubblica, annessa all'attività politica, era largamente preponderante e il fatto di condurre, in quella società, una vita ritirata o spesa fuori dal mondo acquisiva una connotazione negativa, quasi antisociale[28].

Nel Medioevo, il concetto di riservatezza era, se possibile, ancora più aleatorio.

Per i legami interpersonali e di comunità tipici del sistema feudale, sia nelle campagne sia nei borghi, la ricerca di intimità e riservatezza era vista con sospetto. Anche la sfera privata della riservatezza familiare tendeva a sfumare perché le diverse famiglie erano legate tra loro[29]. Più che di una riservatezza individuale o familiare si poteva, dunque, discorrere della riservatezza di un gruppo sociale rispetto ad un altro[30]. Il profilo collettivo tendeva a superare quello individuale, secondo un pendolo della storia che acquisisce oggi, come si vedrà, un nuovo significato.

Con l'avvento dello Stato moderno, il bisogno di proteggere la propria intimità acquisisce una nuova profondità.

La maggiore separazione tra pubblico e privato e, soprattutto, le discriminazioni religiose che seguono la fine dell'unità religiosa conducono, da un lato, a reindividualizzare l'aspirazione a proteggere la propria intimità e, da un altro lato, a far emergere il legame strettissimo tra l'aspirazione a proteggere la propria riservatezza ed il timore di vederla violata per i rischi connessi con lo svelamento delle proprie convinzioni più intime.

Proprio questo legame non verrà più meno ed anzi riemergerà ciclicamente e tristemente in tutti i casi in cui la storia è stata testimone di violenze e persecuzioni sulla base delle convinzioni più intime degli individui: quelle religiose, filosofiche e politiche.

Da questo punto di vista, può quindi dirsi che sicurezza e riservatezza, fin dalla loro emersione, siano due esigenze tra loro intimamente connesse. La paura di subire violenza è il presupposto primo diretto ed indiretto di entrambi i bisogni. Se però comune è il fondamento naturale dell'esigenza di riservatezza e di sicurezza molto diversa è

---

[27] Bibbia, Antico Testamento, Genesi, 3. Il medesimo passo è poi ripreso nel Corano, nella sura "I Lembi" in cui la nudità diventa vergogna «nel momento in cui l'uomo perde la sua primitiva innocenza» Corano Sura VII Al-A'rȃf.

[28] Cfr. S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, 3.

[29] M. Iaselli - S. Gorla, *Storia della privacy*, Roma, 2015, 9 ss.

[30] S. Rodotà, *La privacy tra individuo e collettività*, in *Politica del Diritto*, 1974, 545 ss., 551.

stata nel tempo la loro traduzione giuridica.
Per quanto riguarda il riconoscimento giuridico di una sfera privata intangibile, esso è stato assolutamente recente e non uniforme nei diversi ordinamenti giuridici[31].
Tacendo dei sistemi autoritari, laddove tale sfera di protezione della persona umana non è mai realmente garantita, esistono corpose differenze anche tra i Paesi liberal-democratici.
Il dato comune è che, inizialmente, il riconoscimento giuridico di una sfera privata intangibile è stato parcellizzato nei diversi ambiti della protezione della libertà fisica, del domicilio, della segretezza della corrispondenza, della libertà di associazione e della libertà di espressione. Solo in un secondo momento, il diritto alla riservatezza ha assunto una propria autonomia concettuale e un proprio autonomo riconoscimento, anche di rango costituzionale.
La prima teorizzazione dottrinale unitaria del diritto alla riservatezza, declinato come diritto alla *privacy*, è avvenuta, come noto, grazie a un saggio di Samuel D. Warren e Louis D. Brandeis nel 1890[32]. Non è un caso che ciò sia avvenuto negli Stati Uniti d'America e proprio al termine del secolo decimo nono, in una fase in cui la rivoluzione industriale e la forte innovazione tecnologica nel settore dell'informazione consolidarono, infatti, il legame originario tra il desiderio di intimità e la paura che essa potesse essere violata[33].
Il merito storico più evidente dell'opera di Warren e Brandeis è proprio il tentativo di ricostruire il diritto alla *privacy* come fattispecie giuridica autonoma, non più esclusivamente legata al diritto di proprietà né coincidente con il diritto alla riservatezza delle comunicazioni interpersonali[34]. Per far questo i due autori richiamano tutta una serie di pronunce giurisprudenziali che, in modo più o meno estemporaneo, si erano già riferite, in ambito civile, al diritto di essere lasciati soli[35].
Il saggio di Warren e Brandeis fa, dunque, emergere, come dietro la giurisprudenza americana che si era occupata essenzialmente di identificare le diverse tipologie di illecito civile connesse con la riservatezza (*intrusion upon seclusion, public disclosure of private facts, false light in public eye* e *appropriation),* vi fosse un diritto fondamentale autonomo che gli autori definiscono come *right to privacy*[36].
Dal saggio di Warren e Brandeis all'affermazione, nell'ordinamento costituzionale statunitense, del *right to privacy* come diritto costituzionale trascorrono alcuni decenni e, solo dopo un lungo percorso, la Corte Suprema provvede a tale riconoscimento.

---

[31] Con specifico riferimento alla *privacy*, cfr. V. Frosini, *La protezione della riservatezza nella società informatica*, in *Informatica e diritto*, 1981, 10.

[32] S. Warren-L.D. Brandeis, *The right of privacy*, in *Harvard Law Review*, 4, 1890, 193 ss.

[33] V. in proposito l'affresco di A. Baldassarre, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974, 17 ss.

[34] A. Baldassarre, *Privacy e Costituzione. L'esperienza statunitense*, cit., 45 e 52.

[35] In dottrina, cfr T.M. Cooley, *The elements of tort*, Chicago, 1878, 2 ed., 1895, 9. Per una ricostruzione dei precedenti v. S. Warren-L.D. Brandeis, *The right of privacy,* cit.

[36] Le quattro fattispecie possono essere così tradotte: intrusione negli affari privati di una persona, pubblicazione di fatti privati, divulgazione di notizie atte a porre una persona in una falsa luce agli occhi del pubblico, appropriazione del nome o dell'immagine di altra persona. Questa storica quadripartizione è proposta da W. Prosser, *Privacy*, in *Californian Law Review*, 48, 1960, 383.

Questo avviene compiutamente nella sentenza *Kats v. United States* del 1967 in cui la Corte ritiene illegittima l'assunzione e l'utilizzo di prove procurate dal FBI, senza una previa autorizzazione del giudice, tramite un registratore posto dentro una cabina telefonica solitamente utilizzata dall'indagato[37].

Per giungere a questa conclusione, la Corte Suprema compie alcune affermazioni che possono definirsi storiche e che sono ancora oggi alla base del riconoscimento costituzionale del *right to privacy* nonché principi di riferimento per il modello americano di tutela della *privacy* sia a livello federale che a livello degli Stati.

Primo, la Corte offre una lettura evolutiva, e non più solo testuale, del quarto emendamento della Costituzione americana affermando che esso non protegge solo il domicilio, la corrispondenza, la persona fisica, ma anche la *privacy* dell'individuo contro taluni tipi di intrusione del governo.

In secondo luogo, chiarisce, da un lato, che il quarto emendamento non può essere interamente ridotto al diritto alla *privacy*, e da un altro lato, che il diritto alla *privacy* trova fondamento anche in altre norme costituzionali. In particolare, la Corte osserva che una protezione della *privacy* può essere trovata nell'interpretazione del primo emendamento che vieta le limitazioni governative alla libertà di associazione e alla *privacy* dell'associazione stessa[38], nel divieto, di cui al terzo emendamento di acquartierare dei soldati in tempo di pace in case private senza il consenso dei proprietari e per alcuni aspetti anche nel quinto emendamento che tutela il diritto di ogni individuo a un enclave dove poter condurre una vita privata[39].

Infine, molto importante per il tema qui trattato, è il fatto che la Corte scelga di precisare, che non ogni azione governativa che interferisca con la *privacy* è illegittima, ma si tratta di valutare, caso per caso, se essa viola un divieto posto dalla Costituzione degli Stati Uniti oppure al contrario se essa sia legittima a tutela di un interesse costituzionalmente prevalente. Il ragionamento nella sua apparente banalità è in realtà importantissimo così come lo è il fatto che la Corte Suprema faccia proprio l'esempio della sicurezza nazionale che potrebbe, laddove vi fosse un rischio evidente, anche giustificare una compressione del diritto alla privacy [40].

Senza ora voler entrare nel dettaglio della questione, il pensiero non può che andare, da un lato, alla "vicenda Snowden" e, da un altro lato, alla vicenda che ha visto recentemente contrapposti Apple e FBI nel caso riguardante l'accesso all'I-Phone dei terroristi di San Bernardino. In entrambi i casi una riflessione sui limiti alla privacy nei casi in cui è in gioco la sicurezza nazionale, non può prescindere nell'ordinamento americano

---

[37] *Kats v. United States*, 389 U.S. 347 (1967).

[38] Nelle motivazioni la Corte Suprema richiama il precedente giurisprudenziale *NAACP v. Alabama*, 357 U.S. 449, 462 (1958).

[39] Cfr. sul punto il precedente richiamato *Teban v. Shott*, 382 U.S. 406, 416 (1966).

[40] Questo argomento oggi molto rilevante e centrale anche rispetto ad esempio alla vicenda dello scandalo NSA è sviluppato, con totale diversità di approdi, nell'opinione concorrente del Giudice White (*Kats v. United States*, 389 U.S. 347, 363 (1967) e in quella, anch'essa concorrente, dei Giudici Douglas e Brennan *(Kats v. United States*, 389 U.S. 347, 360 (1967). Il primo ricorda che, nel sistema americano, il Presidente, nei casi attinenti alla sicurezza nazionale, può autorizzare l'intercettazione anche al di fuori delle regole del IV emendamento. A tal proposito cita il precedente *Berger v. New York del 1967,* 388 U.S. 41. Il Giudice Douglas contesta tale possibilità e la sua legittimità costituzionale.

e da quanto affermato dalla Corte Suprema nella sua giurisprudenza[41].

5. La declinazione europea della protezione dei dati personali

La strada che porta all'affermazione costituzionale del diritto alla riservatezza nei Paesi europei è assai diversa[42].

Fino alla fine degli anni ottanta, i singoli Paesi procedono in ordine sparso. Laddove le Costituzioni nazionali dedicano norme *ad hoc* alla protezione della vita privata o alla riservatezza in senso proprio, il riconoscimento è evidentemente molto più agevole. Nei casi in cui, come in Italia, la Costituzione non contiene un'unica norma dedicata alla riservatezza, il percorso è stato più accidentato. Nel diritto alla riservatezza sono stati innanzitutto evidenziati due profili: quello di stampo liberale, consistente nella conoscenza esclusiva delle proprie vicende e quello dinamico consistente nell'interesse al controllo sui propri dati personali[43].

Il riconoscimento giuridico del primo profilo, dopo una giurisprudenza altalenante[44], è stato operato dai giudici comuni riconducendo il diritto alla riservatezza nella categoria dei diritti della personalità. La mancanza di una norma *ad hoc,* anche a livello codicistico, ha fatto sì che la dottrina e la giurisprudenza abbiano dovuto ricorrere a diverse disposizioni sparse nell'ordinamento e poste a protezione di aspetti parziali del riserbo ricorrendo all'analogia, nella duplice forma dell'analogia *legis* e dell'analogia *iuris*[45].

Il riconoscimento costituzionale del diritto alla riservatezza è stato fondato, da un lato, sull'assunto che l'art. 2 della Costituzione consente, ponendo la persona al centro dell'ordinamento, il riconoscimento di diritti anche al di fuori di quelli enunciati dal catalogo costituzionale; e da un altro lato, su una lettura congiunta degli artt. 13, 14, 15 e 21 Cost. che singolarmente tutelano e garantiscono profili diversi della riservatezza

[41] V. sul punto, Z. Bauman - D. Bigo - P. Esteves et al., *Repenser l'impact de la surveillance après l'affaire Snowden: sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance* in *Cultures & Conflits*, 2, 2015, 133 ss. Sia consentito il rinvio a M. Orofino, *FBI v. Apple: il caso è (forse) chiuso, ma le questioni di fondo rimangono apertissime*, in *Diritto Pubblico Comparato ed Europeo (DPCE online)*, 2, 2016.

[42] V. in proposito, U. Pagallo, *La tutela della privacy negli Stati Uniti d'America ed in Europa,* Milano, 2008.

[43] V. l'importante analisi dei due profili di S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973.

[44] V. in proposito G. Gardini, *Le regole dell'informazione. Principi giuridici, strumenti, casi*, Milano, 2005, 216-217.

[45] V. sul punto la pregevole ricostruzione, con completa bibliografia, di D. Caldirola, *Il diritto alla riservatezza*, Padova, 2006, 5-14.

degli individui[46].

A partire dall'inizio degli anni ottanta erompe sulla scena, prima grazie alla CEDU ed alla Corte di Strasburgo, e poi grazie all'Unione europea, il diritto europeo della protezione dei dati personali[47].

Esso, inizialmente, sembra tutelare solo quel profilo del diritto alla riservatezza connesso con il trattamento dei dati personali e, dunque, con il controllo dei propri dati[48]. La riservatezza intesa come conoscenza esclusiva delle proprie vicende sembra rimanere il profilo dominante e il suo riconoscimento rimesso ai singoli Stati.

L'evoluzione tecnologica rende però questa distinzione originaria sempre meno convincente. Ancorché rimangano oggi spazi per i legislatori nazionali, in particolar modo nel bilanciamento tra riservatezza e libertà di espressione e tra riservatezza e trasparenza, la capacità della normativa europea di offrire soluzioni e tutele sempre più forti ha capovolto l'iniziale rapporto. L'espansione del diritto alla protezione dati ha fatto il resto tanto che oggi possiamo affermare che il modello europeo di tutela della riservatezza coincide con la protezione dei dati, fermo restando che vi sono settori che la normativa europea rimette agli Stati, ma pur sempre all'interno del modello complessivo[49].

Con l'entrata in vigore del Trattato di Lisbona, e quindi della Carta dei diritti fondamentali dell'Unione europea, il diritto alla protezione dei dati personali è esplicitamente qualificato, *ex* art. 8[50], come autonomo diritto fondamentale[51].

La norma della Carta dei diritti fondamentali definisce chiaramente, partendo dalla legislazione vigente, ma non rinunciando ad apportare alcune innovazioni[52], l'ambito soggettivo del diritto che è qualificato come diritto dell'uomo e l'ambito oggettivo cioè il suo contenuto. Eventuali limitazioni a tale diritto, come ad ogni altro riconosciuto

---

[46] Così superando, in qualche modo, la storica contrapposizione sulla portata dell'art. 2 Cost. tra chi la ritiene fattispecie aperta, clausola di recepimento di nuovi diritti e chi, invece, avversa questa ricostruzione sostenendo la necessità di riferirsi sempre ad altre fattispecie costituzionali. V. con riferimento proprio al diritto alla riservatezza le posizioni, da un lato, di A. Barbera - F. Cocozza - G. Corso, *Le situazioni giuridiche soggettive. Le libertà dei singoli e delle formazioni sociali. Il principio di eguaglianza*, in G. Amato - A. Barbera (a cura di) *Manuale di diritto pubblico*, I, Bologna, 1997, 286, e da un altro lato di A. Baldassarre, *Diritti inviolabili*, in *Enciclopedia Giuridica*, XIX, Roma, 1989, 19-20. La sentenza in cui la Corte Cost. si avvicina maggiormente ad una prospettiva di compromesso è la 12 aprile 1973, n. 38 laddove ricomprende tra i diritti inviolabili dell'uomo, il diritto alla riservatezza e all'intimità. (*Giurisprudenza costituzionale*, 1973, 354 ss.)

[47] Si v. sul ruolo storico della CEDU nella protezione dei dati personali, F. Pizzetti, *Privacy e diritto europeo alla protezione dei dati personali, vol. I. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 56 ss.

[48] La Convenzione n. 108 adottata a Strasburgo il 28 gennaio 1981 dal Consiglio d'Europa riguarda solo la protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale.

[49] Questo è ancora più evidente con il Regolamento 2016/679 che espressamente prevede settori in cui gli Stati membri sono chiamati a integrare la normativa europea. V. sul punto, F. Pizzetti, *Privacy e diritto europeo alla protezione dei dati personali*, vol. II. *Il Regolamento europeo 2016/679*, Torino, 2016, 17.

[50] Per un'analisi, F. Donati, *Protezione dei dati di carattere personale*, in R. Bifulco – M. Cartabia – A. Celotto (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, Bologna, 2001, 83 ss.

[51] Questo fa cessare la discussione, che oggi sarebbe ormai abbastanza sterile, sul riconoscimento della protezione dei dati personali come diritto costituzionalmente tutelato.

[52] V., ad esempio, la specificazione nella norma della Carta, del principio del consenso, del principio di lealtà e di finalità nel trattamento e dei diritti dell'interessato di accesso e di rettifica che integrano evidentemente il contenuto essenziale del diritto.

nella Carta, devono essere adottate ai sensi della clausola generale di cui all'art. 52, c. 1, della Carta. La norma in questione prevede che esse siano fondate su una previsione legislativa, debbano rispettare il limite del contenuto essenziale del diritto e rispondere a finalità di interesse generale dell'Unione o alla tutela di altri diritti egualmente garantiti[53].

La richiesta che ogni eventuale restrizione risponda a finalità di interesse generale o miri alla protezione di altri diritti merita uno specifico approfondimento, perché la sicurezza può, in teoria, essere declinata sia come interesse generale dell'Unione sia, alla luce dell'art. 6 della Carta medesima, come diritto e, quindi, entrambe le prospettive meritano di essere di seguito analizzate.

6. La sicurezza nazionale e la sicurezza pubblica come fini legittimi per la restrizione del diritto alla protezione dei dati personali

La sicurezza nazionale e la sicurezza pubblica sono certamente fini legittimi, ai sensi sia della CEDU, sia della Carta dei diritti fondamentali dell'Unione europea sia della Costituzione italiana, per imporre, a determinate condizioni, limitazioni del diritto alla protezione dei dati personali.

Il punto di partenza è che tutti gli atti normativi dello storico *corpus* europeo di protezione dati (la direttiva 95/46, c.d. direttiva madre, la direttiva 58/2002, c.d. direttiva e-privacy e la decisione 2008/977/GAI sul trattamento dei dati per la cooperazione giudiziaria in materia penale e per le operazioni di polizia) specificano che le norme europee lasciano inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato e l'applicazione della legge penale[54].

Tra di essi però, occorre segnalare come la direttiva 58/2002, specifichi, facendo sua la giurisprudenza della Corte di giustizia, che eventuali limitazioni al diritto di protezione dei dati debbano essere conformi alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, così come interpretata dalle sentenze della Corte di Strasburgo[55]. Il riferimento alla CEDU si spiega con il fatto che, al momento dell'entrata in vigore della normativa citata, la Convenzione era, in tema di diritti fondamentali, la fonte-parametro da cui desumere le tradizioni costituzionali comuni, che

[53] Sulla scelta di utilizzare tale clausola T. Groppi, *Articolo 52. Portata dei diritti garantiti*, in R. Bifulco – M. Cartabia – A. Celotto (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, Bologna, 2001, 351 ss. V. per un esame analitico della clausola H.D. Jarass, *Charta der Grundrechte der Europäischen Union*, Monaco, 2013, 464 ss. Per un esame della portata di tale clausola generale, ancorché svolto in riferimento alla libertà di espressione, sia consentito rinviare a M. Orofino, *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione*, Torino, 2014, 93 ss.

[54] V. cons. 13 ed art. 3, par. 2 direttiva 95/46; cons. 11 ed art. 1, par. 3 della direttiva 58/2002; art. 1, par. 4 della decisione 2008/977/GAI.

[55] V. espressamente il considerando 11.

secondo la giurisprudenza della Corte di giustizia dell'Unione europea erano già da tempo da considerarsi come principi fondamentali del diritto dell'Unione e cui dovevano conformarsi sia la normativa europea sia quella nazionale di recepimento[56].

Il Regolamento 679/2017 e la Direttiva 680/2017, che abrogheranno, a far data dal 25 maggio 2018, la direttiva 95/46 e la decisione quadro[57], confermano la possibilità di prevedere restrizioni alla protezione dei dati personali per esigenze di sicurezza, ma delimitano questa fattispecie in maniera assai stringente[58].

In particolare, l'art. 23 del Regolamento prevede tutta una serie di casi in cui il diritto dell'Unione – a testimonianza dell'allargamento delle competenze europee in materia– o degli Stati membri possa imporre limitazioni specifiche ai diritti di protezione dei dati garantiti dalla normativa. Tra i fini che possono giustificare restrizioni figurano specificamente la sicurezza nazionale, la difesa, la sicurezza pubblica, la prevenzione, l'indagine, l'accertamento di reati e l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica[59].

Rispetto al precedente quadro normativo, il nuovo Regolamento europeo contiene anche importanti specificazioni riguardo il contenuto delle eventuali restrizioni e i limiti

---

[56] Per un esame delle diverse tappe del riconoscimento giurisprudenziale dei diritti fondamentali v. J.H.H. Weiler - J.S. Lockhart, *"Taking Rights Seriously": The European Court and its Fundamental Rights Jurisprudence* (Part. I e Part. II) entrambi in *Common Market Law Review*, 1995, rispettivamente 51 ss. e 579 ss. Nella dottrina costituzionalista italiana v. M. Cartabia, *Principi inviolabili e integrazione europea*, Milano, 1995, 19 ss. V. per un'ampia ed approfondita analisi della nozione di tradizioni costituzionali comuni nell'ordinamento europeo, A. Ruggeri, *«Tradizioni costituzionali comuni» e «controlimiti», fra teoria delle fonti e teoria dell'interpretazione*, in P. Falzea -A. Spadaro - L. Ventura (a cura di), *La Corte costituzionale e le Corti d'Europa*, Torino, 2003, 505 ss.; O. Pollicino, *Corte di giustizia e giudici nazionali: il moto "ascendente", ovverosia l'incidenza delle "tradizioni costituzionali comuni" nella tutela apprestata ai diritti dalla Corte dell'Unione*, in Consulta OnLine, 1, 2015, 242 ss.

[57] Rimarrà invece in vigore la direttiva 58/2002 che è oggetto attualmente di un procedimento *ad hoc* di revisione. Sul nuovo Regolamento europeo v. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, vol. I e vol. II, cit., *passim*. V. anche i contributi in S. Sica - V. D'Antonio - G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016 e in L. Califano – C.Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017.

[58] Fermo restando che dall'ambito di applicazione del Regolamento permangono esclusi *ex* art. 2, par. 2 lett. d) i trattamenti effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

[59] In modo simile dispone anche la direttiva 680/2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. Da un lato, essa, infatti, posta la particolarità dei dati oggetto di trattamento, nel cons. 14 rammenta che essa non dovrebbe applicarsi al trattamento di dati personali nell'ambito di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione, le attività concernenti la sicurezza nazionale, le attività delle agenzie o unità che si occupano di questioni connesse alla sicurezza nazionale (…). Da un altro lato, le norme della direttiva che disciplinano il diritto di accesso ai dati e i diritti di rettifica prevedono, in modo speculare a quanto visto nel Regolamento 2016/679, la possibilità di adottare misure legislative che limitino tali diritti, per motivi di sicurezza, nel rispetto di stringenti limiti formali e sostanziali. Su tale direttiva v. P. Troisi, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in S. Sica - V. D'Antonio – G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, cit., 313 ss.; P. Milazzo, *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, in L. Califano – C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit., 709 ss.

imponibili.

Innanzitutto è chiarito che la restrizione debba essere necessaria e proporzionata in una società democratica. Il che evidentemente richiama la formula contenuta tanto nella CEDU quanto nella Carta dei diritti fondamentali dell'Unione europea. In secondo luogo, è previsto che la restrizione, legislativamente adottata, debba contenere alcune disposizioni specifiche circa: a) le finalità del trattamento o le categorie di trattamento; b) le categorie di dati personali; c) la portata delle limitazioni introdotte; d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti; e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari; f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento; g) i rischi per i diritti e le libertà degli interessati; e h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

Come si evince dal tenore delle norme qui citate, il test di legittimità circa future restrizioni si preannuncia assai severo, in linea però con la più recente giurisprudenza della Corte CEDU e della Corte di giustizia che rappresenta, pur nella diversità di portata, un riferimento ineludibile per evidenziare i confini entro cui eventuali restrizioni alla protezione dei dati personali sono oggi e saranno domani ritenute legittime.

Per quanto riguarda la Corte CEDU, la giurisprudenza in materia di tutela della vita privata – e di protezione dei dati personali – è assai consistente ancorché molto settoriale[60].

Tra le sentenze più recenti, che meritano una particolare attenzione perché vertono su misure legislative adottate per aumentare la sorveglianza contro il terrorismo e, quindi, toccano direttamente il bilanciamento tra sicurezza nazionale e *privacy rights* occorre considerare con attenzione *Roman Zakcharov v. Russia* (2015)[61].

Il caso in questione originava da un ricorso presentato dall'editore Roman Zakcharov contro il rigetto da parte del giudice nazionale della sua azione contro tre operatori telefonici russi che, secondo il ricorrente, avevano violato il suo diritto alla *privacy*. Il ricorso era stato respinto sul piano interno perché l'attore non era riuscito a provare, in concreto, alcuna violazione, pur avendo depositato prove sulla base delle quali ciò sarebbe potuto, in astratto, avvenire.

La Corte di Strasburgo ha innanzitutto constatato, in punto di ammissibilità, che Zakharov avesse il diritto di dichiararsi vittima di una violazione della Convenzione europea e, quindi, di adire la Corte stessa, pur non essendo in grado di provare di essere stato oggetto di una misura concreta di sorveglianza. Per la Corte, Zakharov non aveva nemmeno bisogno di dimostrare di essersi trovato in una situazione di rischio potenziale posto che la legislazione russa in materia non fornisce un efficace rimedio alla persona che sospetta di essere soggetto di una sorveglianza segreta. Per cui è l'esistenza

[60] Si v. sull'intercettazione di telecomunicazioni *Zakharov v. Russia* (2015) e *Szabo e Vissy v. Ungheria* (2016), sul monitoraggio di email e dell'uso di Internet *Copland v. UK* (2007) e *Barbulescu v. Romania* (2016), sull'installazione di "*listening devices*" *Vetter v. France* (2005), sulla videosorveglianza *Khmel v. Russia* (2013), e con riferimento agli spazi pubblici *Peck v. Uk* (2003), sul tracciamento *Uzun v. Germany* (2010), sulla registrazione di viaggi treno e ed aerei *Shimolov v. Russia* (2011), sulle impronte digitali nei cellulari e sulla profilazione del DNA *S and Marper v. UK* (2008).

[61] V. anche *Szabo e Vissy v. Ungheria* (2016).

stessa della normativa controversa a costituire, di per sé, un'interferenza dei diritti di Zakharov ai sensi dell'art. 8 della CEDU.

Questa posizione è assai interessante perché apre ad un esame differente rispetto a quello svolto ordinariamente dalla Corte[62]. Data la natura segreta delle misure di sorveglianza stabilite dalla legge russa e dato il fatto che esse interessano tutti gli utenti delle comunicazioni telefoniche mobili, la Corte ritiene giustificato esaminare la normativa in questione non dal punto di vista di un caso specifico di sorveglianza, ma in astratto. Per questa ragione, le osservazioni con cui la Corte giunge ad accogliere il ricorso di Zakcharov vanno molto oltre il caso specifico potendosi considerare quasi come un decalogo per ogni sistema di sorveglianza adottato con finalità di antiterrorismo a tutela, quindi, della sicurezza nazionale e della sicurezza pubblica.

Innanzitutto, la Corte rileva, su richiesta della difesa legale del governo russo, che l'intercettazione delle comunicazioni prevista nella legislazione russa persegue fini legittimi di protezione della sicurezza nazionale e della sicurezza pubblica, di prevenzione della criminalità e di protezione del benessere economico del paese. Questi fini sono idonei, ai sensi della CEDU, a giustificare restrizioni del diritto alla vita privata degli individui ed alla protezione dei dati personali. Tuttavia, per la Corte, tenuto conto del rischio che un sistema di sorveglianza di massa segreta può produrre se utilizzato per minare o addirittura distruggere la democrazia invece di difenderla, è necessario accertare se nella legislazione russa vi siano garanzie adeguate ed efficaci contro gli errori di gestione nell'uso del sistema, come l'arbitrarietà o l'abuso.

In proposito, le criticità che vengono evidenziate sono molte.

Primo, le disposizioni giuridiche che disciplinano la sorveglianza delle comunicazioni consentono ai servizi segreti e alla polizia un accesso diretto a tutte le comunicazioni telefoniche mobili.

Secondo, la legislazione non prevede la supervisione dell'intercettazione così assunta, da parte di un giudice o di un'autorità pubblica.

Terzo, la durata di tali misure con particolare riferimento alle circostanze in cui devono essere interrotte non è specificata.

Quarto, non sono specificate le circostanze in cui le autorità pubbliche in Russia hanno il potere di ricorrere a misure di sorveglianza segrete né le procedure per l'autorizzazione dell'intercettazione, per la memorizzazione e per la distruzione dei dati intercettati.

Quinto i rimedi disponibili per contestare l'intercettazione delle comunicazioni, sono disponibili solo per coloro che sono in grado di presentare la prova dell'intercettazione, ma l'ottenimento di tale prova è di fatto impossibile mancando qualsiasi sistema di notifica.

Per quanto, invece, riguarda la giurisprudenza della Corte di giustizia, il riferimento è alle sentenze *Digital Rights Ireland* e *Schrems*, due casi assai noti e su cui esiste ormai

[62] L'art. 34 della CEDU prevede che il ricorrente, per poter presentare ricorso, deve essere in grado di provare di essere stato «*directly affected*» dalla misura. Questo criterio non è tuttavia applicato in maniera rigida. V. tra i precedenti in cui la Corte aveva già fatto riferimento al rischio potenziale, *Klass and Others v. Germany* (1978) e soprattutto *Kennedy v. the United Kingdom* (2010), in cui la «*Court held that sight should not be lost of the special reasons justifying the Court's departure, in cases concerning secret measures, from its general approach which denies individuals the right to challenge a law in abstracto*».

ampia dottrina[63].

Nella sentenza *Digital Rights Ireland*, la Corte di giustizia dell'Unione europea provvede all'annullamento di un importante atto normativo europeo, la direttiva la 2006/24/CE cd. Direttiva *Data Retention*, per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza.

All'attenzione della Corte erano, appunto, le disposizioni della direttiva volte a garantire la conservazione dei dati di traffico telefonico e telematico, i dati relativi all'ubicazione e quelli necessari all'identificazione dell'abbonato, per fini di accertamento e repressione dei reati.

Nelle sue argomentazioni la Corte, dopo aver verificato il rispetto del requisito legale per imporre restrizioni e valutato che la normativa non limitava il contenuto essenziale dei diritti fondamentali alla vita privata e alla protezione dei dati personali di cui agli artt. 7 e 8 della Carta dei diritti fondamentali, affermava anche che le misure in oggetto perseguivano interessi generali, quello della sicurezza internazionale e quello della sicurezza pubblica, meritevoli di tutela ed idonei, ai sensi dei Trattati europei e della Carta dei diritti, a giustificare restrizioni dei diritti.

Il fulcro della pronuncia, da cui poi discende l'annullamento integrale della *data retention* è il mancato rispetto, secondo la Corte, del principio di stretta necessità della limitazione rispetto agli obiettivi perseguiti. La normativa, infatti, per la Corte impone obblighi di conservazione per tutti i mezzi e riguardo a tutte le persone, senza operare le distinzioni necessarie, senza prevedere limitazioni e possibilità di accedere ai dati, senza controllo del giudice, senza garanzie sufficienti di conservazione e senza nemmeno prevedere la distruzione irreversibile allo spirare dei termini di conservazione. Infine, anche la conservazione dei dati sul territorio dell'Unione non è adeguatamente specificata.

Tutto questo significa che in taluni casi il sacrificio della protezione dei dati personali a tutela della sicurezza generale può essere legittimo, ma non può essere, come la Corte evidenzia, generalizzato. Il "legislatore" europeo e quelli nazionali sono chiamati ad operare specifiche distinzioni per le diverse ipotesi di conservazione, a graduare le restrizioni sulla base delle diverse situazioni che intendono disciplinare e a definire sempre le garanzie minime di conservazione dei dati.

Nella sentenza *Schrems*, la Corte di giustizia è chiamata a decidere una questione di estrema rilevanza ossia a pronunciarsi sulla legittimità della decisione della Commissione che attestava l'adeguatezza del livello di protezione dei dati previsto dall'accordo del c.d. *Safe Harbour* ed autorizzava il trasferimento dei dati personali dall'Unione europea

[63] Tra i molti commenti, senza presunzione di esaustività, v. O. Pollicino, *Interpretazione o manipolazione? La Corte di Giustizia definisce un nuovo diritto alla privacy digitale*, in www.federalismi.it - focus TMT, 3, 2014; Id., *La "transizione" dagli atomi ai bit nel reasoning delle Corti europee*, in *Ragion pratica*, 44, 2015, 53 ss.; O. Pollicino – M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in G. Resta – V. Zeno Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dal "Safe Harbour principles" al "Privacy Shield",* Roma, 2016, 73 ss.; P. Falletta, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande sezione), 6 ottobre 2015, Schrems c. Data Protection Commissioner, C - 362/14),* in www.federalismi.it, 24, 2015; R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giurisprudenza costituzionale,* 1, 2016, 289 ss.; G. De Minico, *Antiche frontiere e nuova libertà digitale*, cit., 136; L. Curicciati, *Diritto alla riservatezza e sicurezza nella giurisprudenza delle Corti costituzionali e sovrastatali europee. Il caso della Data Retention Directive*, in *Democrazia e sicurezza*, 2, 2017.

agli Stati Uniti per le imprese americane che lo avessero sottoscritto.
Il giudizio della Corte è in questo caso *tranchant*.
Osservato, infatti, che l'accordo *Safe Harbour* vincola sole le imprese americane che lo sottoscrivono, che le autorità pubbliche degli Stati Uniti non vi sono assoggettate e che le leggi statunitensi in materia di sicurezza nazionale prevalgono sull'approdo sicuro cosicché le imprese americane sono tenute a disapplicare, senza limiti, le norme di tutela previste da tale regime nei casi in cui esse entrino in contrasto con tali esigenze, la Corte di giustizia non può che concludere che la decisione di adeguatezza della Commissione sia illegittima per contrasto con gli art. 7 e 8 della Carta dei diritti fondamentali.
In questo caso, però, l'illegittimità prescinde da valutazioni circa la proporzionalità e la stretta necessità delle restrizioni perché essa deriva direttamente dalla violazione del contenuto essenziale di tali diritti e, specificamente, per quanto riguarda il diritto alla protezione dei dati, i diritti di accesso, rettifica e cancellazione. Questi rappresentano per la Corte un nucleo intangibile che non può mai essere integralmente sacrificato, pena l'illegittimità della restrizione.
Se, dunque, i casi giunti all'attenzione delle Corti dimostrano che, in taluni casi, possa esistere un contrasto tra l'esigenza di proteggere i dati personali e l'esigenza di garantire la sicurezza, occorre però dire che tutti i giudizi delle Corti (a Strasburgo come a Lussemburgo) concorrono a smentire la semplificazione "*privacy* vs. sicurezza". Esse dimostrano, invece, che il bilanciamento o la contestuale tutela può (e deve) svolgersi in modo tale che nessuna delle due esigenze sia sacrificata e, nello specifico, preservando il nucleo essenziale del diritto individuale alla protezione dei dati personali.

7. Sicurezza individuale e protezione dei dati personali

Se dal bilanciamento tra protezione dati e sicurezza nazionale, si passa ora a considerare il rapporto tra tutela della sicurezza individuale e protezione dei dati personali si scopre agevolmente che, piuttosto che di potenziali contrasti, si debba parlare di evidenti affinità.
Questo vale sia se la declinazione è quella del diritto alla sicurezza come sicurezza dei diritti sia se, invece, si voglia far riferimento al diritto alla sicurezza come diritto individuale ed autonomo.
Nel primo caso, occorre considerare che il diritto fondamentale alla protezione dei dati personali sempre più diventa nella società attuale il «presidio irrinunciabile di tutte le libertà classiche delle nostre Costituzioni e, in ultima analisi, della nostra Costituzione»[64].
Le attività di raccolta, correlazione e analisi dei dati consentono, infatti, già oggi una profilazione delle persone singole e dei gruppi sociali talmente precisa da poter condurre a prevedere i loro comportamenti e a orientare le loro decisioni individuali e collettive. In questo modo, la libertà personale, intesa come libertà da ogni controllo illecito, rischia, se tali trattamenti non sono adeguatamente regolamentati, di perdere di

[64] F. Pizzetti, *Privacy e il diritto europeo alla sicurezza*. Vol. I. *Dalla direttiva 95/46 al nuovo Regolamento europeo*, cit., 10.

significato così travolgendo tutte le altre libertà[65].

Proprio il fatto che la protezione dei dati rappresenti ormai un baluardo contro illeciti controlli che incidono sulla nostra libertà, mostra come la protezione dati sia ormai non solo un diritto individuale, ma essa stessa un interesse generale fondamentale dell'Unione europea e degli Stati membri[66].

Il Regolamento europeo sembra accogliere esplicitamente tale prospettiva. Nel considerando 4, infatti, dopo aver rammentato che il diritto alla protezione dei dati pur essendo un diritto fondamentale dell'uomo non è una prerogativa assoluta, aggiunge che esso va considerato alla luce della sua funzione sociale. Questa impressione è successivamente suffragata dalle norme del Regolamento che disciplinano l'obbligo in capo ai titolari della notifica di eventuali violazioni alle autorità di controllo (artt. 33 e 34) nonché dalle norme che impongono al titolare del trattamento di dar prova alle medesime autorità di aver adottato tutte le misure tecniche organizzative adeguate a garantire la sicurezza del trattamento e a minimizzare i rischi (art. 24).

L'idea che il diritto alla protezione dei dati sia, al tempo stesso, il presidio irrinunciabile di tutte le libertà e un interesse generale della società spiega e giustifica anche il tentativo del nuovo apparato normativo di rafforzare il grado di tutela attraverso una serie di innovazioni assai significative che vanno dalla responsabilizzazione (*accountability*) dei titolari e dei responsabili del trattamento alla previsione obbligatoria in determinati casi del *Data Protection Officer*, dall'obbligo di compiere analisi preventive del rischio all'obbligo di adottare meccanismi di *privacy by design* e *by default*, dal rafforzamento dinamico delle misure di sicurezza alle regole di segnalazione e di gestione dei *data breaches*.

Nel secondo caso, laddove si voglia considerare la sicurezza individuale come diritto individuale ed autonomo, la protezione dei dati personali con il suo corredo di istituti, obblighi, controlli, garanzie e sanzioni rappresenta un argine importante contro i rischi che emergono nella società digitale.

Rischi non solo astratti, ma pure assi concreti legati a comportamenti criminali ai danni dei singoli individui. Si pensi ad esempio al fatto che, secondo le statistiche più recenti, oltre l'ottanta per cento dei *data breach* ossia delle violazioni di sicurezza che comportano la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali è di natura non accidentale, perpetrata in larghissima parte da criminali informatici [67].

Si consideri ancora che il reato più diffuso è il furto di identità. Tale fattispecie rappresenta in un contesto *online* il reato più pericoloso perché si configura come il *passepartout* per tutta una serie di altri reati, sia di carattere personale sia di carattere finanziario[68]. Anche la quantità di *account* che possono essere contemporaneamente violati è, come dimostrano alcuni casi recenti, spaventosa potendo risultare coinvolte centinaia di milioni di persone.

Queste considerazioni trovano corrispondenza nelle norme del Regolamento che defi-

[65] *Ibid.,* 10 s. V. con riferimento all'IA anche F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione,* cit., 37 ss.

[66] F. Pizzetti, *Privacy e il diritto europeo alla sicurezza*. Vol. II. *Il regolamento europeo*, cit. 4 s.

[67] Gemalto, *Breach Level Index Report*, 2016.

[68] *Ibid.*

niscono il principio di sicurezza come cardine del trattamento dei dati e impongono ai titolari del trattamento di valutare *ex ante*, a seconda dei dati trattati e delle finalità del trattamento, i rischi e, di conseguenza, adottare tutte le misure tecniche ed organizzative necessarie per minimizzarli, in particolar modo laddove essi possano impattare sui i diritti e sulle libertà delle persone fisiche[69].

Questa attenzione del legislatore europeo rientra pienamente nella logica per cui un apparato normativo in grado di offrire una protezione sufficiente ai dati personali è decisivo tanto per garantire la sicurezza dei cittadini in senso oggettivo quanto per rafforzare la loro percezione soggettiva e, quindi, la loro fiducia nella società digitale.

8. Brevi osservazioni conclusive

Alla luce della complessiva analisi svolta in questo saggio, pare potersi affermare che se si esce dalla dicotomia semplificante "*privacy* (protezione dei dati personali) vs. sicurezza" e si guarda più in profondità sia ai bisogni su cui si fondano ontologicamente i due diritti, sia ai beni costituzionalmente protetti, sia alla disciplina europea in materia di protezione dei dati, si osserva una realtà molto diversa.

In questa realtà è certamente possibile che, in taluni casi, esigenze di sicurezza nazionale e di sicurezza pubblica, richiedano limitazioni specifiche del diritto alla riservatezza e alla protezione dei dati personali[70].

Questa dinamica appartiene, però, alla normale dialettica che il bilanciamento dei diritti e degli interessi costituzionalmente rilevanti impone. In proposito, la giurisprudenza delle Corti europee ha dimostrato che tale bilanciamento non può mai comportare l'integrale sacrifizio dell'uno o dell'altra posizione giuridica tutelata.

Con riferimento alle restrizioni imponibili al diritto fondamentale alla protezione dei dati personali, tanto la Corte EDU quanto la Corte di giustizia hanno concorso, ciascuna con i suoi strumenti e ciascuna nel suo ordinamento, a definire i paletti invalicabili. Questo è avvenuto sia con riferimento alla forma della misura restrittiva, richiedendo sempre l'esistenza di una base legale, sia con riferimento alla sostanza della restrizione. Come si è messo in luce nei paragrafi che precedono, le Corti, proprio in relazione al bilanciamento tra protezione dei dati ed esigenze di sicurezza hanno definito il contenuto minimo o essenziale del diritto alla protezione dei dati e ampiamente richiamato il principio di stretta necessità delle limitazioni concretamente adottate.

[69] In un contesto in cui si adotta un modello flessibile, molto diverso da quello statico della direttiva 95/46 in cui erano elencate le misure minime di sicurezza ed in cui spetta al titolare del trattamento definire e progettare, sulla base di un'analisi dei rischi, le misure di sicurezza adeguate al tipo di trattamento che si intende svolgere. Tra le misure che devono essere valutate dal titolare il Regolamento elenca, non a caso, espressamente la pseudonimizzazione e la cifratura dei dati personali; la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; il ripristino tempestivo della disponibilità e l'accesso dei dati in caso di incidente; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. V. sul punto l'importante lavoro di G. D'Acquisto - M. Naldi, *Big data e privacy by design*, Torino, 2016, spec. 41 ss. e 117 ss.

[70] Di singoli casi in cui si può verificare una contrapposizione parla anche A. Ruggeri, *Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni)*, cit., 375.

Il Regolamento 2016/679 ha certamente recepito queste indicazioni, ma come si è cercato di osservare è andato anche oltre.

Infatti, nell'attenzione che il nuovo Regolamento dedica alla sicurezza dei trattamenti, alla valutazione e alla minimizzazione dei rischi, agli obblighi posti in capo al titolare, alle sanzioni, sembra esserci la piena consapevolezza che le esigenze di sicurezza collettiva non si soddisfano con la generica compressione della *privacy* dei cittadini, ma al contrario con il suo rafforzamento.

Questa prospettiva in cui *privacy* o protezione dei dati e sicurezza sono complementari e non alternative esce ulteriormente rafforzata se si guarda alla protezione dei dati come interesse collettivo della società.

Se infatti, come il Regolamento afferma esplicitamente, la protezione dei dati è non solo un diritto individuale ma ormai compiutamente un interesse primario della società, lo è proprio perché esso appare strumentale, da un lato, alla garanzia dei diritti e, dall'altro lato, alla tenuta complessiva degli ordinamenti democratici.

In questo senso, la protezione dei dati è necessaria sia a garantire la sicurezza declinata come sicurezza dei diritti sia la sicurezza come percezione soggettiva di sicurezza e collante ultimo delle società. Per cui sembra di poter concludere, confortati dall'analisi condotta, affermando che l'espressione dicotomica "*privacy* (protezione dei dati personali) vs. sicurezza" sia in realtà molto meno idonea a descrivere la realtà di quanto non possa farlo piuttosto l'affermazione contraria e cioè che "*privacy* (protezione dei dati personali) è sicurezza".

La tutela dell'oblio tra intimità e condivisione senza filtri*

Aurora Vesto

Abstract

Il saggio analizza il ruolo del "diritto all'oblio" nel contesto delle reti sociali, affinché le persone possano esercitare un controllo sugli elementi dei loro dati personali che sono accessibili al pubblico; spesso le informazioni che riceviamo da Internet sono "datate" e non più attuali.
Il diritto all'oblio, in questa tensione tra "informazione" e "privacy", tra "diritto" e "interesse", tutela la posizione della persona che desidera ostacolare la divulgazione di tutte quelle notizie che non corrispondono più alla realtà storica.

The essay analyses the role of "right to be forgotten" in the context of social networks, by which individuals are vested with the power to control which aspects of their personal data are accessible to the public; more and more frequently, in fact, the information that we get from the Internet is "dated" and does not reflect the current status quo. The right to be forgotten, in this tension between "information" and "privacy", between "right" and "interest", strengthens the legal position of individuals wishing to prevent and stop the spread of news no longer corresponding to the historical truth.

Sommario

1. Genesi ed evoluzione del diritto all'oblio come situazione autonoma. – 2. Il diritto all'oblio nell'informazione "indomabile" di Internet. – 3. Una possibile tutela dell'oblio come manifestazione di "interesse legittimo".

Keywords: Diritto all'oblio, Dati personali, Riservatezza, Informazioni, Interesse sociale

1. Genesi ed evoluzione del diritto all'oblio come situazione autonoma

L'impostazione di qualunque discorso sul diritto all'oblio implica la consapevolezza del collegamento funzionale col diritto alla privacy, col diritto di cronaca e col diritto al trattamento dei dati personali. Il diritto alla riservatezza[1], infatti, si articola principal-

[1] Per una recente disamina sulla tutela della privacy e della protezione dei dati personali, anche con profili di diritto internazionale privato, si rinvia a AA.VV., *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Temi scelti, (a cura di) M. Distefano, Napoli, 2017.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio anonimo, in quanto riproduce la relazione presentata dall'A. al convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno" (Messina, 26-27 maggio 2017).

mente in due sottospecie: diritto alla protezione dei dati personali e diritto al rispetto della propria vita privata[2]; questi due aspetti sono strettamente connessi in quanto il diritto al rispetto della vita privata può essere messo in discussione da un trattamento abusivo dei dati personali.

Nonostante il codice civile non includa il diritto alla riservatezza tra i diritti della personalità, alcuni importanti riferimenti normativi hanno condotto all'individuazione di un diritto alla riservatezza che trae origine dal diritto della personalità. Si rinviene, infatti, il fondamento del diritto alla riservatezza nell'espressione generale di cui all'art. 2 Cost., per il quale «la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo nelle formazioni sociali ove si svolge la sua personalità»; la tutela volta a preservare l'individuo da intrusioni esterne è rintracciabile, inoltre, nell'art. 8 Cedu, che riconosce ad «ogni persona» il «diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza».

L'origine del diritto alla riservatezza è di natura giurisprudenziale: in particolare, secondo la dottrina, il *leading case* può essere identificato nella decisione della Suprema Corte del 27 maggio 1975, n. 2129[3], in cui per la prima volta i giudici di legittimità affermano la fondatezza della costruzione giuridica di questo nuovo diritto[4]. Sono seguite diverse pronunce che hanno riconosciuto copertura costituzionale del diritto alla riservatezza nell'art. 2 Cost., nonché precipuo riferimento nell'art. 8 Cedu, mettendo in rilievo la finalità del d.lgs. 30.06.2003, n. 196, volto a garantire che «il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali» (art. 2, c. 1, Codice della privacy).

In questa cornice si è acquisita la consapevolezza che è fondamentale operare il giusto bilanciamento tra il diritto alla riservatezza (art. 2 Cost.) e il diritto di cronaca (art. 21 Cost.), per verificare le ragioni della prevalenza eventuale dell'uno o dell'altro nel contesto concreto.

Il diritto all'oblio, che rinviene la propria ragion d'essere nel decorso del tempo e nella naturale propensione dell'uomo a dimenticare il passato, è nato - per creazione giurisprudenziale - come specificazione del diritto alla riservatezza ma con peculiarità autonome e distinte. Infatti, il diritto all'oblio non è volto ad impedire la divulgazione di notizie e fatti riservati appartenenti alla sfera intima dell'individuo, ma ad ostacolare la rievocazione, a distanza di molto tempo, di fatti già resi di dominio pubblico, quando è venuta meno l'attualità della notizia, fino al punto da divenire estranea alla sfera sociale e/o lavorativa dell'interessato.

In altri termini, la ripubblicazione della notizia, ormai priva di utilità sociale nell'ambito della funzione tipica dell'informazione, determina un *vulnus* nella sfera esistenziale della persona, fino ad assumere i contorni del carattere diffamatorio, trattandosi di notizia vetusta e non più attuale.

Ecco perché, oggi, il diritto all'oblio è una proiezione assiologica del dato oggettivo

[2] È questa la nozione comunemente espressa dal termine *privacy*, che ha segnato l'origine della dottrina della riservatezza.

[3] In *Giur. it.*, I, 1976, 970.

[4] G. Alpa, *Manuale di diritto privato*, IX ed., Vicenza, 2015, 175.

emergente, cioè dell'affievolimento dell'interesse sociale alla notizia.
Il nostro ordinamento tutela l'attualità dell'immagine sociale della persona, specialmente in relazione al diritto di cronaca, in una dimensione esistenziale caratterizzata da una instancabile ricerca di visibilità. Prima dell'avvento della tecnologia digitale e dei network globali, dimenticare una notizia era più facile, costituiva quasi la regola ed era difficile riesumarla a distanza di tempo. Oggi, viceversa, dimenticare una notizia rappresenta un'eccezione e la sua facilità di nuova divulgazione è capace di causare danni alla vita di un consociato.
E' vero che l'interessato può chiedere la cessazione del fatto lesivo con un ricorso rivolto al Garante per la protezione dei dati personali (art. 145, d.lgs. n. 196/2003) o esercitando un'azione inibitoria innanzi all'autorità giudiziaria, ma occorre la verifica dell'effettiva efficacia del rimedio. Anzi, una "coraggiosa posizione"[5] della giurisprudenza di merito[6], supportando le proprie argomentazioni con una rigorosa interpretazione delle regole attuative della Direttiva 2000/31/CE sul commercio elettronico, ha "fissato il principio secondo cui, una volta emersa l'illiceità dei contenuti, il social network ha l'obbligo di eliminare i link e le informazioni ingiuriose anche a prescindere da un ordine dell'autorità amministrativa o giudiziaria"[7].
Secondo un'autorevole dottrina, «il diritto all'oblio tutela l'interesse del soggetto a che informazioni relative alla propria immagine o ai propri dati personali del passato siano attualizzate o cancellate»[8]; non a caso esso trova una specifica fonte nella disciplina del c.d. codice della privacy, laddove si attribuisce all'interessato il diritto alla cancellazione, alla trasformazione, al blocco, alla rettificazione, all'aggiornamento e integrazione dei propri dati personali (art. 7, d.lgs. 196/2003).
La tutela del diritto all'oblio che ha come contraltare il "diritto ad essere ricordati", dunque, evita al soggetto la ripubblicazione ovvero la permanenza nel mondo di *internet* di notizie sul proprio conto che siano divenute prive di interesse sociale, che possono, invece, solo nuocere all'evoluzione della persona nella dimensione attuale.
La giurisprudenza ha riconosciuto l'importanza del "diritto a non essere ricordati" in

[5] Efficacemente così definita da A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, in *Nuove leggi civ. comm.*, 2, 2017, 440.

[6] Trib. Napoli Nord, sez. II civ., ord. 3 novembre 2016 (in *DeJure*), ove si legge che «pur non essendovi un obbligo di controllo preventivo dei contenuti presenti né una posizione di garanzia, sussiste tuttavia un obbligo successivo di attivazione di modo che la responsabilità *a posteriori* dell'*hosting provider* sorge per non aver ottemperato una richiesta (diffida) di rimozione dei contenuti illeciti proveniente dalla parte che assume essere titolare dei diritti, ovvero per non aver ottemperato a un ordine dell'autorità, sia essa giurisdizionale o amministrativa, cui si sia rivolto il titolare del diritto per ottenere il medesimo effetto».

[7] A. Thiene, *Segretezza e riappropriazione*, cit., 440.

[8] C.M. Bianca, con la collaborazione di M. Bianca, *Istituzioni di diritto privato*, Milano, 2014, 102.

diverse pronunce, in particolar modo di natura europea[9], che elevano il diritto all'oblio a diritto inviolabile. Si pensi alla sentenza del 2015 del Tribunale di Roma[10], secondo cui il diritto all'oblio rappresenta il «legittimo interesse di ciascuno a non rimanere indeterminatamente esposto ad una rappresentazione non più attuale della propria

[9] V. CGUE, C-131/12, *Google Spain* (2014). La sentenza è stata commentata in Italia da molti autori, tra cui si ricorda, senza spirito di esaustività, F. Melis, *Il diritto all'oblio e i motori di ricerca nel diritto europeo*, in *Giorn. dir. amm.*, 2, 2015, 171-177; A. Palmieri - R. Pardolesi, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi Quaderni del Foro Italiano*, Quaderno n. 1 (27 maggio 2014), in www.foroitaliano.it/wp-content/uploads/2014/05/quaderno-n-1.pdf; G. Giannone Codiglione, *Motori di ricerca, trattamento di dati personali ed obbligo di rimozione: diritto all'oblio o all'autodeterminazione informativa?*, in *Nuova giur. civ. comm.*, 2014, 1072-1079.
A tal proposito si ricorda l'atteso Regolamento (UE) 2016/679 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati*, con applicazione diretta a partire dal 25 maggio 2018 (per un primo commento si rinvia a F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016), dove si assiste al trionfo della c.d. autodeterminazione informativa (per approfondimenti si rinvia a A. Thiene, *Segretezza e riappropriazione*, cit., spec. 428). Questo Regolamento presenta una previsione molto attesa: l'art. 17 c.d. diritto all'oblio. Si tratta specificatamente della previsione contenuta nel primo paragrafo dell'art. 17, alla lett. *f*), in cui si contempla il diritto alla cancellazione quando i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'art. 8, par. 1. Previsione che può essere compresa solo attraverso una lettura sinottica del 65° *considerando* («un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che lo riguardano e il "diritto all'oblio" se la conservazione di tali dati violi il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento. In particolare, l'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento. Tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore [...]») dove si afferma che il diritto alla cancellazione è particolarmente rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento. L'interessato, tuttavia, dovrebbe poter eliminare tale tipo di dati personali, in particolare in una realtà sempre più distante dalla materialità quale Internet, indipendentemente dal fatto che non sia più minore. Gli utenti potranno, quindi, esigere dal titolare del trattamento la cancellazione delle informazioni inserite *online* in violazione della regola contenuta all'art. 8 relativa all'età minima necessaria per poter esprimere validamente in autonomia il consenso al trattamento dei dati effettuati da siti di socializzazione (A. Thiene, *Segretezza e riappropriazione*, cit., 425-426). Si rileva, altresì, come «nell'articolo rubricato con una, forse indebita, sovrapposizione dei termini oblio e cancellazione, vengono individuate delle situazioni tassative in cui è possibile esercitare il diritto alla cancellazione, disciplinato ora in modo molto più specifico rispetto al generico richiamo contenuto all'art. 12 (*Diritto all'accesso*) della Direttiva 95/46/CE e al corrispondente art. 7, par. 3, lett. *b* (*Diritto all'accesso ai dati personali ed altri diritti*)» (cit., 426-427). Lo scopo del Regolamento è di rappresentare «una poderosa opera di riorganizzazione e di riformulazione del diritto europeo sulla protezione dei dati personali a un livello di generalizzazione adeguato a un testo normativo che mira a essere il perno, o ancor meglio la cornice, della legislazione europea in materia» (F. Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2, 2017, 375).

[10] Trib. Roma, sez. I civ., 3 dicembre 2015, n. 23771, in *Danno e resp.*, 3, 2016, 299-302, con commento di F. Russo, *Diritto all'oblio e motori di ricerca: la prima pronuncia dei Tribunali italiani dopo il caso* Google Spain, 302-309. La pronuncia, nel tentativo di operare un bilanciamento tra il diritto all'oblio e l'interesse pubblico a rinvenire notizie sul *web*, applica i principi elaborati dalla Corte di giustizia UE nella sentenza sul caso *Google Spain*, in una vicenda in cui un avvocato chiedeva al giudice di obbligare un motore di ricerca (nel caso di specie, *Google*) a rimuovere dai propri risultati (cd. "deindicizzazione") i *link* a quei siti che riteneva lesivi del suo "diritto all'oblio" (o "*right to be forgotten*"). Orbene, si trattava di una vicenda giudiziaria (risalente agli anni 2012/2013), relativa a presunte truffe e guadagni illeciti legati alla c.d. banda della Magliana, nella quale l'avvocato ricorrente era rimasto coinvolto senza tuttavia esser mai stato condannato. Il giudice di merito ha rigettato la domanda dell'avvocato, sul presupposto che l'interesse pubblico a rinvenire sul *web*, attraverso il motore di ricerca gestito dalla società resistente, notizie circa il ricorrente deve prevalere sul diritto all'oblio del professionista, anche in considerazione dell'assenza del requisito del trascorrere del tempo e del ruolo svolto dall'interessato nella vita pubblica.

persona derivante dalla reiterata pubblicazione di una notizia (ovvero nella specie il permanere della sua indicizzazione sui motori di ricerca), con pregiudizio alla propria reputazione e riservatezza (attesa l'attenuazione dell'attualità della notizia e dell'interesse pubblico all'informazione con il trascorrere del tempo dall'accadimento del fatto)»[11].
Il rapporto tra il diritto all'oblio e le informazioni veicolate dalla "implacabile invadenza dei motori di ricerca"[12] è stato al centro dell'importante sentenza europea della Corte di giustizia UE (caso *Google Spain*) del 2014[13], la quale affronta la problematica concernente la possibilità per una persona di far valere il proprio diritto all'oblio formulando ai motori di ricerca[14] apposita richiesta di non indirizzare gli utenti su una determinata risorsa contenente una notizia ormai non attuale e non più gradita, al fine di ripristinare l'anonimato di quella persona.
La questione ha avuto un grande impatto mediatico, in quanto pone il quesito «se il diritto dell'Unione europea conferisca agli individui il diritto di ottenere la rimozione dei propri dati personali da parte dei soggetti che ne effettuano il trattamento su Internet, quando le finalità per le quali tale trattamento si svolge siano già state soddisfatte o siano venute meno. (…) Questione dibattuta (…), è se un siffatto diritto possa dirsi esistente anche in assenza di un esplicito riconoscimento legislativo, e se - traendo spunto da alcune disposizioni della Carta - le corti siano abilitate a garantirne l'*enforcement*»[15].

[11] Trib. Roma, sez. I civ., 3 dicembre 2015, n. 23771, in *Danno e resp.*, cit., 300.

[12] L'espressione è di A. Thiene, *Segretezza e riappropriazione*, cit., 434, ove l'Autrice afferma come l'azione pervasiva dei motori di ricerca, consentendo di individuare informazioni attraverso l'inserimento di una parola chiave (nome della persona), determini una forma di controllo sulla vita delle persone: «questa consapevolezza, già apparsa in una ridda di provvedimenti del Garante, è nitidamente emersa anche nel pensiero della Corte di giustizia, nella oramai celebre la sentenza Google Spain (…) decisione destinata ad incidere in modo rivoluzionario sulle modalità di circolazione delle notizie».

[13] C-131/12, cit.

[14] Sul ruolo dei motori di ricerca, i quali, tuttavia, facilitano la violazione del diritto all'oblio, costituendo «un complesso sistema informatico, composto da elementi *software* e *hardware* che vengono tutti combinatamente impiegati dal soggetto che gestisce il motore di ricerca per consentire all'utente di ottenere i risultati richiesti» si rimanda a P. Sammarco, *Il motore di ricerca, nuovo bene della società dell'informazione: funzionamento, responsabilità e tutela della persona*, in *Dir. inf.*, 2006, 622.

[15] O. Pollicino, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in www.forumcostituzionale.it, 31 dicembre 2013, 15, ove in particolare, l'A. rileva come le conclusioni rassegnate dall'Avvocato generale (Niilo Jääskinen) documentino la valorizzazione interpretativa che, nel nuovo contesto tecnologico, sembra caratterizzare il portato normativo della Carta di Nizza-Strasburgo quale parametro privilegiato, e finalmente di natura super primaria, per le operazioni di bilanciamento da parte dei giudici di Lussemburgo. Dunque, ci si domanda se l'art. 7 e 8 della Carta, in combinato disposto con alcune disposizioni contenute nella direttiva 95/46 (segnatamente, l'art. 12, lett. b) e l'art. 14, lett. a) che attribuiscono agli interessati, rispettivamente, il diritto di ottenere la cancellazione o il blocco dei dati e il diritto di opporsi al trattamento), possano offrire un fondamento giuridico al diritto all'oblio. A tale quesito risponde l'Avvocato generale, per il quale nessun generalizzato diritto all'oblio può desumersi in alcun modo dalle disposizioni della direttiva, nemmeno se interpretate conformemente al parametro "costituzionale" dell'art. 7 della Carta. Infatti, secondo il ragionamento dell'Avvocato generale, se i gestori dei motori di ricerca in Internet fossero gravati della rimozione dei risultati segnalati dagli utenti come lesivi dei propri diritti, senza una previa consultazione o richiesta del gestore delle rispettive pagine *web*, si assisterebbe a una combinazione non equilibrata tra la libertà di espressione e di informazione e la tutela della vita privata degli interessati.

Si coglie, così, l'evoluzione che ha interessato il diritto all'oblio[16], il quale nasce per indicare il diritto all'attualità della notizia per poi, oggi, realizzarsi come «diritto al controllo della propria immagine sociale nella rete Internet, esprimendo l'esigenza di una dimensione attualizzata dei propri dati e della propria identità personale nei *social networks*»[17].

[16] C'è chi in dottrina (G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. inf.*, 4-5, 2014, 591-604) opportunamente rileva come l'espressione "diritto all'oblio" venga utilizzata almeno in tre differenti accezioni.
Secondo una prima accezione, con il diritto all'oblio si fa riferimento al diritto di un soggetto a non vedere pubblicate alcune notizie relative a vicende, già legittimamente pubblicate, rispetto all'accadimento delle quali è trascorso un notevole lasso di tempo; per questa accezione, dunque, il diritto all'oblio è relativo a vicende che hanno costituito fatti di cronaca o comunque in relazione alle quali la pubblicizzazione, cioè la fuoriuscita dalla sfera della riservatezza degli interessati, era da considerarsi lecita (cit., 592). Già in questa prima definizione il tempo gioca un ruolo importante anche qualora non si tratti di eventi di cronaca, ma di eventi in relazione ai quali un periodo significativo sia ormai trascorso e invece manchino elementi di contestualizzazione nel tempo: ecco perché, in questi casi, la giurisprudenza ha ravvisato la violazione del diritto all'identità personale (cit., 593).
Una seconda accezione, invece, si può ravvisare con l'utilizzo di Internet e delle reti telematiche per diffondere l'informazione. In questi casi, infatti, non si tratta solo o necessariamente di una ripubblicazione dell'informazione, ma piuttosto di una permanenza della stessa nella rete, giacché muta l'esigenza che si vuole soddisfare. Infatti, in tali casi, «il tempo da considerare non è più quello trascorso tra la pubblicazione dell'informazione e la ripubblicazione, ma quello trascorso dal tempo della pubblicazione che perdura. (…) Siamo di fronte ad un *continuum* temporale e non più a due eventi puntuali», sicché l'esigenza non è quella di non ripubblicare bensì quella di collocare la pubblicazione, avvenuta magari legittimamente molti anni addietro, nell'attuale presente (cit., 593), nell'ambito di uno scenario che vede l'identità come protagonista.
Per una terza accezione, infine, in sintonia con la proposta di regolamento europeo generale sulla protezione dei dati, il diritto all'oblio «si riferisce al diritto alla cancellazione, al blocco, al congelamento dei dati o all'opposizione al trattamento dei dati previsti dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"(cit., 594); in questa prospettiva, volendo delineare i confini «si può definire la cancellazione come un'operazione sui dati che esclude ogni ulteriore conservazione degli stessi, mentre l'oblio sembra piuttosto essere una finalità, che si può raggiungere con la cancellazione, ma anche con il blocco» (cit., 596).
Nelle prime due accezioni, il diritto all'oblio «appare strumentale al diritto all'identità personale» (cit., 600), poiché in entrambi i casi il bene giuridico tutelato è quello dell'identità personale; viceversa, nella terza accezione, il diritto all'oblio consiste nella cancellazione dei dati, in quanto (in questo caso) la protezione dei dati personali costituisce il bene giuridico da tutelare. Dunque, in questo ultimo caso, «il diritto a cancellare è strumentale al diritto alla protezione dei dati personali. Il dato personale può essere cancellato, come afferma la Corte, se non è più adeguato, aggiornato pertinente» (cit., 601). Tuttavia è bene sottolineare che «i due diritti in considerazione, il diritto all'identità personale il diritto alla protezione dei dati personali, sono diritti molto vicini e volti a tutelare un unico bene: quello dell'identità della persona» (*ibidem*).
Con riferimento al dato temporale, inoltre, l'Autrice conclude asserendo che «il tempo gioca un ruolo essenziale: la persona è ciò che è in un determinato momento storico e l'identità muta col tempo. Divengono essenziali la contestualizzazione e la storicizzazione. Eventi occorsi in una certa epoca possono non corrispondere più alla personalità di un soggetto in un diverso momento storico. Sul terreno di questo conflitto, fra la verità della storia e l'identità attuale, nasce il diritto all'oblio» (cit., 602).

[17] C.M. Bianca, *Istituzioni*, cit., 102. In tal senso anche C. D'Agata, *Danni da illegittimo trattamento dei dati personali: riservatezza, protezione dei dati e diritto all'oblio*, in G. Cassano (a cura di), *Il danno alla persona*, Milano, 2016, 666, ove l'Autrice afferma che la «tematica (…) del diritto all'oblio che, nata sotto l'egida del diritto alla riservatezza in senso stretto, sta assumendo una collocazione ben più complessa intersecando, sotto diversi profili, la protezione dei dati, l'identità personale e il diritto alla c.d. "immagine sociale"». Cfr. S. Niger, *Il diritto all'oblio*, in G. Finocchiaro (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, Padova, 2007, 59 ss.; T. Auletta, *Diritto alla riservatezza e "droit à l'oubli"*, in G. Alpa - M. Bessone - L. Boneschi - G. Caiazza (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, 127 ss.

2. Il diritto all'oblio nell'informazione "indomabile" di Internet

C'è chi con profondità e creatività si è interrogato su chi, nel mondo contemporaneo, abbia il compito di scrivere un "palinsesto della vita"[18] di nuovo conio, nella consapevolezza che l'autodeterminazione della persona esprima la più intensa libertà sia esistenziale che giuridica: su questo sfondo si staglia la questione dei rapporti tra autonomia, autodeterminazione e partecipazione.

La partecipazione alla socialità spesso riduce la libertà dell'individuo a favore di una identità atomistica o seriale, che non supera l'insidia di «un fenomeno anomalo e allarmante di omologazione sociale e di obliterazione della diversità, intesa e percepita come un ingombro»[19].

Questo accade anche perché all'identità (che si incastrava perfettamente nel precedente momento storico, ma non più nella condizione contemporanea) oggi sembra sostituirsi l'"identificazione", concepita come (non un prodotto finito ma) un incessante e infinito processo di riproduzione e riciclo.

L'identità, invece, è l'immagine della persona che si evince dalle interazioni sociali nella prospettiva pubblica, delineando così un prodotto finito (si pensi a un documento di riconoscimento) che si pone tra la persona e l'ambiente, con il conseguente riconoscimento della persona con riferimento alle altre persone. Diversamente opera la identificazione, che è capace di moltiplicare l'identità ricreandola in una discontinuità di relazioni che vengono costantemente negoziate. Senza trascurare che il «web, agendo come vetrina dell'identità umana, ha lasciato vittime sulla propria rete di connessione: tanti infatti sono stati i suicidi come conseguenza di un accanimento subdolo e violento nei confronti di individui particolarmente fragili»[20].

Del resto, «la razionalità tecnologica ha formalizzato un modo di affrontare la questione dell'identità che approda a procedure di costruzione nelle quali il contributo dell'altro non si affianca all'autonomia della persona, ma tende a sovrapporsi a essa, a sostituirla. (…) ad esempio con l'algoritmo di Google che stabilisce quali siano le informazioni che, per prime, compaiono quando si avvia una ricerca, così la decisione complessiva su che cosa sia l'identità di una persona può essere trasferita a sistemi che ordinano secondo la propria logica le informazioni ricevute e proiettano all'esterno la

[18] S. Rodotà, *Il diritto di avere diritti*, Bari, 2012, 250, ove l'A. afferma che «a questa domanda, espressa in forma insolita, è stata data una risposta che cerca di ridefinire non solo e non tanto le modalità del rapporto tra giuristi e scienziati, ma il ruolo stesso del diritto, da una parte, e di biologia e genetica, dall'altra, individuando così anche le condizioni che contribuiscono a definire il contesto all'interno del quale la persona si autodetermina».

[19] C. Mazzù, *Riflessioni sullo* status *tra passato e futuro*, in *Il diritto civile all'alba del terzo millennio*, v. I, *Famiglia - Successioni - Contratto - Patrimoni separati*, Torino, 2011, 44.

[20] T. Leoncini, *Trasformazioni sessuali e amorose. Decadenza dei tabù nell'era dell'e-commerce sentimentale*, in Z. Bauman - T. Leoncini, *Nati liquidi. Trasformazioni nel terzo millennio*, Milano, 2017, 70. Cfr. A. Thiene, *Segretezza e riappropriazione*, cit., 440, ove l'Autrice, richiamando la sentenza partenopea sulla drammatica lesione dell'intimità personale di una donna che a causa di ciò si è suicidata, ha affermato che innanzi «all'incrudelirsi delle aggressioni alla riservatezza e alla reputazione, che possono tingersi della drammaticità che ben conosciamo proprio perché amplificate dalla possibilità di pubblicazione e condivisione senza filtri di immagini e informazioni con un numero infinito di utenti, il diritto alla cancellazione costituisce uno strumento più che mai prezioso».

"loro" rappresentazione della persona. Giungiamo così a identità "fratturate" dall'attraversamento di troppi confini, virtuali certamente, ma drammaticamente reali»[21].
Attraverso Internet, che sfuggendo al principio di territorialità della legge, ostacola l'ingresso della norma per tutelare i diritti lesi, una persona può costruirsi diverse identità, ma può anche desiderare l'aggiornamento o la cancellazione di notizie non più rappresentative della sua posizione sociale. Escluse le ipotesi, in media meno frequenti, in cui le persone sono coinvolte in fatti di cronaca, capita quasi a tutti di vedere, anche contro la propria volontà, una propria immagine in Internet, o perché inserita in un "*post*" da altri o perché il motore di ricerca assorbe una foto da noi inserita in un *social network*. Ecco che, quindi, è sufficiente consultare un comune motore di ricerca, inserendo il nominativo di una qualunque persona, per attingerne informazioni, che tuttavia possono essere sgradite e non più adeguate a "rappresentare" all'esterno quella determinata persona che, per quanto detto, ha «un diritto ad essere dimenticato allorquando la vicenda è da ritenersi conclusa e non più di rilievo per la collettività»[22].
Già Aristotele disquisiva di oblio politico greco, quando riassumeva il "patto a non ricordare", il "decreto dell'oblio voluto nel 403 a.C. da Trasibulo per porre fine alla guerra civile, dopo la cacciata da Atene dei Trenta Tiranni: secondo questo patto "nessuno ha più diritto di serbare rancore del passato contro un altro"[23]; dunque, la riappacificazione passava attraverso l'esplicito divieto di ricordare. Questo «patto è stato ripetutamente indicato come modello di prevalenza dell'oblio sulla memoria, espressione dunque di realismo politico e non di attenzione per la verità»[24].
Dunque la questione ruota attorno all'interrogativo su come e quando sia possibile coordinare la memoria sociale e il diritto all'oblio, che il singolo vuole difendere.
L'evoluzione della finalità del diritto all'oblio induce a riflettere sulla potenzialità lesiva dei *social networks* quando vengono utilizzati dagli utenti con il precipuo scopo di minare la serenità altrui e, altresì, della perenne possibilità di usufruire di notizie passate, in una dimensione in cui la «privacy (…) eliminata dal discorso morale e politico» diventa «un pezzo di anticaglia destinato a soccombere di fronte all'irresistibile fascino della condivisione»[25].
Per queste ragioni è importante che il soggetto a cui appartengono i dati personali possa avere un diritto al "controllo" alla contestualizzazione e all'aggiornamento della propria immagine sociale. In tal senso si è orientata la Cassazione civile a partire dal 2012, quando con una importante pronuncia, che costituisce un *leading case* nel riconoscimento del diritto all'oblio, ha affermato che in caso di memorizzazione nella rete Internet, mero deposito di archivi dei singoli utenti che accedono alla rete e cioè dei titolari dei siti costituenti la fonte dell'informazione (c.d. siti sorgente), deve riconoscersi al soggetto cui appartengono i dati personali oggetto di trattamento ivi contenuti il diritto all'oblio, e cioè al relativo controllo a tutela della propria immagine sociale che,

[21] S. Rodotà, *Il diritto*, cit., 302-303.

[22] M. Mezzanotte, *La memoria conservata in* internet *ed il diritto all'oblio telematico: storia di uno scontro annunciato*, in *Dir. int.*, 4, 2007, 399.

[23] Aristotele, *La Costituzione degli Ateniesi*, 39.6.

[24] S. Rodotà, *Il diritto*, cit., 215.

[25] A. Thiene, *Segretezza e riappropriazione*, cit., 410.

anche quando trattasi di notizia vera, e *a fortiori* se di cronaca, può tradursi nella pretesa alla sua contestualizzazione e aggiornamento, se del caso, avuto riguardo alla finalità della conservazione nell'archivio e all'interesse che la sottende, financo alla relativa cancellazione[26].

Infatti, la concezione del diritto all'oblio è mutata con l'avvento di Internet, poiché in rete l'informazione permane, in modo gratuito e libero, astrattamente disponibile all'infinito, con l'aggravante della sincronica capacità di collegamento dei motori di ricerca[27] che determina la presenza della notizia in Rete in diversi siti e in diverse forme contemporaneamente.

Ciò conferisce natura dinamica alla tutela della *privacy* devolvendo al titolare il controllo della diffusione delle notizie passate che lo riguardano, senza trascurare la particolare evoluzione della latitudine del diritto ad essere dimenticati, giacché da diritto prevalentemente elitario è diventato un diritto attribuito alla generalità dei soggetti.

Il fenomeno non coinvolge solo persone "pubblicamente" note, ma anche la singola identità dei consociati che non devono subire all'esterno l'alterazione del proprio patrimonio intellettuale, professionale, etico. Ecco, dunque, perché la giurisprudenza considera il diritto all'oblio quale diritto a "contestualizzare" le informazioni della persona presente, senza incorrere nella riproposizione informatica di notizie a lui risalenti nel tempo e non desiderate, poiché legate a momenti lontani e dissimili dalla attuale condizione sociale, che perciò rischierebbe di non essere aggiornata e anche discreditata.

Quindi il diritto all'oblio si rafforza o si affievolisce a seconda dell'attualità dell'interesse pubblico alla conoscenza di determinati avvenimenti. In questa prospettiva, perciò, è decisivo il trascorrere del "tempo", il quale fa riacquistare l'originaria natura di fatto privato ad avvenimenti che sono stati oggetto di vicende giudiziarie, così come evidenziato dalla sentenza n. 23771/2015 del Tribunale di Roma, secondo la quale «il trascorrere del tempo, ai fini della configurazione del diritto all'oblio, si configura quale elemento costitutivo, come risultante anche dalla condivisibile sentenza n. 5525/2012 della Suprema Corte, nella quale questo viene configurato quale diritto "a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino oramai dimenticate o ignote alla generalità dei consociati"» [28].

Viceversa, se le notizie sono recenti, è esclusa la sussistenza in capo alla persona di un

[26] Cass. civ., sez. III, 5 aprile 2012, n. 5525, in *Danno e resp.*, 7, 2012, 750, con commento di F. Di Ciommo - R. Pardolesi, *Notizia vera, difetto di attualità, diritto all'oblio*, 753; in *Nuova giur. civ. comm.*, 2012, 836-843, con nota di A. Mantelero, Right to be forgotten *ed archivi storici dei giornali. La Cassazione travisa il diritto all'oblio*, 843-849. La fattispecie riguarda la vicenda di un esponente politico di un piccolo Comune lombardo, il quale viene arrestato nel 1993 per corruzione ma, alla fine del procedimento giudiziario, viene prosciolto. A distanza di molti anni, il politico lamentava che ancora la notizia che appariva in rete era quella dell'arresto ma senza alcun riferimento al successivo epilogo (il proscioglimento dalle accuse) della vicenda giudiziaria. Con questa sentenza la corte di legittimità, «invocando il diritto all'oblio (*rectius* il diritto a ripristinare la completezza della notizia mercé aggiornamenti e integrazioni dell'originale), impone ai gestori di archivi storici l'obbligo di predisporre un sistema idoneo a segnalare la sussistenza di seguiti e sviluppi della notizia» (F. Di Ciommo-R. Pardolesi, *Notizia vera, difetto di attualità*, cit.).

[27] Infatti, c'è chi asserisce che «Corollario di tali premesse è che oggi Internet costituisce un'immensa banca dati; anzi una immensa banca di banche dati, continuamente arricchite da milioni di informazioni immesse in Rete ogni secondo, a carattere globale, senza soluzione di continuità, da chiunque voglia farlo» (F. Di Ciommo, *Quello che il diritto non dice. Internet e oblio*, in *Danno e resp.*, 12, 2014, 1103).

[28] Trib. Roma, sez. I civ., 3 dicembre 2015, n. 23771, in *Danno e resp.*, cit., 301.

diritto (non alla cancellazione del dato ma solo) alla deindicizzazione[29] delle informazioni contenute sul *web* attraverso i motori di ricerca.

Tuttavia, pur assumendo autonoma rilevanza, il diritto del soggetto a pretendere che le proprie vicende personali non siano pubblicamente rievocate, trova un limite nel diritto di cronaca[30], tutte le volte in cui sussista un interesse (speculare ma) effettivo ed attuale alla loro diffusione[31]. Ma, se non sussiste simile interesse, la notizia già pubblicata in precedenza deve essere aggiornata o cancellata: questo compito spetta al titolare del sito e non al motore di ricerca.

Ecco che si tratteggiano gli stretti legami tra il diritto all'oblio e i diritti di cancellazione, blocco, aggiornamento e opposizione al trattamento dei dati personali disciplinati dagli artt. 7 e 8 del codice della privacy; senza tralasciare il ruolo preventivo che l'Autorità

[29] Infatti, al diritto all'oblio si affianca quale sua specificazione «l'ulteriore e distinto interesse del soggetto a non vedere più comparire tra i risultati forniti agli utenti dai motori di ricerca e collegati al proprio nome le informazioni riguardanti la propria sfera personale» (F. Russo, *Diritto all'oblio e motori di ricerca*, cit., 304). Cfr. F. Di Ciommo – R. Pardolesi, *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la Rete, bellezza!*, in *Danno e resp.*, 7, 2012, 701-716.

[30] Il diritto di cronaca è una particolare espressione della libertà di stampa, la quale rientra nell'ambito della libertà di manifestazione del pensiero (art. 21 Cost.), ed è esercitabile a condizione che vengano rispettati tre concorrenti profili: veridicità del fatto, effettiva sussistenza di un interesse pubblico alla conoscenza della notizia e continenza espositiva. Siffatti limiti all'esercizio del diritto di cronaca sono stati enunciati prima dalla Cass. civ., sez. I, 18 ottobre 1984, n. 5259 (in *Foro it.*, 1984, I, 2711), poi dalla Cass. civ., sez. III, 4 settembre 2012, n. 14822 (in *DeJure*) e confermati dalla sentenza n. 5525/2012 (cit.) secondo cui l'interessato ha diritto a che l'informazione dei suoi dati risponda ai criteri di proporzionalità, necessità, pertinenza allo scopo, esattezza e coerenza con la sua attuale ed effettiva identità personale o morale. In altri termini il diritto di cronaca è esercitato correttamente tutte le volte in cui vengono rispettate le tre condizioni suindicate, e, per quanto riguarda l'oblio, con particolare riferimento al requisito della pertinenza, poiché l'interesse pubblico alla conoscenza del fatto oggetto di cronaca soccombe in caso di eccessivo sacrificio del diritto alla riservatezza.

[31] In tal senso si esprime giurisprudenza consolidata [tra cui si ricorda Cass. civ., sez. III, 26 giugno 2013, n. 16111, in *Danno e resp.*, 3, 2014, 271-274 (la fattispecie aveva ad oggetto il diritto all'oblio invocato da un soggetto che, in relazione ad un'antica militanza in bande terroristiche – Brigate rosse –, aveva scontato la relativa pena e, dunque, desiderava non essere più accostato, agli occhi della pubblica opinione, a fatti di terrorismo, trattandosi di una parte della sua esistenza ormai chiusa), con nota di commento di M.C. Daga, *Diritto all'oblio: tra diritto alla riservatezza e diritto all'identità personale*, 274-278] e recente dottrina: «se l'interesse pubblico alla persistente conoscenza di un fatto avvenuto in epoca di molto anteriore trova giustificazione nell'attività politica svolta dal soggetto titolare dei dati, e tale vicenda ha registrato una successiva evoluzione, non si può prescindere da quest'ultima altrimenti la notizia diviene non aggiornata e pertanto sostanzialmente non veritiera» (C. D'Agata, *Danni da illegittimo trattamento*, cit., 746).

Garante per la protezione dei dati personale è deputata a svolgere[32].

In questa direzione si collocano le copiose istanze volte ad ottenere l'aggiornamento della propria notizia (specie se oggetto di cronaca giornalistica), a salvaguardia della contestualizzazione della identità del soggetto[33], affinché essa non venga appiattita nel mare di Internet. In simili ipotesi, il provvedimento del Garante è rivolto non più al motore di ricerca ma all'editore, in quanto grava su quest'ultimo l'onere di predisporre, nell'ambito dell'archivio storico *online*, un sistema per l'aggiornamento dei dati idoneo a segnalare "l'esistenza del seguito o dello sviluppo della notizia in modo da assicurare all'interessato il rispetto della propria (attuale) identità personale, quale risultato della completa visione di una serie di fatti che lo hanno visto protagonista e ad ogni lettore di ottenere un'informazione attendibile e completa"[34].

[32] A tal proposito, il Garante ha rintracciato un punto di equilibrio fra le contrapposte esigenze, finalità giornalistiche e documentaristiche, facendo ricorso a protocolli informatici che permettano di interdire l'indicizzazione automatica, da parte dei motori di ricerca esterni ai siti internet in cui le pubblicazioni *online* sono riproposte, delle pagine o delle sezioni contenenti dati personali (tra i tanti, Gpdp., provv. del 27 gennaio 2016, doc. web n. 4749676). Tale soluzione è stata anche confermata dalla Corte di giustizia dell'Unione Europea (*Google Spain*) che ha avallato la posizione del Garante in ordine al riconoscimento in capo all'interessato del diritto ad ottenere la deindicizzazione del proprio nome da un certo risultato della ricerca effettuata dal *search engine* (C. D'Agata, *Danni da illegittimo trattamento*, cit., 668). Secondo questa pronuncia, infatti, il diritto all'oblio deve essere bilanciato con il diritto di cronaca e con l'interesse pubblico alla conoscenza dei fatti acquisibili per il tramite dei *links* forniti dal motore di ricerca (C. D'Agata, *op. ult. cit.*, 744).
Di diverso avviso rispetto alla sentenza della CGUE del 2014, si pone la pronuncia del 9 marzo 2017 (causa C-398/15) - *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. M.* (in *Notariato*, 3, 2017, 314-318, con commento di G. Arcella, *Il diritto all'oblio per i dati personali cede rispetto alle esigenze di pubblicità legale*, 318-323), con la quale la Corte di giustizia dell'Unione europea rinviene nell'esigenza di pubblicità dei dati personali contenuti in un Registro Pubblico un limite al diritto all'oblio. La fattispecie ha origine in Italia, dove l'amministratore unico di una società edile, a seguito di un appalto, ottenuto per la costruzione di un complesso turistico, si rivolge al Tribunale di Lecce per ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati presenti nel Registro delle Imprese che lo ricollegano al fallimento di una precedente società di cui era stato amministratore unico e liquidatore, evidenziando che la permanenza di tali dati lo danneggia nello svolgimento della sua attuale attività imprenditoriale. La Corte di giustizia, accogliendo le conclusioni dell'avvocato generale, afferma che la pubblicità del Registro delle imprese assolve ad una funzione pubblica essenziale, poiché garantisce la certezza del diritto nelle relazioni tra le società e i terzi: corollario di ciò è che il semplice trascorrere del tempo (nel caso di specie, un decennio) o la cessazione della società cui i dati di si riferiscono, non affievoliscono l'interesse dei terzi a consultare le informazioni contenute nel registro delle imprese. Ciononostante, la sentenza prevede che le persone fisiche interessate possano richiedere un accesso limitato ai dati personali ma tale valutazione spetta agli Stati membri. Cioè, «l'aver ribadito che esistono delle esigenze superiori rispetto agli interessi dei singoli, che permangono nonostante il decorso del tempo, significa che la pubblica fede, connessa a prerogative statuali, è riconosciuta come un valore» (G. Arcella, *Il diritto all'oblio per i dati personali*, cit., 323).

[33] Cfr. Cass. civ., 5 maggio 2012, n. 5525, in *Foro it.*, 2013, 305, secondo cui se una vicenda ha registrato una successiva evoluzione non può prescindersi dall'informazione in ordine a quest'ultima, giacchè altrimenti la notizia (originariamente completa e vera) diviene non aggiornata, risultando quindi parziale e non esatta, e pertanto sostanzialmente non vera.

[34] Garante privacy, provv. 24 gennaio 2013 (doc. web n. 2286820).

3. Una possibile tutela dell'oblio come manifestazione di "interesse legittimo"

Pur in assenza di una esplicita definizione legislativa, sia la giurisprudenza italiana[35] che la dottrina[36], in maniera unanime, hanno attribuito all'oblio natura di "diritto soggettivo". Ciononostante è possibile avanzare una diversa posizione teorica, che muove dalla teoria che individua l'esistenza dell'interesse legittimo nel diritto privato, intesa come situazione giuridica attiva posta a tutela del soggetto nei confronti di altri soggetti privati.

Come è noto, tra le situazioni giuridiche soggettive il diritto soggettivo ha un ruolo preminente, consistendo in una situazione giuridica attiva, di vantaggio, che attribuisce al suo titolare "la liceità di agire per la soddisfazione di determinati interessi"[37].

Al pari del diritto soggettivo, come situazione giuridica attiva, vi è l'interesse legittimo che, viceversa, ha sempre dovuto "stentare" per ottenere pieno riconoscimento (prima) nel diritto amministrativo[38], in quanto la sua irrisarcibilità era un caposaldo della dottrina tradizionale e costituiva l'archeologia della regola[39], nonostante la formale tutela attribuitagli dalla nostra Costituzione (art. 24 Cost).

In dottrina, a cogliere l'essenza dell'interesse legittimo, in considerazione del suo stretto legame con l'esercizio del potere pubblico, è pervenuta la teoria normativa di Mario Nigro, che ravvisa nell'interesse legittimo una posizione qualificata di vantaggio, che conferisce al titolare poteri atti ad influire sullo svolgimento dell'azione amministrativa per conseguire il bene finale.

Mentre, ad oggi, nel terreno amministrativo l'interesse legittimo ha comunque natura attiva, così non è nel campo privato[40] dove l'interesse legittimo è stato ricostruito come

---

[35] Cfr.: Cass. civ., sez. III, 9 aprile 1998, n. 3679, in *Danno e resp.*, 1998, 882-883; Cass. civ., sez. I, 18 ottobre 1984 n. 5259, in *Giur. it.*, 1985, 762; Trib. Roma, 15 maggio 1995, in *Dir. inf. e informatica*, 1996, 427; Cass. pen., sez. V, 24 novembre 2009, n. 45051, in *Studium Iuris*, 2010, 577.

[36] Tra i tanti che, seppur implicitamente, si evince accolgono la natura di diritto soggettivo, si ricordano: F. Di Ciommo, *Quello che il diritto non dice. Internet e oblio*, cit.

[37] Questa teoria, travalicando l'impostazione tradizionale che identifica il diritto soggettivo nel potere, attribuisce valore fondamentale al momento della liceità, definendo così il diritto soggettivo come "*ágere licère*"(D. Barbero, *Il diritto soggettivo*, in *Foro it.*, IV, 1939, 42)

[38] Per una ricostruzione si rimanda a: A. Falzea, *Gli interessi legittimi e le situazioni giuridiche soggettive*, in *Riv. dir. civ.*, I, 2000, 680 ss.; G. Alpa, *Il révirement della Corte di Cassazione sulla responsabilità per lesione di interessi legittimi*, in *Resp. civ. prev.*, 4-5, 1999, 907 ss.; A. Romano, *Sono risarcibili; ma perché devono essere interessi legittimi?*, in *Foro it.*, 1999, 3222 ss.; M. Protto, *Crolla il muro dell'irrisarcibilità delle lesioni di interessi legittimi: una svolta epocale?*, in *Urb. app.*, 1999, 1067 ss.; A. Di Majo, *Il risarcimento degli interessi "non più solo legittimi"*, in *Corr. giur.*, 11, 1999, 1376 ss.; F.D. Busnelli, *Lesione di interessi legittimi: dal muro di sbarramento alla rete di contenimento*, in *Danno e resp.*, 1997, 269 ss.; S. Giacchetti, *La risarcibilità degli interessi legittimi e Don Ferrante*, in *Rass. Cons. St.*, 1997, 1471 ss.; F.G. Scoca, *Contributo sulla figura dell'interesse legittimo*, Milano, 1990; Id., *Ma che cos'è questo interesse legittimo?*, in *Foro amm.*, 1988, 331 ss.

[39] Prima della Cass. civ., sez. un., 22 luglio 1999, n. 500 (in *Giust. civ.*, I, 2261 ss.). Cfr.: F. Satta, *La sentenza n. 500 del 1999: dagli interessi legittimi ai diritti fondamentali*, in *Giur. cost.* 1999, 3236; S. Giacchetti, *La risarcibilità degli interessi legittimi è «in coltivazione»*, in *Cons. St.*, II, 1999, 1598 ss.

[40] Ad ammettere per la priva volta, nel diritto privato, la configurabilità di interessi legittimi, fu Cass. civ., sez. un., 2 novembre 1979, n. 5688 (in *DeJure*). Il dibattito è stato avviato in occasione del c.d. "caso Santhià", cioè del licenziamento che ha coinvolto un lavoratore per ragioni politiche. Altresì, di recente cfr. Trib. Trani, ord. 22 settembre 2011 (in *DeJure*).

situazione di vantaggio ma *inattiva*[41], poiché il soddisfacimento dell'interesse non dipende dalla condotta del titolare ma dall'esercizio di un potere di natura privatistica da parte di un altro soggetto. Affinché possa configurarsi questa situazione, è necessario che il potere, che fa da contraltare all'interesse legittimo, sia limitato da norme che ne disciplinano (in modo non vincolante) le modalità di esercizio, lasciando al soggetto un certo margine di discrezionalità in ordine al suo uso.

Oggi si registra nel diritto privato lo stesso atteggiamento di ritrosia sviluppatosi nel campo amministrativo, al punto da confermare l'affermazione di Nigro[42], per il quale l'interesse legittimo rappresentava uno dei più grossi rompicapo della teoria generale del diritto.

A tal proposito c'è chi[43], partendo dalle acquisizioni teoriche della Scuola pisana e riconsiderando le categorie fondamentali del diritto civile, ritiene: che il catalogo dei contesti di operatività dell'interesse legittimo nel diritto privato sia suscettibile di integrazione; che l'interesse legittimo di diritto privato sia un situazione giuridica totalmente attiva; che il comportamento del soggetto titolare dello speculare potere non può essere esercitato in modo meramente arbitrario ma in modo discrezionale, seppur attenendosi ai principi di buona fede e sussidiarietà.

In particolare, degno di nota appare il ruolo della figura dell'interesse legittimo nella ricostruzione della disciplina sul trattamento dei dati sensibili (concessione e/o revoca), nella dialettica tra diritto alla *privacy* e diritto alla notizia, nel «noto dibattito sul "diritto all'oblio", in cui il fattore "tempo"[44], quale indice di attualità e, solo per questo, di meritevolezza dell'interesse alla notizia, assolve alla funzione di misuratore del sacrificio esigibile dal privato rispetto al diritto di cronaca»[45]. La possibile ricostruzione dell'oblio come interesse legittimo può delinearsi per la lesione che il privato subisce in caso di notizia, non più veritiera ed attuale, che permane nei motori di ricerca; se fosse un diritto soggettivo la richiesta di rimozione dei dati dovrebbe essere più semplice e, anzi, operare automaticamente; mentre, l'effettiva tutela della posizione del privato è rimessa all'affidamento di un comportamento improntato alla correttezza da parte dei

[41] La tesi è della Scuola Pisana, in particolare di L. Bigliazzi Geri, *Contributo ad una teoria dell'interesse legittimo nel diritto privato*, Milano, 1967. Infatti l'Autrice considera il diritto soggettivo «una tipica situazione attiva e di vantaggio, cioè attiva-attiva» (cit., 18), mentre l'interesse legittimo come una «situazione bensì di vantaggio, e in questo senso attiva, ma, per il resto, sostanzialmente inattiva» (cit., 19), dunque si tratta di una situazione "inattiva-attiva". L'inattività indica che manca un contenuto specifico di attività e, perciò, che la realizzazione dell'interesse è subordinata ad una condotta altrui.
Nel 1998, nei giorni 29-30 maggio, è stato organizzato a Pisa un Convegno di Studi dal titolo "Il diritto privato nel prisma dell'interesse legittimo", in ricordo della prof.ssa Lina Bigliazzi Geri, i cui contributi sono pubblicati in U. Breccia - L. Bruscuglia - F.D. Busnelli (a cura di), *Il diritto privato nel prisma dell'interesse legittimo*, Torino, 2001. Attraverso questo scritto i colleghi e gli allievi pisani hanno adattato la figura dell'interesse legittimo di diritto privato a nuovi orizzonti, come il trattamento dei dati personali e la disciplina consumeristica.

[42] Cfr. M. Nigro, *Silvio Spaventa e la giustizia amministrativa come problema politico, Studi in onore di A. Papaldo*, Milano, 1975.

[43] C. Mazzù, *La logica inclusiva dell'interesse legittimo nel rapporto tra autonomia e sussidiarietà*, Torino, 2014.

[44] Indiscutibilmente il "tempo" assolve un ruolo importante nei fenomeni giuridici; infatti, c'è chi ne disquisisce in termini di "tempo vuoto" (che rappresenta un tempo senza interessi umani), come "tempo senza eventi e senza comportamenti" (A. Falzea, *Fatto naturale*, in *Ricerche di teoria generale del diritto e di dogmatica giuridica*, *II. dogmatica giuridica*, Milano, 1997, 375), o di "tempi e spazi riempiti" (cit., 374).

[45] Sia consentito il rinvio a A. Vesto, *Interessi legittimi, normativa antitrust e disciplina sulla* privacy, in C. Mazzù, *La logica inclusiva*, cit., 279-280.

gestori dei motori di ricerca.
Negli ultimi anni si è avuto un incremento delle istanze per avviare la procedura di segnalazione dei contenuti *online* che il richiedente desidera vengano rimossi dai servizi dei motori di ricerca, ai sensi delle leggi vigenti.
Anche da qui la riprova dell'acquisita maggiore coscienza dell'operatività dello strumento giuridico di protezione, inquadrato nella dinamica delle situazioni giuridiche ricostruite secondo una logica dialettica fondata sul principio di uguaglianza e di tutela della persona umana ed in un'ottica solidale.

Impiego di droni armati nella lotta al terrorismo e accesso alla giustizia da parte delle vittime*

Nicola Colacino

Abstract

L'articolo propone alcune brevi riflessioni sul tema della protezione delle vittime delle missioni antiterrorismo effettuate mediante velivoli a pilotaggio remoto (più comunemente noti come droni), muovendo dall'analisi della limitata, eppur significativa, prassi internazionale. L'indagine non perviene a conclusioni definitive, ma intende piuttosto evidenziare alcuni aspetti solo marginalmente considerati nel dibattito dottrinale, con l'obiettivo di contribuirvi da una prospettiva diversa. In particolare, si ritiene che, in determinate circostanze, l'uso dei droni come strumento di lotta al terrorismo internazionale abbia contribuito a innovare le regole dello *ius ad bellum*, rendendo possibile l'esecuzione più capillare e diffusa di missioni di *targeted killing* considerate, invece, troppo rischiose se condotte con strumenti e tecnologie tradizionali. Il numero delle vittime causate da tali missioni deve, pertanto, essere calcolato in termini assoluti e non relativi (come sembra, invece, suggerire la diplomazia ufficiale degli Stati interessati). Ciò presenta un'incidenza sulla valutazione dell'obbligo di riparazione, che deve tener conto dell'assenza di un chiaro contesto normativo in cui gli attacchi dei droni risultano inquadrabili.

The article offers some brief reflections on the issue of the protection of victims of counter-terrorism missions carried out through Unmanned Aerial Vehicles (UAVs, more commonly known as drones), moving from the analysis of the limited, but significant, international practice. The survey does not come to definitive conclusions, but rather intends to highlight some aspects only marginally considered in the doctrinal debate, with the aim of contributing to it from a different perspective. In particular, it is believed that the use of drones, in certain situations, has contributed to innovate the *ius ad bellum* rules, making possible the widespread execution of targeted killing missions that would otherwise be considered too risky. The number of victims caused by these missions must therefore be considered in absolute and not relative terms (as the official diplomatic positions seems to suggest). This has an impact on the assessment of the obligation to repair, which must take into account the absence of a clear regulatory framework in which drone attacks can be classified.

Sommario

1. Introduzione. – 2. La controversa legittimità dei "*drone strikes*" con finalità di antiterrorismo in base alle regole dello *ius ad bellum*. – 3. La posizione del governo statunitense. – 4. L'assenza di rimedi giurisdizionali a tutela delle vittime secondo la prassi rilevante e l'insufficienza delle riparazioni *ex gratia*. – 5. Considerazioni di sintesi.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio anonimo, in quanto riproduce la relazione presentata dall'A. al convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno" (Messina, 26-27 maggio 2017).

Keywords: Droni, Terrorismo, *Ius ad bellum,* Vittime, Obbligo di riparazione

1. Introduzione

Il presente lavoro propone alcune brevi riflessioni sul tema della tutela spettante alle vittime delle missioni antiterrorismo eseguite tramite velivoli a controllo remoto (*Unmanned Aerial Vehicles - UAVs*, più comunemente noti come *droni*), muovendo dall'analisi della limitata, eppur significativa, prassi rilevante. L'indagine qui condotta non perviene a conclusioni definitive, ma intende piuttosto mettere in evidenza alcuni aspetti solo marginalmente considerati nel dibattito dottrinario acceso intorno al tema di cui si discute, allo scopo di contribuirvi da una prospettiva diversa[1].

È ormai da oltre quindici anni[2] che l'impiego di droni in operazioni militari e di «polizia internazionale» è divenuto di uso corrente, al punto da caratterizzare la stessa strategia di contrasto condotta dal governo statunitense (in particolare sotto la Presidenza di Barack Obama e quella attuale di Donald Trump) nei confronti di gruppi terroristici di matrice fondamentalista.

I vantaggi derivanti dal ricorso a questa nuova tecnologia sotto l'aspetto del rapporto tra costi e benefici sono, in effetti, piuttosto evidenti. È sufficiente avere riguardo alla circostanza che l'uso dei droni assicura, a fronte di un'elevatissima percentuale di successo e di un significativo contenimento dei costi della missione, la piena incolumità del personale militare e dei servizi di *intelligence* coinvolto[3].

È per tali ovvie ragioni che il programma di sviluppo dei droni armati è cresciuto in modo inarrestabile nel corso degli anni e ha condotto a un impiego degli *UAVs* in contesti tra loro piuttosto eterogenei, caratterizzati da conflitti armati, internazionali e non, ma anche da situazioni di grave instabilità o di mancato controllo del territorio da parte del governo centrale (Afghanistan, Pakistan, Siria, Yemen, Somalia, Iraq). Ciò che accomuna le missioni di *targeted killing* eseguite da droni è l'individuazione di un bersaglio nei cui confronti l'uso della forza unilaterale è ritenuto (dal soggetto agente)

[1] Sul tema si rinvia a Q. Eijkman - M. Bakker, *Access to an Effective Remedy and Reparations for Civilian Victims of Armed Drone Strikes* in B. Custers (ed.), *The Future of Drone Use, Opportunities and Threats from Ethical and Legal Perspectives*, Leiden, 2016, 289 ss.; J. Andresen, *Due Process of War in the Age of Drones*, in *Yale Journal of International Law*, 41, 2016, 155 ss.; A. Buchanan - R.O. Keohane, *Toward a Drone Accountability Regime*, in *Ethics & International Affairs*, 1, 2015, 15 ss.; S. I. Vladeck, *Targeted Killing and Judicial Review*, in *The George Washington Law Review Arguendo*, 82, 2014, 11 ss.; G.-J. A. Knoops, *Drones at Trial: State and Individual (Criminal) Liabilities for Drones Attacks*, in *International Criminal Law Review*, 14, 2014, 42 ss.; T. M. MacDonnell, *Sow What You Reap? Using Predator and Reaper Drones to Carry Out Assassinations or Targeted Killings of Suspected Islamic Terrorists*, in *George Washington International Law Review*, 44, 2012, 243 ss. V. anche H. Duffy, *The 'War on Terror' and the Framework of International Law*, Cambridge, 2005.

[2] Il primo «*lethal strike*» messo a segno da un drone risale al 7 ottobre 2001 in Afghanistan. La cronaca della missione è riferita da C. Woods, *The Story of America's Very First Drone Strike*, in *The Atlantic*, 30 maggio 2015.

[3] Per un approfondimento si rinvia al Rapporto dell'Istituto di Ricerche Internazionali IRIAD dell'aprile 2017, dal titolo *Droni militari: proliferazione o controllo?*, spec. 8 ss.

legittimo, ancorché sia esercitato al di fuori di un tipico scenario di conflitto[4].
Questa "confusione" di fondo in ordine al contesto nell'ambito del quale le missioni dei droni vengono programmate ed eseguite, puntualmente evidenziata dalla dottrina[5], è accentuata dalla progressiva militarizzazione dell'azione terroristica di matrice fondamentalista, che porta a qualificare gli attentati come veri e propri atti di guerra. A partire dall'11 settembre 2001, ma già in occasione degli attacchi alle ambasciate statunitensi in Kenya e Tanzania, si è compreso, infatti, come la configurazione strutturale e le capacità operative dei terroristi siano più correttamente riconducibili a quelle di gruppi militari che a quelle di gruppi criminali – per così dire – ordinari, sotto diversi profili: dall'ideologia eversiva propugnata, di portata transnazionale, all'assetto organizzativo e alle sue ramificazioni, alle modalità di addestramento dei membri del gruppo, all'uso di tecnologie avanzate, ecc. Di conseguenza, l'impiego della forza letale in tali missioni viene a essere giustificato non in forza del rinvio a regole giuridiche chiare e predeterminate (ad es., quelle del diritto internazionale umanitario), bensì in base alla pericolosità intrinseca del soggetto destinatario e alla praticabilità concreta delle modalità di svolgimento dell'operazione. Resta, quindi, impregiudicata ogni valutazione circa lo *status* giuridico formale (terrorista, combattente, insorgente) che il bersaglio riveste o le condizioni effettive di ingaggio nell'ambito di un conflitto.
Non è, pertanto, sufficientemente chiara la cornice normativa in cui le missioni anzidette devono correttamente collocarsi e ciò ha portato a sollevare più di una perplessità sulla loro effettiva conformità agli standard previsti dal diritto internazionale[6]. Le

[4] Sul punto, è interessante mettere a confronto il documento (recentemente desecretato) recante le *Procedures for approving direct action against terrorist targets located outside the United States and areas of active hostilities*, messo a punto dal Dipartimento della Giustizia statunitense il 22 maggio 2013, sotto l'amministrazione del Presidente Obama, con il nuovo orientamento proposto dall'amministrazione Trump, che punta a estendere ulteriormente la sfera giuridica entro la quale i *lethal strikes* contro i terroristi sono ritenuti legittimi, in virtù del deciso allentamento dei (già piuttosto ampi) criteri di ammissibilità di simili operazioni al di fuori di contesti bellici formalmente dichiarati. In sostanza, in nome dell'autoattribuita legittimazione giuridica internazionale della *war on terror*, si sostiene la possibilità di derogare ai tradizionali principi di diritto internazionale umanitario… al di fuori di un conflitto armato. Per un approfondimento, si rinvia a L. Hartig, *Trump's New Drone Strike Policy: What's Any Different? Why It Matters*, in www.justsecurity.org, 22 settembre 2017 e L. Tayler, *How Obama's Drones Rulebook Enabled Trump*, ivi, 26 settembre 2017.

[5] A. Buchanan - R.O. Keohane, *op. cit.*, 15-16.

[6] In dottrina si segnalano opinioni fortemente discordanti tra coloro i quali si mostrano favorevoli all'utilizzo delle *killing machines* per questo genere di operazioni (considerato anzitutto il minore impatto – politico e mediatico – rispetto alle missioni che comportano l'invio di contingenti militari) e tendono perciò a giustificarle sul presupposto della piena applicabilità delle regole del diritto internazionale umanitario anche nella «guerra al terrorismo», nonostante le evidenti differenze rispetto ai conflitti armati tradizionali (J. J. Paust, *Self-Defense Targetings of non-State Actors and Permissibility of U.S. Use of Drones in Pakistan*, in *Journal of Transnational Law & Policy*, 19, 2010, 237 ss.) e chi, invece, contesta radicalmente l'ammissibilità di una simile ricostruzione, qualificando i *lethal strikes* dei droni come operazioni vietate perché implicanti l'uso illegittimo della forza armata oltre i limiti imposti dal diritto internazionale (M. E. O' Connell, *Remarks: The Resort to Drones Under International Law*, in *Denver Journal of International Law and Policy*, 39, 2011, 585 ss.).

critiche più ricorrenti, che provengono da inchieste condotte da ONG[7] e da organi di stampa internazionali[8], si concentrano essenzialmente sull'assenza di dati certi riguardanti il numero di attacchi compiuti e di vittime collaterali cagionate, mentre un'attenzione più marginale è riservata alla valutazione delle missioni in punto di legittimità ai sensi delle norme internazionali applicabili[9].

Sennonché, rispetto al tema oggetto del presente contributo, la corretta qualificazione giuridica dell'impiego di droni armati in attività di antiterrorismo e, in specie, per l'esecuzione di *lethal strikes*, presenta un rilievo preliminare. Ove, infatti, si ritenga che il contesto nel quale tali missioni sono promosse sia formalmente riconducibile a quello di un conflitto armato, per attestare la legittimità di un attacco, anche con riguardo alla condizione delle vittime, sarà necessario verificare esclusivamente il rispetto dei principi e delle norme di diritto internazionale umanitario nelle circostanze concrete di esecuzione. Al contrario, qualora si ritenga che, fuori dai casi in cui simili attacchi sono condotti all'interno di una guerra formale e dichiarata, il contesto in cui i *targeted killings* sono generalmente eseguiti non sia in alcun modo assimilabile a una situazione di conflitto armato, la valutazione della loro (discutibile) legittimità ai sensi del diritto internazionale dei diritti umani assume un'importanza decisiva anche per quanto attiene allo specifico profilo in esame.

L'accertamento dell'ammissibilità degli omicidi mirati di terroristi in rapporto alle legittime condizioni dell'uso della forza armata nel diritto internazionale (lo *ius ad bellum*) ha, quindi, natura preliminare rispetto all'accertamento ulteriore della loro conformità allo *ius in bello*. Ciò in quanto solo un esito positivo del primo scrutinio (che, in termini generali, pertiene alla valutazione della legittimità dell'uso della forza armata nella lotta al terrorismo) dà rilievo al secondo. Si tratta di ambiti di indagine formalmente autonomi, benché tra loro collegati sotto il profilo logico-consequenziale[10].

---

[7] Amnesty International ha pubblicato nel 2013 il rapporto *"Will i be next?" US drone strikes in Pakistan*, in www.amnestyusa.org. Nel 2014, Human Rights Watch ha pubblicato un proprio rapporto dal titolo *A Wedding That Became a Funeral US Drone Attack on Marriage Procession in Yemen*, in www.hrw.org. Anche la Open Society Foundations ha pubblicato due importanti rapporti, rispettivamente nel 2014 e nel 2015: *After the Dead are Counted: U.S. and Pakistani Responsibilities to Victims of Drone Strikes*, www.opensocietyfoundations.org e ivi *Death by Drone - Civilian Harm Caused by U.S. Targeted Killings in Yemen*. Molto attive in campagne di sensibilizzazione sui *drone strikes* sono anche l'organizzazione Reprieve, l'European Center for Constitutional and Human Rights e la Nuhanovic Foundation.

[8] Si veda il reportage di M. Bowden, *The Killing Machines*, in *The Atlantic*, September 2013, in www.theatlantic.com, e altresì tradotto in italiano sul settimanale *Internazionale*, 4-10 ottobre 2013, 38 ss.).

[9] Sul punto si vedano, ad es., i recenti rapporti dell'European Center for Constitutional and Human Rights, intitolato *Litigating Drone Strikes - Challenging the Global Network of Remote Killing* , del maggio 2017, e della Columbia Law School Human Rights Clinic & Sana'a Center for Strategic Studies, dal titolo *Out Of the Shadows*, del giugno 2017. Si veda anche il rapporto del Sottocomitato sui diritti umani del Parlamento europeo, dal titolo *Towards an EU Common Position on The Use of Armed Drones*, del 5 giugno 2017, che fa seguito alla risoluzione adottata, sempre dal PE, nel 2014: *European Parliament Resolution on the Use of Armed Drones*, 2014/2567(RSP).

[10] È appena il caso di ricordare, d'altro canto, che la «dicotomia» *ius ad bellum-ius in bello* (secondo l'accezione di N. Bobbio, *Dalla struttura alla funzione. Nuovi studi di teoria del diritto*, Milano, 1977, 145 ss., in proposito richiamata da S. Pietropaolo, *Jus ad bellum e jus in bello. La vicenda teorica di una "grande dicotomia" del diritto internazionale*, in *Quaderni fiorentini*, 38-I, 2009, 1169 ss., spec. 1170) viene in rilievo, in ambito giusinternazionalistico, solo a partire dal secondo dopoguerra, per effetto del ripudio generale dell'uso della forza armata come mezzo ammissibile per la risoluzione delle controversie internazionali.

2. La controversa legittimità dei "*drone strikes*" con finalità di antiterrorismo in base alle regole dello *ius ad bellum*

Lo *ius ad bellum*, com'è noto, regola le condizioni del ricorso legittimo all'uso della forza ai sensi del diritto internazionale vigente. Riferimento normativo di ordine generale è la Carta delle Nazioni Unite, che, all' art. 2, par. 4, sancisce l'illiceità della minaccia o dell'uso della forza armata «contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato» o «in qualunque altra maniera» che risulti incompatibile con i fini dell'Organizzazione, contemplando come uniche eccezioni l'esercizio del diritto naturale di autotutela armata in risposta a un attacco altrui (art. 51), ovvero l'autorizzazione all'uso della forza concessa dal Consiglio di sicurezza nei casi in cui si renda necessario «mantenere o ristabilire la pace e la sicurezza internazionale» (art. 42).
Affinché l'impiego di droni armati nell'ambito della «guerra al terrorismo» sia giustificabile in base alle richiamate eccezioni al divieto dell'uso della forza è necessario, quindi, che i *lethal strikes* formino parte integrante delle azioni belliche condotte all'interno di un conflitto armato (al punto che il terrorista obiettivo della missione sia sovrapponibile alla figura del combattente nemico disciplinata dal diritto internazionale umanitario), ovvero che la stessa *war on terror* integri di per sé una (nuova) ipotesi di uso legittimo della forza armata, rilevando come fattispecie autonoma idonea a giustificare, per le finalità perseguite, l'impiego di droni per l'esecuzione di missioni letali. In altri termini, l'impiego di droni «in tempo di pace» per colpire individui appartenenti a gruppi terroristici, sia pure in zone non soggette a un sufficiente controllo delle forze dello Stato territoriale o in situazioni di transizione politica derivanti dal «fallimento» dello Stato medesimo, può essere riconosciuto legittimo ai sensi del diritto internazionale solo ove si ritenga che la «guerra al terrorismo» configuri una modalità di uso della forza riconducibile a una delle due eccezioni al divieto generale sopra richiamate, ovvero un *tertium genus* suscettibile di ampliare lo spettro dei regimi eccezionali ammissibili. Verso quest'ultima ipotesi – come si vedrà – sembrano orientarsi le posizioni ufficiali della diplomazia statunitense, muovendo dal duplice presupposto della segnalata eccezionalità del fenomeno terroristico che gli Stati Uniti e i loro alleati sono chiamati a contrastare e dell'inadeguatezza del modello di *law enforcement* a essere applicato in contesti di fragilità istituzionale e di limitato (se non del tutto assente) controllo del territorio da parte delle forze militari o di polizia dello Stato in cui le missioni sono eseguite[11]. Una "zona grigia" (o *più zone grigie*, tenuto conto della varietà di contesti geopolitici in cui la prassi dei *lethal strikes* è riscontrabile), quindi, assimilabile a una situazione di conflitto armato a bassa intensità o, in senso speculare, di obiettiva impossibilità di gestione dell'ordine pubblico, che autorizzerebbe al ricorso a strumenti di *law enforcement* più "robusti" di quelli utilizzabili in condizioni ordinarie.
Tale ricostruzione, non priva di estimatori in dottrina[12], si basa sull'assunto che le modalità operative caratterizzanti l'esecuzione dei *targeted killings* non incidono in quanto

[11] Cfr. Duffy, *op. cit.,* in particolare 332 ss.; K. Roth, *The Law of War in the War on Terror*, in *Foreign Affairs*, 2004, in www.foreignaffairs.com.

[12] A. Buchanan - R. O. Keohane, *op. cit.*, 18 ss.

tali sull'ampliamento della gamma delle situazioni in cui l'impiego della forza armata è ritenuto lecito dal soggetto agente. Si ritiene, in altri termini, che la tecnologia militare innovativa utilizzata per compiere le missioni, ossia i droni armati, sia un elemento *neutrale* e non contribuisca, quindi, in alcun modo a qualificare le missioni stesse, in rapporto alle regole dello *ius ad bellum*, in modo differente da quelle eseguite mediante mezzi "tradizionali" (velivoli armati con pilota a bordo, truppe di terra, ecc.).

Tuttavia, ove si consideri il fenomeno del crescente ricorso alla tecnologia in argomento non quale risposta all'esigenza di contrastare in modo adeguato l'innalzamento del livello della minaccia terroristica, bensì – muovendo da una prospettiva diametralmente opposta – quale elemento in sé idoneo a favorire l'allargamento dello spettro di opportunità di impiego della forza armata in contesti e situazioni ritenuti fino a quel momento inaccessibili o non convenienti per lo Stato agente, non è irragionevole sostenere che sia proprio la disponibilità di tale tecnologia a pilotaggio remoto (a tacere degli ulteriori sviluppi dei sistemi di pilotaggio automatico) ad aver reso possibile – *rectius*: più vantaggioso, perché privo di rischi e poco costoso, oltre che non inviso all'opinione pubblica interna – l'uso della forza armata in simili contesti, determinando, per l'effetto, la creazione delle anzidette "zone grigie". In buona sostanza, la stessa missione (l'omicidio mirato di un membro di un gruppo terrorista), che fino all'avvento della tecnologia in argomento era solo occasionalmente, se non addirittura eccezionalmente, programmata ed eseguita (per via degli elevati costi economici, dei rischi per i militari impiegati e dell'impatto negativo sull'opinione pubblica e sui rapporti internazionali), grazie all'impiego del sistema a pilotaggio remoto diviene ordinaria, per il solo fatto di essere realizzabile in condizioni di sicurezza, segretezza e a costi contenuti. Essa concorre, così, a formare una prassi inedita che esige di essere regolata. Sarebbe logicamente errato ritenere che sia la gravità della minaccia terroristica a "imporre" l'esecuzione degli omicidi mirati. È, invece, la possibilità di eseguire questi ultimi a condizioni più agevoli che introduce un elemento di novità nel contesto preesistente, interrogando il giurista sull'adeguatezza delle norme vigenti a disciplinare la prassi di cui si discute.

La suggerita inversione di prospettiva trae spunto dagli studi più accurati elaborati dalla dottrina sulle conseguenze etico-sociali dell'impiego dei droni sulle popolazioni residenti nei territori interessati dalle missioni[13]. Ora, applicando il medesimo ragionamento – in base al quale, come detto, lo strumento utilizzato per i *targeted killings* non è affatto neutrale, ma contribuisce esso stesso a "creare l'occasione" per agire militarmente contro i terroristi – allo specifico problema delle vittime innocenti provocate dagli *strikes*, appaiono assai poco condivisibili le giustificazioni addotte dal governo statunitense, nella persona dell'allora Presidente Barack Obama, a sostegno dell'uso dei droni armati in luogo di altri mezzi meno efficaci per colpire i terroristi, in particolare laddove il *Commander-in-chief* affermava che *«[c]onventional airpower or missiles are far less precise than drones, and are likely to cause more civilian casualties and more local outrage»*[14]. Tale asserzione, in sé astrattamente condivisibile, acquista un significato diverso se letta alla

[13] G. Chamayou, *Teoria del drone. Principi filosofici del diritto di uccidere* (trad. it. di M. Tarì), Roma, 2014.

[14] Sono le parole pronunciate dall'allora Presidente degli Stati Uniti Barack Obama nel discorso tenuto alla National Defense University il 23 maggio 2013.

luce delle precedenti considerazioni e di alcune affermazioni dello stesso Presidente Obama, utili per comprendere come l'opzione dell'attacco militare nella lotta al terrorismo non sia particolarmente conveniente, se eseguita con modalità tradizionali: «*it's also not possible for America to simply deploy a team of Special Forces to capture every terrorist. Even when such an approach may be possible, there are places where it would pose profound risks to our troops and local civilians – where a terrorist compound cannot be breached without triggering a firefight with surrounding tribal communities, for example, that pose no threat to us; times when putting U.S. boots on the ground may trigger a major international crisis*». L'uso dei droni, pertanto, estende in modo consistente le capacità di intervento militare nella *war on terror*, generando così non già meno vittime collaterali rispetto a quelle ipoteticamente causate da un conflitto armato tradizionale, ma semplicemente nuove vittime.

Anche le Nazioni Unite si sono ovviamente occupate del tema attraverso i propri organi di promozione della tutela dei diritti umani. Già il Relatore Speciale del Consiglio dei Diritti Umani Philip Alston, nel suo *Report on extrajudicial, summary or arbitrary executions*[15], aveva evidenziato come, al di fuori di un conflitto armato formalmente accertato, la possibilità di un «*intentional, premeditated and deliberate use of lethal force*» realizzato mediante l'impiego di droni non possa ritenersi ammissibile «*under international law*». I successivi *Reports on extrajudicial, summary or arbitrary executions*[16] e *on Promotion and protection of human rights and fundamental freedoms while countering terrorism*[17] rispettivamente redatti dai Relatori Speciali Christof Heyns e Ben Emmerson, hanno confermato che la prassi in argomento pone alcune rilevanti questioni di «*legal controversy*», in particolare per quanto attiene alle condizioni di liceità dell'uso della forza «*outside situations of armed conflict*»[18], pur senza approfondire i segnalati profili problematici.

3. La posizione del governo statunitense

Come anticipato, le posizioni ufficiali del governo statunitense – che attualmente, se si eccettua il limitato ricorso a tale tecnologia da parte di Israele e del Regno Unito, sono l'unico Paese che utilizza i droni con finalità di antiterrorismo – e della dottrina favorevole alla definizione di una cornice normativa *ad hoc* per la collocazione dei *lethal strikes* sembrano essere orientate a giustificare il mezzo in ragione dell'eccezionalità della situazione in cui è impiegato, nonché della moralità dello scopo cui tende.

Già sotto la Presidenza di George W. Bush e sotto le due amministrazioni successive, il governo statunitense ha strenuamente sostenuto la legittimità dei *drone strikes* contro i terroristi, teorizzando – con argomentazioni invero non particolarmente accurate –

[15] U.N. doc. A/HRC/14/24/Add.62 del 28 maggio 2010.

[16] U.N. doc. A/68/382 del 13 settembre 2013.

[17] U.N. doc. A/68/389 del 18 settembre 2013.

[18] Tra i documenti adottati dal Consiglio dei diritti umani delle NU, si vedano anche la risoluzione *Ensuring use of remotely piloted aircraft or armed drones in counterterrorism and military operations in accordance with international law, including international human rights and humanitarian law* (U.N. doc. A/HRC/RES/25/22 del 15 aprile 2014) il *Summary of the interactive panel discussion of experts on the use of remotely piloted aircraft or armed drones in compliance with international law* (U.N. doc. A/HRC/28/38 del 15 dicembre 2014), panel promosso dalla citata risoluzione.

l'esistenza, a partire dall'11 settembre 2001, di un conflitto armato non internazionale combattuto dagli Stati Uniti contro organizzazioni terroristiche nemiche (Al-Qaeda e gruppi ad essa affiliati). Il coinvolgimento degli Stati Uniti in tale conflitto è inquadrabile a titolo di legittima difesa contro gli attacchi già compiuti e quelli programmati o anche solo meramente ideati dai terroristi contro i propri cittadini o propri interessi. Più precisamente, secondo Harold Koh[19], *legal advisor* della Casa Bianca sotto la Presidenza di Barack Obama, l'uso dei droni in operazioni antiterrorismo è legittimato in primo luogo dall'*Authorization for the use of military force against terrorists* (*AUMF*), rilasciata dal Congresso al Presidente degli Stati Uniti il 14 settembre del 2001 per consentire l'impiego di ogni mezzo necessario a perseguire i responsabili degli attentati dell'11 settembre e ogni individuo o gruppo fiancheggiatore, ed è da ritenersi, altresì, conforme al diritto internazionale, poiché, dopo gli attacchi sul suolo americano e nei confronti dei contingenti militari impegnati all'estero, gli Stati Uniti sarebbero stati – loro malgrado – attirati in un conflitto armato contro le milizie di *al-Qaeda* e sarebbero, per ciò stesso, legittimati all'uso della forza ai fini di autodifesa. Di qui la legittimazione degli attacchi eseguiti da droni sul territorio di qualsiasi Stato – sia esso impegnato o meno in un conflitto armato – in cui i terroristi-nemici possano ritenere di aver trovato il proprio *safe haven*.

La riferita ricostruzione riflette pienamente la tradizionale «autoreferenzialità» della posizione statunitense: oltre ad anteporre gli obblighi interni derivanti dall'applicazione dell'AUMF all'osservanza dei principi di diritto internazionale, in linea con un consolidato orientamento interpretativo che fa leva sul primato del diritto costituzionale, il *legal advisor* propone un'interpretazione «estensiva» della nozione di legittima difesa (come già accaduto, d'altronde, in occasione del secondo conflitto iracheno e dell'applicazione della teoria della legittima difesa preventiva) per giustificare l'ammissibilità, in punto di diritto, della conduzione di un conflitto armato «diffuso» (perché potenzialmente esportabile in qualsiasi luogo geografico) e «permanente» (perché destinato a concludersi solo quando la minaccia terroristica sarà definitivamente sventata) contro i terroristi.

In tal senso, la prassi dei *lethal strikes* è tra le manifestazioni più concrete di quella tendenza in atto nel diritto internazionale generale che pare orientata a riconoscere la

[19] Si fa riferimento al discorso tenuto alla Oxford Union il 7 maggio 2013, intitolato *How to End the Forever War?*.

non-illegittimità dell'uso unilaterale della forza per la protezione di interessi statali[20], in situazioni che, a fronte del silenzio, della paralisi o dell'implicito avallo del Consiglio di sicurezza delle NU, pure esulano dall'ambito di applicazione dell'istituto della legittima difesa nella sua configurazione classica – e tuttora vigente – di risposta necessaria, immediata e proporzionata a un attacco armato. Diversi fattori, tuttavia, inducono a essere piuttosto prudenti sul punto, dal momento che la stessa idea di una «*permanent worldwide war*» contro il terrorismo sembra poco accettabile, anche sul piano concettuale. In particolare, è difficile ammettere la possibilità di condurre un conflitto o eseguire singole missioni implicanti l'uso della forza letale sul territorio di uno Stato straniero senza il consenso – almeno implicito – di quest'ultimo. Né la semplice assenza di volontà o la constatazione dell'incapacità operativa dello Stato territoriale ai fini della persecuzione dei terroristi appaiono da sole condizioni idonee a legittimare sul piano giuridico un intervento militare in via sussidiaria per scopi di autodifesa[21].

[20] Alcuni indizi tratti dalla prassi più recente sembrano confermare l'esistenza di un simile processo evolutivo, certamente non apprezzabile come fenomeno compiuto, quanto piuttosto come tendenza in sviluppo (e quindi suscettibile di futuro consolidamento o, al contrario, di regressione), basata sull'accettazione diffusa, benché non sempre manifesta, di inedite interpretazioni delle regole internazionali legittimanti l'uso della forza. Si fa riferimento proprio al problematico ampliamento dei limiti operativi del principio di legittima difesa nei confronti di attori non statali responsabili di gravi azioni terroristiche (ritenute idonee a integrare la fattispecie dell'attacco armato) e del conseguente riconoscimento di una responsabilità internazionale "indiretta" degli *host States*. L'irruzione di tali elementi nella prassi internazionale già all'indomani degli attentati dell'11 settembre 2001 ha portato la dottrina a interrogarsi sull'ammissibilità della relativa qualificazione alla stregua di "consuetudini istantanee", ossia di norme generali formatesi per effetto del contestuale accertamento di un'*opinio iuris* sostanzialmente uniforme riguardo al loro contenuto, ma prive del conforto di una sufficiente pratica applicativa. Nell'impossibilità di dar conto in questa sede anche solo dei contenuti salienti del dibattito coevo (rispetto al quale sia consentito rinviare a N. Colacino, *La comunità internazionale, il suo nemico perfetto e il «diritto naturale» di combatterlo: rilievi critici sul ricorso alla legittima difesa contro il terrorismo*, in *Ordine internazionale e diritti umani*, 2016, 670 ss. e alla bibliografia ivi citata; da ultimo, v. anche l'ampia trattazione di P. Picone, *Obblighi "*erga omnes*" e uso della forza*, Napoli, 2017, che reca una critica puntuale dei tentativi di ricondurre entro la cornice normativa della Carta delle Nazioni Unite la controversa prassi degli interventi armati degli ultimi due decenni), va detto che proprio la diffusa accettazione del rilievo dei predetti elementi di novità nella disciplina dello *ius ad bellum* sembra aver costituito – più o meno deliberatamente – la base giuridica sulla quale vengono a innestarsi gli ulteriori mutamenti in atto nel settore. Si tratta, in particolare, della tendenza a considerare lecita l'autotutela armata nei confronti di gruppi terroristici ben oltre i tradizionali limiti di proporzionalità, necessità e immediatezza, la quale presuppone l'adesione a una concezione di legittima difesa "permanente" e "parcellizzata", assai poco riconducibile al modello codificato dall'art. 51. A sostegno di tale concezione si pone, inoltre, l'elaborazione di criteri idonei a giustificare l'intervento armato (in autotutela, contro gruppi terroristici) condotto sul territorio di altri Stati qualora essi si dichiarino, anche per *facta concludentia*, contrari a o incapaci di (*unwilling or unable*) approntare una reazione adeguata al livello di reazione alla minaccia preteso dallo Stato interveniente. Orbene, l'impossibilità di ricondurre formalmente i predetti criteri – e gli interventi armati condotti in base alla relativa applicazione – al paradigma onusiano della legittima difesa è evidente: basti solo pensare all'esito paradossale di un simile intervento ove eseguito sul territorio di uno Stato non consenziente, ancorché non direttamente rivolto nei suoi confronti. Detto Stato avrebbe titolo a reagire a sua volta in... legittima difesa contro l'invasore. Sennonché, il conflitto siriano, nella sua fase più acuta, ha assunto caratteristiche del tutto sovrapponibili all'ipotesi descritta e ciò vale a denunciare nei fatti la palese inadeguatezza della riferita costruzione teorica a soddisfare l'esigenza di un uso regolato della forza armata per finalità di tutela di interessi pubblici (come il contrasto al terrorismo internazionale), ove esso sia ricondotto a uno schema improprio (perché essenzialmente idoneo a giustificare il ricorso alla forza armata per la protezione di interessi statali, anche se collettivi). Si interroga, da ultimo, sull'incerta combinazione degli elementi che caratterizzano il conflitto siriano G. Guarino, *Il conflitto in Siria tra guerra rivoluzione e terrorismo. Alla ricerca di una logica (…normativa?)*, Napoli, 2017, in particolare 161 ss.

[21] Cfr. T. Reinold, *State Weakness, Irregular Warfare, and the Right to Self- Defense Post-9/11*, in *The American Journal of International Law*, 105, 2011, 244 ss.

4. L'assenza di rimedi giurisdizionali a tutela delle vittime secondo la prassi rilevante e l'insufficienza delle riparazioni *ex gratia*

Dalla pur sommaria analisi fin qui condotta riguardo ai profili teorici dell'inquadramento normativo dei *drone strikes* emerge come l'atteggiamento degli Stati che si avvalgono di tale tecnologia sia poco incline all'accettazione di un sistema di regole condiviso e conforme agli standard internazionali pertinenti. Per contro, la totale assenza di trasparenza riguardo alle modalità di conduzione delle missioni impedisce qualsiasi valutazione in ordine alla corrispondenza ai predetti standard delle norme unilateralmente adottate, anche per quanto attiene allo specifico profilo alla tutela delle vittime e ai rimedi accessibili per ottenere un'equa riparazione.

La prassi, come anticipato, annovera casi tra loro piuttosto eterogenei. Droni armati sono stati utilizzati, infatti, nell'ambito dei conflitti combattuti in Afghanistan e in Iraq, ma si tratta di un numero di casi limitato se messo in relazione con quello in cui i *targeted killings* sono stati eseguiti sul territorio di Stati non formalmente coinvolti in conflitti armati.

L'opinione pubblica internazionale solleva regolarmente il problema della segnalata assenza di trasparenza delle regole di ingaggio, evidenziando come le vittime innocenti dei *drone strikes* e i loro congiunti siano ulteriormente penalizzati per via dell'impossibilità di accedere a rimedi giudiziari effettivi per ottenere almeno forme di ristoro economico. La quasi totalità delle vittime non ha, infatti, finora ricevuto alcun riscontro alla propria domanda di giustizia.

Ciò è conseguenza del fatto che nessuno Stato coinvolto ha mai acconsentito a chiarire formalmente la propria posizione riguardo al fondamento giuridico sul quale le missioni riposano. Questo vale con riferimento sia agli Stati autori dei *drone strikes*, sia a quelli che prestano il loro consenso alla relativa esecuzione sul proprio territorio, sia, infine, a quelli che mettono a disposizione le loro basi per il decollo degli *UAVs*. L'Italia e la Germania – presso le rispettive basi di Sigonella e Ramstein[22] – sono coinvolte proprio a tale titolo, ma, mentre nel caso tedesco è stato accertato il coinvolgimento formale dell'infrastruttura di Ramstein nell'esecuzione delle missioni, l'accordo che autorizza l'impiego della base di Sigonella per i supposti medesimi fini non è stato finora reso pubblico.

Il 27 maggio 2016 il Tribunale amministrativo di Colonia ha rigettato un ricorso presentato da tre cittadini yemeniti (Faisal bin Ali Jaber e a.), i cui congiunti erano stati uccisi durante una festa matrimoniale il 29 agosto 2012, a seguito del bombardamento

[22] Riferisce il Rapporto *Droni militari: proliferazione o controllo?* (cfr. n. 2), 43 che «[l]a stazione di Sigonella dovrebbe assicurare la metà delle trasmissioni del sistema dei velivoli senza pilota e operare in appoggio al sito di Ramstein in Germania, già interconnesso con la base di Creech in Nevada, il principale centro mondiale di controllo dei droni. I droni controllati dal nuovo centro saranno utilizzati per le missioni pianificate dai comandi strategici EUCOM, AFRICOM e CENTCOM, basati a Sigonella, in modo da fornire in tempo reale le informazioni aggiornate ai reparti combattenti. La stazione di Ramstein, completata nel 2013, consente di trasmettere via satellite i comandi al drone e di riceverne le informazioni con tempestività. In altre parole, è a Ramstein che si crea il collegamento tra il pilota e il drone. L'UAS Satcom Relay di Sigonella opererà come una stazione gemella di Ramstein, assicurando il backup delle operazioni di intelligence e di telecomunicazione».

eseguito da un drone, pur non essendo in corso alcun conflitto armato nella zona e pur non essendo le vittime mai state accusate di attività di terrorismo o di legami con gruppi terroristici. L'azione promossa intendeva far valere la corresponsabilità del governo tedesco proprio rispetto alla sua partecipazione al programma di *lethal strikes* eseguito in Yemen tramite i droni in partenza dalla base di Ramstein[23]. Secondo i ricorrenti, la Germania, nel concedere la base per l'esecuzione di attività illecite, avrebbe violato il dovere di garantire, anche al di fuori del proprio territorio, il diritto fondamentale alla vita delle persone, tutelato dall'art. 2 della *Grundgesetz*. Il Tribunale ha ritenuto ammissibile il caso (e il ruolo svolto dalla base di Ramstein nel programma di omicidi mirati lanciato dagli Stati Uniti), ma ha escluso che sul governo tedesco gravasse l'obbligo di impedire l'utilizzo della base per le missioni dei droni. I ricorrenti hanno, quindi, promosso appello innanzi al Tribunale amministrativo superiore di Monaco di Vestfalia, a tutt'oggi pendente.

In una vicenda analoga, il coinvolgimento dei servizi segreti britannici e pakistani nella programmazione ed esecuzione di un *lethal strike* ha portato il ricorrente, un cittadino pakistano (*Noor Khan*, il cui padre era stato ucciso da un drone insieme ad altre quaranta persone durante una *jirga*) a promuovere ricorso sia innanzi alle Corti britanniche, sia innanzi a quelle pakistane. Nel primo caso, la Corte d'Appello di Londra si è dichiarata priva di giurisdizione, sul presupposto dell'insindacabilità di atti compiuti dal governo di uno Stato straniero, sia pure con il supporto di agenti britannici[24]. La Corte ha ritenuto, infatti, che l'accertamento della responsabilità di questi ultimi avrebbe inevitabilmente sotteso un analogo accertamento delle responsabilità gravanti sul governo statunitense[25]. Queste avrebbero potuto venire in rilievo innanzi alla Corte solo in circostanze eccezionali, che nella fattispecie non sono state, invece, ritenute presenti[26]. Solleva qualche perplessità la scelta della Corte di sottrarsi al normale esercizio dell'accertamento in via incidentale di un'ipotesi di responsabilità che, seppur in misura diversa, gravava sugli agenti di entrambi i Paesi. Un simile scrutinio non sembrava, infatti, esserle precluso, essendo strettamente funzionale alla valutazione della legittimità dell'operato degli agenti nazionali.

Esito diverso ha avuto il giudizio innanzi ai Tribunali pachistani. Con una sentenza emessa nel maggio 2013, la High Court di Peshawar ha dichiarato gli Stati Uniti colpevoli per crimini di guerra in relazione all'uso di droni armati nel nord-ovest del Paese, ordinando al governo pachistano di adottare misure appropriate per impedire l'esecuzione di nuovi attacchi, tra cui il deferimento della questione al Consiglio di sicurezza

---

[23] Il testo della sentenza sul caso n. 35625/14 è reperibile online.

[24] Il testo della sentenza è reperibile online.

[25] *Ibid.*, par. 37, ove si legge: *«[i]n my view, a finding by our court that the notional UK operator of a drone bomb which caused a death was guilty of murder would inevitably be understood (and rightly understood) by the US as a condemnation of the US. In reality, it would be understood as a finding that (i) the US official who operated the drone was guilty of murder and (ii) the US policy of using drone bombs in Pakistan and other countries was unlawful. The fact that our courts have no jurisdiction to make findings on either of these issues is beside the point. What matters is that the findings would be understood by the US authorities as critical of them. Although the findings would have no legal effect, they would be seen as a serious condemnation of the US by a court of this country»*.

[26] Così il dispositivo della sentenza: *«[t]here is no escape from the conclusion that, however the claims are presented, they involve serious criticisms of the acts of a foreign state. It is only in certain established circumstances that our courts will exceptionally sit in judgment of such acts There are no such exceptional circumstances here»*.

delle NU e, in casi estremi, l'abbattimento dei droni. Infine, la Corte ha stabilito l'obbligo a carico del governo statunitense di compensare le famiglie delle vittime, ordinando al governo pachistano di sollecitare un rapido avvio delle procedure di riparazione[27].
I casi qui riportati sono sintomatici della difficoltà di ottenere, in sede giurisdizionale, un accertamento puntuale delle responsabilità derivanti dall'esecuzione dei *drone strikes*. Se si eccettua, infatti, la sentenza della High Court di Peshawar (peraltro eccessivamente sbrigativa in alcuni passaggi cruciali delle relative motivazioni), gli organi giudiziari interpellati hanno escluso forme di responsabilità concorrente a carico degli Stati che, a vario titolo, contribuiscono alla progettazione o all'esecuzione di omicidi mirati. A tale atteggiamento di prudenza fa riscontro il costante rifiuto del governo statunitense, con pochissime eccezioni[28], di affermare pubblicamente la propria responsabilità per i *targeted killings*, inclusi quelli che hanno provocato vittime innocenti.
Nel caso Ali Jaber, le autorità yemenite hanno offerto ai parenti delle vittime un risarcimento pari a centomila dollari, come riparazione *ex gratia* corrisposta, in via non ufficiale, direttamente dal governo degli Stati Uniti. Ciò a condizione che i destinatari rinunciassero a ogni pretesa sul piano legale, inclusa la richiesta di scuse formali da parte dei governi coinvolti. È evidente che si tratta di una forma di riparazione non sufficiente e incompatibile con la finalità generale cui le stesse richieste di tutela giurisdizionale tendono, quella cioè di far luce sui criteri di *targeting* applicati dai servizi segreti e di pervenire, in ultima analisi, a una definitiva *disclosure* delle regole di ingaggio per verificarne la conformità agli standard internazionali di tutela dei diritti umani. D'altro canto, l'attribuzione e l'eventuale accettazione di un ristoro *ex gratia* non esime lo Stato sul cui territorio vengono eseguiti gli *strikes* dal duplice obbligo di pretendere l'osservanza del divieto di uccisioni arbitrarie da parte di altri Stati e di garantire alla propria popolazione un'incolumità effettiva rispetto a tali azioni.

5. Considerazioni di sintesi

Sebbene il dibattito avviato, non solo in ambito dottrinario, ma anche in seno all'opinione pubblica internazionale, sulla legittimità dei *drone strikes* sia molto aperto, non sembra che il tema delle riparazioni da accordare alle vittime rappresenti una priorità nell'ambito delle diplomazie nazionali e nelle sedi istituzionali internazionali. È significativo che, in occasione di un panel tenutosi nel 2014 presso il Consiglio dei diritti umani delle Nazioni Unite, solo due dei ventitré Stati partecipanti hanno espresso la loro preoccupazione riguardo al problema dell'impossibilità di accedere a rimedi giuri-

[27] Il testo della sentenza è reperibile online.

[28] Solo in occasione dei raid compiuti in Pakistan, precisamente nel nord Waziristan, il 17 marzo 2011 e a seguito delle pressioni del governo pachistano, che di propria iniziativa ha deciso di offrire una riparazione economica ai familiari dei civili uccisi o feriti nel corso dell'operazione (pari a circa tremila dollari a famiglia per ogni congiunto ucciso e a mille dollari per ogni ferito), il Rappresentante speciale per l'Afghanistan e il Pakistan del governo degli Stati Uniti, l'Ambasciatore Marc Grossman, ha espresso il proprio cordoglio e le proprie scuse per le vittime innocenti causate dai *drone strikes* durante una conferenza stampa a Bruxelles.

sdizionali effettivi da parte delle vittime dei bombardamenti e dei loro familiari[29].
A ben vedere, tuttavia, proprio la questione dell'accesso alla giustizia assume un rilievo fondamentale per considerare nella giusta prospettiva i problemi posti dall'utilizzo dei droni nella lotta al terrorismo. L'avvio di procedimenti giudiziari volti alla tutela dei diritti fondamentali delle vittime dei *drone strikes* potrebbe, infatti, costituire un elemento determinante per sollecitare una maggiore trasparenza da parte dei governi dei Paesi coinvolti e giungere all'elaborazione di un regime di regole condiviso che riconduca tali missioni in un ambito di piena legalità.
L'incerta evoluzione della prassi e l'assenza di una chiara *opinio iuris* sulle condizioni e i limiti di impiego di tale tecnologia militare – in ipotesi, presto affiancata o finanche sostituita da sistemi di pilotaggio automatico, rispetto ai quali il problema dell'accertamento della responsabilità per atti internazionalmente illeciti si pone in termini diversi e certamente più complessi – accresce l'esigenza di elaborare in tempi brevi una disciplina *ad hoc*. Fino ad allora, sembra opportuno, tuttavia, continuare a riferirsi alle categorie più solide del diritto internazionale vigente, mantenendo una chiara distinzione tra l'impiego dei droni nell'ambito di conflitti armati e in situazioni di pace. In quest'ultimo scenario, a prescindere dal livello di instabilità politica e dalla maggiore o minore propensione del governo locale a sostenere a *war on terror*, il ricorso alla forza letale dovrebbe essere ammesso solo come *extrema ratio* e a condizioni determinate e ogni perdita umana dovrebbe essere adeguatamente risarcita.

[29] Il contenuto della discussione (UN Human Rights Council, Panel discussion on *Ensuring use of remotely piloted aircraft or armed drones in counterterrorism and military operations in accordance with international law, including international human rights and humanitarian law*) è disponibile online.

Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani*

Letizia Seminara

Abstract

La sorveglianza segreta, oggi influenzata dalle nuove tecnologie, ha invertito nei tempi più recenti i termini dell'attività di sorveglianza tradizionale, la quale è ormai caratterizzata dalla domanda, agli individui, di trasparenza e, allo stesso tempo, dalla segretezza dei sorveglianti. Il diritto europeo dei diritti dell'uomo è basato sull'idea secondo cui le misure di sorveglianza segreta sono tipiche dello stato di polizia e che, possono pertanto essere ammesse soltanto se rigorosamente necessarie e associate alle dovute garanzie per il sorvegliato. Il presente lavoro mira a definire quali sono tali condizioni e garanzie nel diritto europeo. L'articolo esamina le relative disposizioni della Convenzione europea dei diritti dell'uomo, nonché la giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di giustizia dell'Unione europea in materia.

Secret surveillance as influenced by new technologies has currently inverted the terms of traditional surveillance activities, which are characterised now by a claim of transparency for individuals, on the one hand, and by the secrecy of surveillants, on the other hand. The European law of human rights is based on the idea that secret surveillance is typical of the police state; therefore, it can be admitted only if strictly necessary according to a number of conditions and, if admitted, it must be applied in association with due guarantees for the surveilled. The present work aims at defining those conditions and guarantees as set by the European law. It examines the concerned provisions of the European Convention of Human Rights, as well as the jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union in this field.

Sommario

1. Introduzione. - 2. La base legislativa della sorveglianza segreta e le nuove tecnologie. - 3. Lo scopo della sorveglianza segreta e le nuove tecnologie. - 4. La necessità e la proporzionalità delle misure di sorveglianza segreta e le nuove tecnologie. - 5. Conclusioni.

Keywords: Sorveglianza, Nuove tecnologie, Privacy, Sicurezza nazionale, Data retention

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio anonimo, in quanto riproduce la relazione presentata dall'A. al convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno" (Messina, 26-27 maggio 2017).

1. Introduzione

In una delle prime sentenze della Corte europea dei diritti dell'uomo in materia di sorveglianza segreta –la celebre sentenza *Malone* del 1984- il giudice Louis-Edmond Pettiti affermava in una sua opinione separata, con riguardo alle nuove tecnologie, alla Convenzione europea dei diritti umani e alla vita privata delle persone, che la Convenzione, ai nostri tempi, pone la necessità di preservare l'identità dell'uomo, di rifiutare la totale trasparenza della società, di mantenere la riservatezza della sua personalità.[1] Tale affermazione si inseriva nel contesto di un sistema di tutela dei diritti umani che, da una parte, era stato fondato con l'intento di limitare l'esercizio del potere pubblico a tutela dell'individuo e che, dall'altra, era stato instaurato in un momento in cui, come lo ricordava il giudice Pettiti, le tecniche di ingerenza nella vita privata erano ancora arcaiche. Poi, già all'epoca della sentenza, lo stesso giudice avvertiva quali erano i rischi di una società permanentemente e segretamente sorvegliata, situazione che egli percepiva come un "pericolo" e che descriveva nel modo seguente:

«Il pericolo che minaccia le società democratiche degli anni 1980-1990 risulta dalla tentazione che hanno i poteri pubblici di ottenere la "trasparenza" della situazione dei cittadini. Per rispondere ai bisogni di pianificazione, della politica sociale e fiscale, lo Stato deve moltiplicare le sue ingerenze. Le tecniche amministrative lo conducono a moltiplicare le schede di identificazione, poi a trattarle attraverso l'informatica. Già in più Stati membri del Consiglio d'Europa, ogni cittadino è schedato 200 a 400 volte. In una seconda fase, l'autorità pubblica cerca, attraverso le sue statistiche e le sue motivazioni decisionali, di definire il "profilo" di ogni cittadino. Le indagini si moltiplicano; le intercettazioni telefoniche sono un mezzo privilegiato di questa indagine permanente».[2]

Come è spesso ricordato, storicamente i diritti umani si sono posti, almeno nel contesto europeo, come limite al potere pubblico e, più in generale, come limite alle azioni di chi esercita detto potere. Se, dunque, tale limitazione esigeva, ed esige tuttora, che l'espletamento dei poteri si fermi dinanzi alla sfera privata degli individui, allo stesso tempo esigeva, ed esige, trasparenza nell'esercizio del potere pubblico. Sfera privata dunque per gli individui e, allo stesso tempo, trasparenza per gli organi pubblici.
La questione dell'uso di nuove tecnologie nella sorveglianza segreta degli individui, presenta delle caratteristiche che vanno ad invertire i sopramenzionati rapporti tradizionali perché le tecnologie permettono oggi la completa segretezza dell'esercizio di poteri sull'individuo, con un corrispettivo controllo quasi totale sulla vita privata dello stesso. Ciò risulta in un sistema perfettamente contrario a quello sopradescritto in cui i termini si sono invertiti: la sfera di riservatezza degli individui viene annientata e, invece, aumenta quella dei sorveglianti con una notevole riduzione della trasparenza di chi esercita il potere, che agisce, nella segretezza. Nell'odierno sistema, dunque, si doman-

[1] Cfr. *Opinion concordante de M. le juge Pettiti*, nel caso *Malone c. Regno Unito*, 2 agosto 1984, n. 8691/79. Si veda, in seguito, L. Pettiti, *A l'écoute: pour une législation européenne des interceptions des correspondances*, in *Liber Amicorum Dean Spielmann*, Oisterwijk, 2015, 485-494.

[2] *Opinion concordante de M. le juge Pettiti*, cit. La traduzione è nostra.

da trasparenza all'individuo e si conferisce segretezza al sorvegliante. L'esatto opposto. Con la conseguenza che, come affermava il giudice Petitti nel contesto della citata causa, gli individui sono sempre più vulnerabili come risultato della nuova tecnologia.[3] Anzi, l'individuo si trova, oggi, in una situazione di assoluta vulnerabilità nei confronti del sorvegliante, segreto e talvolta immune.

Evidentemente, questa situazione non può tradursi in una mancanza di diritti per il sorvegliato. Celebre è la formula utilizzata dalla Corte europea dei diritti dell'uomo nella sentenza *Klass c. Germania*, secondo cui «la Cour ne saurait admettre que l'assurance de bénéficier d'un droit garanti par la Convention puisse être ainsi supprimée du simple fait de maintenir l'intéressé dans l'ignorance de sa violation».[4]

Dinanzi a questo pericolo, si è creato in sede europea un sistema di tutela dell'individuo che gira intorno a due idee. La sorveglianza segreta è un'attività propria dello stato di polizia e viene perciò ammessa *soltanto se rigorosamente necessaria*. Laddove fosse poi ammessa *deve offrire determinate garanzie*. Garanzie contro l'arbitrario e contro ogni abuso. Occorre inoltre ribadire che il soddisfacimento delle garanzie richieste è anche una condizione per la legittimità delle misure di sorveglianza segreta, nel senso che, se tali garanzie non sono assicurate, non potrà esservi sorveglianza segreta. Il sistema europeo di tutela dei diritti fondamentali è centrato, nello specifico, sulle suddette idee di rigorosità nell'ammettere come necessaria una determinata misura di sorveglianza segreta e dell'assicurazione di certe garanzie, se (e affinché) questa sia considerata legittima.

La "pre-garanzia" offerta dalla Corte EDU a partire dal caso *Klass*, tende ad assicurare all'individuo potenzialmente soggetto a tali misure di sorveglianza la possibilità di pretendersi "vittima" di una violazione della CEDU, anche nel caso in cui non sia in grado di allegare di aver subito una misura concreta di sorveglianza. Nel più recente caso *Roman Zakharov c. Russia*, la stessa Corte ha enunciato i fattori da valutare per decidere se il ricorrente potrà essere o meno considerato vittima, tra cui lo scopo della legislazione che autorizza le misure di sorveglianza segreta, esaminando se il ricorrente può presumibilmente essere affetto da tale legislazione, da una parte, e l'esistenza di rimedi a livello nazionale e la loro effettività, dall'altra.[5]

La sorveglianza segreta è ritenuta un'ingerenza grave nel diritto al rispetto della vita privata delle persone. Conviene dunque riferirsi al sistema di tutela che si è costruito intorno al secondo paragrafo dell'art. 8 della Convenzione europea dei diritti dell'uomo e agli artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'Unione europea, che tutelano il diritto al rispetto della vita privata e la protezione dei dati personali e stabiliscono in quali condizioni tale ingerenza può essere ritenuta legittima. Se il punto di partenza in materia è la sentenza *Klass*, la Corte europea dei diritti dell'uomo si è riferita con meticolosità alla questione delle nuove tecnologie anche (tra molte altre) nella recente sentenza *Szabó e Vissy c. Ungheria*, ritenendo che dati i progressi tecnologici che si sono succeduti dalla citata sentenza, le potenziali ingerenze nell'email, telefoni cellulari e servizi di Internet, così come la sorveglianza di massa, richiedono una protezione più

[3] *Ibidem*.

[4] Cfr. CEDU, *Klass c. Germania*, ric. 5029/71 (1978), par. 36.

[5] Cfr. CEDU, *Roman Zakharov c. Russia* [GC], ric. 47143/06 (2015), par. 171.

pungente della vita privata da parte della Convenzione.[6]
Bisogna fin da subito notare che, se tale protezione è stata tradizionalmente richiesta come limite posto all'esercizio del potere pubblico nei casi in cui ad attuare la sorveglianza segreta erano gli organi dello Stato, la stessa Corte si è riferita di recente, nel caso *Vukota-Bojic c. Svizzera,* alle attività di sorveglianza segreta praticate da un'agenzia di investigazione privata.[7] Si pone, dunque, anche il caso dei sistemi di sorveglianza privata, estranei completamente ai sistemi di sorveglianza statuali, ma anche quella dei sistemi di sorveglianza parastatali, parzialmente estranei a tali sistemi. Tale situazione richiama la questione della tutela dei diritti fondamentali nei confronti dell'esercizio del potere privato (e non già soltanto pubblico) perché le nuove tecnologie sono ormai adoperate non soltanto dagli organi pubblici, ma anche e soprattutto dai privati. Ed occorre sollevare anche un'altra questione perché, se il sistema europeo di tutela dei diritti umani si era apprestato, con il trascorrere degli anni e soprattutto dalla sua creazione nel dopoguerra, a costruire un sistema di garanzia a favore degli individui come risposta alle interferenze degli organi pubblici, tale sistema di garanzie era stato pensato in minor misura in relazione alle ingerenze dei privati. Al tempo stesso, con l'avvenire della globalizzazione e di una maggiore democratizzazione della società, nella quale l'esercizio del potere non corrisponde più soltanto all'organo pubblico, le ingerenze si sono spostate verso l'ambito di azione dei privati, rimanendo però il settore della protezione dei diritti impreparato nei confronti di quest'ultimi. Trova applicazione, in questa ipotesi, la dottrina degli obblighi positivi che pesano sugli Stati, di creazione pretoria, che la Corte europea dei diritti dell'uomo ha costruito nel tempo per prevenire e rimediare alle violazioni commesse da parte dei privati, come lo dimostra, anche nello specifico, la più recente sentenza *Bărbulescu c. Romania*.[8]
Detto questo, conviene fare riferimento allo stato dell'arte che si è concretizzato principalmente intorno al secondo paragrafo dell'articolo 8 della Convenzione europea dei diritti dell'uomo, che tutela il diritto al rispetto della vita privata, nonché all'analogo articolo 7 della Carta dei diritti fondamentali dell'Unione europea.

2. La base legislativa della sorveglianza segreta e le nuove tecnologie

Con riguardo alla CEDU, la Corte europea dei diritti dell'uomo ha spesso posto l'enfasi sul primo requisito enunciato dall'art. 8, il quale esige che ci sia una base legislativa se si vuole procedere all'esercizio della sorveglianza segreta.[9] La Corte esige oramai degli Stati non soltanto che vi sia una base legislativa per le attività di sorveglianza segreta

[6] Cfr. CEDU, *Szabó e Vissy c. Ungheria*, ric. 37138/14 (2016), par. 53.

[7] Cfr. CEDU, *Vukota-Bojic c. Svizzera*, ric. 61838/10 (2016).

[8] Cfr. CEDU, *Bărbulescu c. Romania* [GC], ric. 61496/08 (2017), par. 108-112. Nella sentenza, la Corte ha fatto riferimento a tali obblighi in un caso riguardante una società commerciale che aveva implementato un sistema di sorveglianza delle comunicazioni elettroniche dei suoi impiegati.

[9] Si vedano, tra gli altri, CEDU, *Kopp c. Svizzera*, ric. 23224/94 (1998); *Copland c. Regno Unito*, ric. 62617/00 (2007); *Shimovolos c. Russia*, ric. 30194/09 (2011); *Szabó e Vissy c. Ungheria*, ric. 37138/14 (2016).

(base legislativa che stabilisca in modo chiaro la portata ed il modo di esercizio di tale sorveglianza), ma ha imposto anche dei requisiti che riguardano la qualità della legge che disciplina tale attività di controllo.

Per essere autorizzata, l'attività di sorveglianza segreta deve essere, in primo luogo, prevista dalla legge, la quale deve fornire in modo sufficientemente chiaro e dettagliato una base legislativa che definisca la portata ed il modo di esercizio di tale controllo e deve offrire delle garanzie adeguate ed effettive contro gli abusi. A questo riguardo, la Corte europea dei diritti dell'uomo ha ricordato nel caso *Roman Zakharov c. Russia*, in relazione alle intercettazioni segrete delle comunicazioni telefoniche, alcune delle principali garanzie che tale base legislativa deve comprendere, cd. "minimum safeguards" per evitare abusi di potere: la natura dei reati che possono dare luogo ad un ordine di intercettazione; la definizione delle categorie di persone suscettibili di essere oggetto di intercettazioni; un limite alla durata delle intercettazioni; la procedura da seguire per l'esame, l'uso e l'archiviazione dei dati ottenuti; le precauzioni da prendere al momento di comunicare i dati a terzi; e le circostanze nelle quali tali registrazioni possono o devono essere cancellate o distrutte.[10] Dette garanzie devono essere assicurate anche nella messa in pratica di tali misure[11] e devono essere inoltre offerti, a livello interno, rimedi effettivi se tali garanzie mancassero.[12]

Quanto alle nuove tecnologie, già negli anni novanta la stessa Corte faceva riferimento alle speciali esigenze che lo sviluppo della tecnologia comporta, sottolineando la natura essenziale di tali requisiti specialmente perché la tecnologia disponibile si stava facendo sempre più sofisticata.[13] Nella più recente decisione *Köpke*, la Corte europea dei diritti dell'uomo ha rilevato la necessità di una maggiore attenzione sulla protezione della vita privata, al fine di contrastare le nuove tecnologie della comunicazione che permettono di archiviare e trattare dati personali. Nel caso, che interessava l'impiegato di un supermercato sospettato di aver commesso irregolarità, il quale era stato sottoposto a videosorveglianza da parte di una agenzia privata di investigazioni, la Corte, sebbene ammettendo che nella specie lo Stato non avesse fallito nell'operare un giusto bilancio degli interessi contrapposti, ha tuttavia precisato che avrebbe dato a tali interessi *un peso diverso nel futuro*, tenendo conto della portata delle intrusioni nella vita privata rese possibili dalle nuove e sempre più sofisticate tecnologie.[14]

Sempre con riferimento alle tecnologie utilizzate, si pone la questione di sapere se la tecnologia impiegata sia stata, in un caso determinato, autorizzata dalla legge dato che, si evince da tale giurisprudenza che la legislazione deve definire in modo chiaro e preciso il modo in cui la sorveglianza può essere effettuata, ciò che comprende, eviden-

[10] Cfr. CEDU, *Roman Zakharov c. Russia* [GC], ric. 47143/06 (2015), par. 231.

[11] Cfr. CEDU, *Dragojević c. Croazia*, ric. 68955/11 (2015), nel quale la Corte condanna lo Stato croato perché il sistema non offriva, in pratica, garanzie sufficienti contro ogni possibile abuso.

[12] Cfr. CEDU, *Mustafa Sezgin Tanrıkulu c. Turchia*, ric. 27473/06 (2017). Non essendo stata dimostrata l'effettività dei rimedi indicati, la Corte rileva nel caso una violazione dell'art. 13 della Convenzione. Tali rimedi, infatti, avrebbero dovuto permettere alle persone soggette, o che avessero il sospetto di essere soggette all'intercettazione dei telefoni o delle comunicazioni elettroniche, di proteggere i loro diritti.

[13] Cfr. CEDU, *Kruslin c. France*, ric. 11801/85 (1990), par. 33.

[14] Cfr. CEDU, *Köpke c. Germania* (decisione), ric. 420/07 (2010).

temente, una enunciazione chiara e dettagliata della tecnologia permessa, mancando dunque la base legislativa se effettuata con mezzi non autorizzati. Nel caso *Bykov*, ad esempio, la tecnologia utilizzata in una operazione "test" non era prevista dalle disposizioni che regolamentavano le misure di sorveglianza in causa, non essendo nemmeno il ricorso alla tecnica usata definito da regole specifiche e dettagliate che fornissero delle garanzie adeguate contro eventuali abusi. La Corte europea dei diritti dell'uomo ha ritenuto nella specie che mancava la base legislativa richiesta dall'art. 8 e che la misura di sorveglianza, non era, di conseguenza, conforme alla Convenzione.[15] Anche l'uso improprio delle tecnologie autorizzate, o quello che va oltre gli usi concessi dalla legge, difetta di base legislativa adeguata. Così, nel caso *Taylor-Sabori c. Regno Unito*, la Corte ha rilevato una violazione della Convenzione perché, nel contesto di un'operazione segreta di polizia, erano state effettuate intercettazioni su messaggi inviati via pager, allorché all'epoca degli eventi non vi era alcuno statuto che regolamentasse l'intercettazione di messaggi di pager trasmessi attraverso un sistema di telecomunicazione privato.[16]

Nell'ambito dell'Unione europea, in particolare, la *Risoluzione del Consiglio 96C 329/01* del 17 gennaio 1995 sull'intercettazione legale delle telecomunicazioni prevede inoltre, al punto 1.3, che «non possono essere trasmesse telecomunicazioni non comprese nell'autorizzazione relativa all'intercettazione».

Le garanzie offerte dalla legge devono andare, dunque, di pari passo con gli sviluppi della tecnologia. Laddove l'utilizzo della nuova tecnologia non sia previsto dalla legge in modo sufficientemente chiaro e dettagliato, l'attività di sorveglianza non sarà ritenuta previsibile e sarà, perciò, contraria alle disposizioni della Convenzione, che richiedono invece che la portata ed il modo di controllo esercitati abbiano dette qualità. Sebbene, di conformità con la giurisprudenza della Corte europea dei diritti dell'uomo, l'obbligo di prevedibilità non significhi che, in caso di misure segrete, gli Stati debbano avvertire il sorvegliato delle concrete misure di controllo in corso[17] -anche se alcuni Autori rilevano già i problemi che l'impossibilità di sapere comporta per la tutela dei diritti degli individui sorvegliati[18] e rilevano addirittura l'esistenza di un *right of notification*, una volta

[15] Cfr. Corte EDU, *Bykov c. Russia* [GC], ric. 4378/02 (2009).

[16] Cfr. Corte EDU, *Taylor-Sabori c. Regno Unito*, ric. 47114/99 (2002).

[17] Cfr. di recente, Corte EDU, *Roman Zakharov c. Russia* [GC], ric. 47143/06 (2015), par. 229.

[18] Si veda l'opinione, critica, della dottrina, cui rileva i seri problemi che l'assenza della notifica al sorvegliato può generare per la tutela dei suoi diritti. Così, P. Toomey - B. M. Kaufman, *The notice paradox: secret surveillance, criminal defendants, & the right to notice*, in *S. Clara Law Rev.*, 54, 2014, 843-900, i quali definiscono tale situazione come un paradosso, nel quale l'opportunità dell'individuo sorvegliato di contestare la misura di sorveglianza che lo riguarda è nell'intero controllo del governo, il quale decide se comunicargli o meno la misura.

i dati raccolti e le misure di sorveglianza portate a termine-[19] il sorvegliato deve essere in grado di prevedere con sufficiente chiarezza in quali circostanze e le condizioni in cui lo Stato sarà autorizzato a ricorrere a tali misure. Tale requisito comprende anche la possibilità del pubblico di conoscere e di accedere a tale legislazione.[20] L'assenza del requisito della legalità rende tali misure illegittime, nel cui caso sono talvolta definite come attività di "sorveglianza clandestina", cioè non autorizzata dalla legge; situazione che è oggi ingrandita dal fatto che le nuove tecnologie sono adoperate anche dai privati, spesso illegalmente.[21] In questo senso, la Corte europea dei diritti dell'uomo ha precisato che, come conseguenza dei suoi obblighi positivi, lo Stato è tenuto ad adottare un quadro normativo tendente a proteggere il diritto dell'individuo al rispetto della sua vita privata e della sua corrispondenza.[22]

L'altra questione che si pone è quella delle garanzie fornite da tale legislazione. Il tema dell'accessibilità ai dati personali ottenuti attraverso l'utilizzo della tecnologia è una delle questioni più spinose a questo riguardo. Recentemente la Corte EDU si è riferita a detta necessità nella sentenza *Vukota-Bojic*, censurando nella specie le misure segrete di sorveglianza attuate perché la legislazione in questione non precisava le procedure da seguire per l'archiviazione, l'accesso, l'esame, l'uso, la comunicazione o la distruzione dei dati raccolti, ciò che aumentava il rischio di accesso non autorizzato a tali dati o di divulgazione dei materiali oggetto della sorveglianza.

Se, dunque, è condizione essenziale l'esistenza di una base legislativa che autorizzi le attività di sorveglianza segreta attuate, compresa una enunciazione dei mezzi tecnologici che possono essere utilizzati, è altrettanto importante la qualità della legislazione in questione. E la qualità della legislazione va valutata anche alla luce della tecnologia disponibile, ma non sia inteso che la legge deve inevitabilmente conformarsi allo sviluppo della tecnologia perché, invero, sono le tecnologie che devono adeguarsi alle necessarie garanzie. Rileva a questo riguardo la decisione della Corte EDU nel caso *Shimovolos c. Russia*, la cui sentenza ha ritenuto che la creazione, l'aggiornamento e il funzionamento della banca dati "delle sorveglianze", contenente, nella specie, i dati di

[19] Cfr. F. Boehm - P. de Hert, *Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law*, in *European Journal of Law and Technology*, 3, 2012, i quali fanno riferimento al caso della Corte europea dei diritti dell'uomo, *Associaton for the European Integration and Human Rights e Ekimdzhiev c. Bulgaria*, 28 giugno 2007, n. 62540/00. Nella sentenza citata, la Corte precisa che «as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned» (par. 90). In particolare, per quanto riguarda le misure di sorveglianza dei datori di lavoro nei confronti dei lavoratori, l'obbligo di avvertire con precedenza il sorvegliato dell'attività di sorveglianza attuata vige in 34 Stati membri del Consiglio d'Europa. Si veda, a questo riguardo, la sentenza della Corte EDU, *Bărbulescu c. Romania* [GC], 5 settembre 2017, n. 61496/08, par. 53.

[20] CEDU, *Liberty e altri c. Regno Unito*, ric. 58243/00 (2008); *Shimovolos c. Russia*, ric. 30194/09 (2011).

[21] Tuttavia, la questione della "sorveglianza clandestina" ha raramente dato luogo in quanto tale ad analisi da parte della dottrina. Si vedano, tra i pochi Autori che trattano la questione, R. Costello, *The Right to Privacy, Clandestine Surveillance and International Trade in the United States and European Union*, in *Trinity C. L. Rev.*, 17, 2014, 37-63; K. Lippel, *The private policing of injured workers in Canada: legitimate management practices or human rights violations?*, in *Policy and Practice in Health and Safety*, 1, 2003, 98-118.

[22] Cfr. nel contesto delle relazioni di lavoro con il datore di lavoro privato, *Bărbulescu c. Romania*, cit., par. 116.

un militante per i diritti umani, costituiva una violazione dell'art. 8 della Convenzione, perché, essendo stata istituita da un decreto ministeriale non pubblicato né accessibile al pubblico e non essendo sottoposti allo scrutinio e alla conoscenza del pubblico, le ragioni per la registrazione di una persona nella banca dati, le autorità competenti per ordinare tale registrazione, la durata della misura, la precisa natura dei dati raccolti, le procedure di conservazione e utilizzo dei dati né i controlli e le garanzie esistenti contro gli abusi, il diritto interno non indicava con sufficiente chiarezza la portata e il modo di esercizio del potere di discrezione conferito alle autorità interne per raccogliere e conservare nella banca dati, informazioni sulla vita privata dei particolari.[23]

3. Lo scopo della sorveglianza segreta e le nuove tecnologie

Quanto al requisito dello scopo legittimo della misura segreta, posto anch'esso dall'art. 8 della CEDU, è necessario notare che le nuove tecnologie, essendo oggi ugualmente adoperate dai privati, ma anche nel caso in cui siano adoperate dalle autorità pubbliche, sono utilizzate non soltanto a fini di sicurezza nazionale o prevenzione del crimine, ed occorre dunque chiedersi se taluni odierni utilizzi siano legittimi dal punto di vista giuridico.[24]

Ritornando al voto del giudice Pettiti, egli osservava nel caso *Malone* che gli obiettivi perseguiti dalle misure di sorveglianza segreta si sono *diversificati*. L'intercettazione della polizia per la prevenzione dei crimini e dei reati è soltanto una delle pratiche utilizzate; si aggiungono quelle politiche, quelle giornalistiche e delle personalità...[25] Ne è chiaro esempio il sopracitato caso *Bărbulescu c. Romania*, in cui il datore di lavoro del ricorrente (una società commerciale di diritto privato) aveva messo in pratica un sistema di sorveglianza al fine di controllare l'uso che gli impiegati facevano di Internet, per evitare e reprimere così l'uso personale, da parte dei lavoratori, di tale tecnologia, messa a disposizione sul luogo di lavoro per l'uso professionale.[26] Orbene, nella specie, la Corte EDU ha osservato che non risultava che «le giurisdizioni nazionali avessero sufficientemente verificato la presenza di ragioni legittime che giustificassero la messa in pratica

[23] Cfr. CEDU, *Shimovolos c. Russia*, ric. 30194/09 (2011), par. 69-71.

[24] Si veda, tra gli altri, CEDU, *Brambilla e altri c. Italia*, ric. 22567/09 (2016), nel quale erano state applicate sanzioni a tre giornalisti che avevano intercettato le radiocomunicazioni della gendarmeria con lo scopo di recarsi velocemente sul luogo del crimine e riportare le informazioni ad un giornale. La Corte ha ritenuto, nella specie, che le sanzioni applicate ai tre giornalisti non costituivano una violazione della Convenzione, le quali, in particolare, non infrangevano la libertà di espressione e di informazione tutelata dall'art. 10 della CEDU. Cfr. anche, *Perry c. Regno Unito*, ric. 63737/00 (2003), nel quale la polizia aveva installato una telecamera per filmare in segreto una persona sospettata di aver commesso una serie di rapine, ai fini della sua identificazione, filmati che erano stati poi utilizzati nel contesto delle procedure che lo coinvolgevano, anche se in questo caso la CEDU non fa riferimento esplicito al requisito dello scopo legittimo della misura, bensì al fatto che l'uso della telecamera fosse andato oltre quello consentito dalla legge, ciò che aveva costituito una violazione della Convenzione.

[25] Cfr. *Opinion concordante*, cit.

[26] Cfr. CEDU, *Bărbulescu c. Romania*, cit.

della sorveglianza delle comunicazioni del ricorrente», motivo che è stato di peso per condannare lo Stato romeno, data l'ingerenza nella vita privata del ricorrente.[27]
Poiché non tutte le motivazioni ora invocate sembra che possano giustificare un'ingerenza nella vita privata, occorre stabilire quali tra le finalità che, con l'uso delle nuove tecnologie si vanno diversificando, sono legittime. Innanzitutto, e con riguardo allo scopo della sicurezza nazionale e della prevenzione del crimine se, di conformità con l'art. 8 della CEDU, la Corte ha tendenzialmente accettato che detto obiettivo sia un legittimo scopo tale da poter giustificare l'uso di nuove tecnologie nella sorveglianza segreta delle persone, senza troppo fermarsi a verificare se, effettivamente, l'obiettivo perseguito nella specie fosse tale, potrebbe rivelarsi necessaria una rivalutazione di tale approccio. Infatti, sembrerebbe oggi che i sopramenzionati "obiettivi" siano utilizzati come un passe-partout che tutto può giustificare e, invero, sarebbe quanto meno ingenuo pensare che tutto quello che oggi è sottoposto a sorveglianza segreta al fine di "sicurezza nazionale e prevenzione del crimine", risponda sempre ed esclusivamente a tali scopi.
Un'indagine scrupolosa delle fattispecie esaminate dalla Corte europea dei diritti dell'uomo conduce a pensare che talvolta la finalità non sia questa (o almeno non soltanto questa). Oltre alle sentenze già citate, di recente, ad esempio, la Corte ha ammesso di esaminare in *Vukota-Bojic* un caso di sorveglianza segreta attuata col fine di evitare le frodi alle assicurazioni, anche se nel caso specifico la Corte non ha messo al vaglio la questione dello scopo della misura, indagando invece sulla mancata legalità della stessa.[28] Si citerà inoltre il già citato caso *Perry c. Regno Unito*, nel quale lo scopo perseguito non si inquadrava perfettamente nel contesto della sicurezza o la lotta alla criminalità.[29]
L'urgenza di un maggiore scrutinio sulla questione, da parte della Corte, si rivela palese specialmente in vista del fatto che le tecnologie permettono oggi di fare un controllo (anche massivo) sulla popolazione senza fare distinzioni sulle finalità perseguite.
Poi, più in generale, occorrerebbe chiedersi anche *quali siano gli scopi che autorizzerebbero tali misure*. Gli scopi enunciati nel secondo paragrafo dell'art. 8 CEDU,[30] i quali giustificherebbero una limitazione del diritto al rispetto della vita privata, sebbene chiaramente tassativi, sembrano per così dire "onnicomprensivi" e, a dir vero, potrebbero conficcarvisi i più svariati obiettivi, rivelandosi indispensabile l'intervento delle Corti europee per far chiarezza sul tema. In passato la Corte EDU ha eluso la questione, come l'ha fatto nel caso *Copland c. Regno Unito*, analizzando sotto il profilo della mancata legalità le misure di sorveglianza segreta attuate che, secondo il governo britannico servivano, nella specie, ad evitare abusi nell'utilizzo delle strutture professionali (telefono, posta elettronica e Internet) da parte della ricorrente, la quale svolgeva le mansioni di assistente personale in uno stabilimento scolastico, ma senza esaminare la questione dello

[27] *Ibidem*, par. 135.

[28] Cfr. CEDU, *Vukota-Bojic c. Svizzera*, ric. 61838/10 (2016).

[29] Cfr. CEDU, *Perry c. Regno Unito*, ric. 63737/00 (2003).

[30] Gli obiettivi enunciati dal secondo paragrafo dell'art. 8 CEDU sono: la sicurezza nazionale, la pubblica sicurezza, il benessere economico del paese, la difesa dell'ordine e la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui.

scopo della misura.[31] Tuttavia, nel recente caso *Bărbulescu*, la Corte è andata a ribadire la necessità che le misure di sorveglianza siano giustificate da un legittimo obiettivo[32] anche se, un intervento più minuzioso che stabilisca con più chiarezza qual è il margine di manovra degli Stati in questo ambito, sarebbe quanto meno urgente.

4. La necessità e la proporzionalità delle misure di sorveglianza segreta e le nuove tecnologie

Se anche la misura di sorveglianza segreta si rivelasse idonea a perseguire uno scopo legittimo, i mezzi utilizzati, comprese le nuove tecnologie, devono essere *necessari* e *proporzionati*. Per rispondere a tale esigenza conviene esaminare la portata delle misure segrete attuate e chiedersi cosa permette in concreto di fare tale sistema di sorveglianza. In breve, occorre sapere qual è il grado di intrusione del sistema di sorveglianza nella vita privata dell'individuo e rammentare, innanzitutto, che l'intero Diritto europeo dei diritti umani (compreso il diritto derivato dalla CEDU) è basato sul principio secondo cui il fine non sempre giustifica i mezzi, essendo assolutamente irrilevante dal punto di vista giuridico il tanto (e tristemente) diffuso pensiero machiavellico secondo cui, guardando al fine, «i mezzi saranno sempre giudicati onorevoli e da ciascuno lodati».[33] In materia è stata cruciale la sentenza della Corte di giustizia dell'Unione europea nella causa *Digital Rights Ireland e Seitlinger e altri*.[34] Nella fattispecie, si chiedeva in via pregiudiziale sulla validità della Direttiva 2006/24/CE del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione (cd.

[31] Cfr. CEDU, *Copland c. Regno Unito*, ric. 62617/00 (2007).

[32] Cfr. CEDU, *Bărbulescu c. Romania*, cit.

[33] Si veda per quest'ultimo pensiero, N. Machiavelli, ne *Il Principe*, (capitolo XVIII), in *Tutte le opere di Niccolò Machiavelli*, volume unico, Firenze, 1833, 310. In senso completamente contrario a tale pensiero, si vedano i "secondi paragrafi" degli articoli 8 a 11 della CEDU, dai quali scaturisce che, anche in presenza di uno scopo legittimo, è requisito per la limitazione dei diritti enunciati che la misura adottata sia "necessaria in una società democratica"; nozione che ha dato luogo ad una giurisprudenza molto acuta della Corte EDU intorno alla "proporzionalità" delle misure di restrizione dei diritti. Rinvieremo, per questo argomento, a Y. Arai-Takahashi, *The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR*, Antwerp, 2002. Più recentemente, E. Cannizzaro - F. De Vittor, *Proportionality in the European Convention on Human Rights*, in R. Kolb - G. Gaggioli (eds.), *Research handbook on human rights and humanitarian law*, Cheltenham, 2013, 125-145; J. Christoffersen, *Human Rights and Balancing: the Principle of Proportionality*, in Ch. Geiger (ed.), *Research handbook on human rights and intellectual property*, Cheltenham, 2015, 19-38; E. Lambert-Abdelgawad, *La proportionalité dans le système de la Convention européenne des droits de l'homme*, in H. Ruiz Fabri - L. Gradoni (sous la direction de), *La circulation des concepts juridiques: le droit international de l'environnement entre mondialisation et fragmentation*, Paris, 2009, 427-473.

[34] Cfr. CGUE, C-293/12 e C-594/12, Digital Rights Ireland e Seitlinger e a. (2014).

direttiva sulla *data retention*),[35] che imponeva ai fornitori di tali servizi, di conservare, all'insaputa delle persone interessate, i dati elencati all'art. 5 della stessa al fine di renderli all'occorrenza accessibili alle autorità nazionali competenti. I giudici della CGUE si sono posti due domande decisive intorno alle quali, si gioca, in generale, la legittimità delle misure di sorveglianza segreta, che miravano a chiarire principalmente due questioni: gli atti in questione erano idonei a realizzare gli obiettivi legittimi perseguiti dalla normativa di cui trattasi? Gli stessi atti superavano i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi?

L'Avvocato generale, mettendo il dito nella piaga, precisava che il sistema di conservazione ed utilizzo dei dati personali in causa, poteva ingenerare nelle persone la sensazione che la loro vita privata fosse oggetto di costante sorveglianza, elemento che la Corte di giustizia ha messo in risalto –e, in questo senso, la dottrina ha già avvertito la Comunità internazionale sul "*chilling effect*" di talune misure contro il terrorismo;[36] effetto che, come sappiamo, cerca già di evitarsi nella specifica disciplina della tutela della libertà di espressione e di informazione. Precisamente, per rigettare la validità della Direttiva in causa, la Corte di giustizia si è riferita all'uso delle nuove tecniche di indagine, affermando che, se si deve constatare che la lotta contro la criminalità grave, in particolare contro la criminalità organizzata e il terrorismo, è di capitale importanza per garantire la sicurezza pubblica e *la sua efficacia può dipendere in larga misura dall'uso delle moderne tecniche di indagine*, tuttavia, «simile obiettivo di interesse generale, per quanto fondamentale, *non può di per sé giustificare il fatto che una misura di conservazione, come quella istituita dalla direttiva 2006/24, sia considerata necessaria ai fini della suddetta lotta*».[37] Di fatto, il sistema previsto dalla Direttiva, che non offriva né chiarezza legislativa né garanzie, eccedeva, secondo la Corte di giustizia, i limiti imposti dal *principio di proporzionalità*.[38]

Occorre rilevare, come lo ha fatto la stessa Corte di giustizia nella sua sentenza, che tale sistema di conservazione dei dati interessava «in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traf-

[35] Si vedano, M.-P. Granger - K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, in *Eur. Law Rev.*, 39, 2014, 835-850; T. Konstadinides, *Mass Surveillance and Data Protection in EU Law – the data Retention Directive Saga*, in M. Bergström - A. Jonsson Cornell (eds.), *European police and criminal law*, Oxford, 2014, 69-84; E. Stoeva, *The Data Retention Directive and the right to privacy*, in *ERA Forum*, 15, 2014, 575-592; M. Nettesheim, *The CJEU's Decision on the Data Retention Directive*, in B. Hess - C.M. Mariottini (eds.), *Protecting privacy in private international and procedural law and by data protection: European and American developments*, Farnham, 2015, 57-69; L. Marin, *The Fate of the Data Retention Directive: about Mass Surveillance and Fundamental Rights in the EU Legal Order*, in V. Mitsilegas *et al.* (eds.), *Research handbook on EU criminal law*, Cheltenham, 2016, 210-229.

[36] E. Fura - M. Klamberg, *The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA*, in *Essays in honour of Nicolas Bratza*, Oisterwijk, 2012, 463-481.

[37] Sentenza *Digital Rights*, cit., par. 51. Il corsivo è nostro.

[38] Sull'importanza del principio di proporzionalità per la tutela del diritto al rispetto della vita privata nel sistema europeo di tutela dei diritti fondamentali, si veda, R. Costello, *The Right to Privacy, Clandestine Surveillance and International Trade in the United States and European Union*, in *Trinity C. L. Rev.*, 17, 2014, 59, che osserva, distinguendo in questo senso il sistema europeo dal sistema statunitense, che *«[t]he European approach as embodied in the Articles 7 and 8 of the European Charter of Fundamental Rights and Article 8 of the European Convention on Human Rights have long conceptualised privacy as allied with rights to personal dignity and family life in which proportionality acts as the watchword for any infringement»*.

fico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi»[39] e che la Direttiva non imponeva «alcuna relazione tra i dati di cui prevede la conservazione e una minaccia per la sicurezza pubblica».[40] La Corte di giustizia rilevava inoltre che la direttiva 2006/24 non prevedeva alcun criterio oggettivo che permettesse di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali riguardanti reati che potessero essere considerati sufficientemente gravi da giustificare siffatta ingerenza e che tale Direttiva non conteneva nemmeno le condizioni sostanziali e procedurali ad esso relative, oltre alla lunga durata di sei mesi, della conservazione dei dati.[41] Tale sistema, dunque, né prevedeva norme chiare e precise che delimitassero la portata della misura, né offriva delle garanzie ai sorvegliati. Di gran peso è stato il fatto che la Direttiva 2006/24 non prevedesse garanzie sufficienti, come richieste dall'art. 8 della Carta dei diritti fondamentali dell'UE, che permettessero di assicurare una protezione efficace dei dati conservati contro i rischi di abuso, nonché contro eventuali accessi e usi illeciti dei suddetti dati, oltre alla questione, già nota, che la Direttiva non imponesse che i dati fossero conservati sul territorio dell'Unione. Tutto ciò, eccedeva, secondo la Corte di giustizia, i limiti imposti dal principio di proporzionalità.

In materia occorre anche menzionare, sebbene sulla base di fatti completamente diversi, il sopramenzionato caso *Bărbulescu*, nel quale erano stati registrati e archiviati sia i flussi che i contenuti delle comunicazioni del ricorrente, tra cui vi erano comunicazioni personali, anche a carattere intimo. Nella specie, il ricorrente non era stato informato con precedenza della portata e della natura della sorveglianza attuata dal suo datore di lavoro, né della possibilità che quest'ultimo avesse accesso al tenore stesso delle sue comunicazioni.

Nella sua sentenza, la Corte EDU ha ammesso di essere cosciente che la situazione si evolve rapidamente in questo ambito, ma che, tuttavia, «*elle estime que la proportionnalité et les garanties procédurales contre l'arbitraire sont des éléments essentiels*», ragione per la quale ha enunciato una serie di "fattori" di cui le autorità interne devono tenere conto al fine di valutare se la misura di sorveglianza attuata è proporzionale ed offre le garanzie adeguate. L'elenco fornito dalla Corte costituisce una sorta di "test" che ogni misura di sorveglianza adottata in questo ambito dovrebbe poter superare al fine di essere considerata una misura proporzionale, a sapere: l'individuo, è stato informato della possibilità che il sorvegliante prendesse delle misure di sorveglianza della sua corrispondenza e delle sue comunicazioni, così come dell'attuazione di tali misure? Qual è la portata della misura di sorveglianza e il grado di intrusione nella vita privata dell'individuo? Il sorvegliante, ha avanzato dei motivi legittimi per giustificare la sorveglianza di tali comunicazioni e l'accesso al loro contenuto? Sarebbe stato possibile attuare un sistema meno intrusivo? Quali sono state le conseguenze della sorveglianza per l'individuo che è stato oggetto delle misure e, in che modo il sorvegliante ha utilizzato i risultati della misura di sorveglianza? Sono state offerte delle garanzie adeguate al sorvegliato?[42] I

[39] CGUE, *Digital Rights*, cit., par. 57.

[40] *Ibidem*, par. 59.

[41] *Ibid.*, par. 60-64.

[42] Cfr. CEDU, *Bărbulescu c. Romania* [GC], ric. 61496/08 (2017), par. 121.

fattori elencati, sebbene, nello specifico, inseriti nel contesto delle relazioni tra datori di lavoro e lavoratori, possono senz'altro servire da guida per misurare la proporzionalità delle misure di sorveglianza anche in altri contesti.

5. Conclusioni

L'esercizio del potere viene rappresentato oggi, tra molti altri fattori, dall'uso illimitato delle nuove tecnologie. Correlativamente, i diritti umani si pongono come limite a tale esercizio illimitato del potere. Proprio perché il Diritto dei diritti umani tende (e deve tendere) a tutelare l'individuo dall'illimitatezza delle situazioni che la realtà impone, se la realtà impone all'individuo delle circostanze che possono mettere in pericolo o recare danno ai suoi diritti, il Diritto, da esso creato, deve tendere a delimitare tali situazioni, in modo che egli possa essere ragionevolmente protetto da tali minacce.
Dinanzi a tale tendenza all'uso illimitato delle tecnologie della sorveglianza, si rivela necessario che tali sistemi soddisfino determinati requisiti ed offrano delle garanzie affinché non rappresentino, a sua volta, un rischio per le persone, e che soltanto taluni sistemi possano essere autorizzati. Occorre dunque che l'obiettivo della trasparenza (che puntava, ab origine, i suoi riflettori sugli individui), punti ora l'obiettivo verso i controllori, al fine di offrire le necessarie garanzie agli individui. Ciò, al fine di evitare che, come affermava la Corte nella sua celebre sentenza *Klass*, l'assicurazione offerta dalla Convenzione di beneficiare di un diritto garantito non possa essere soppressa dal semplice fatto di mantenere l'interessato nell'ignoranza della sua violazione.
D'altra parte e, allo stesso tempo, sembra che taluni sistemi di sorveglianza che si vanno diffondendo nei tempi più recenti, che non hanno uno scopo definito, come i cd. sistemi "acchiappa-farfalle", contravvengano palesemente i termini della Convenzione europea dei diritti dell'uomo, la quale enuncia tassativamente gli scopi che possono giustificare un'ingerenza nella vita privata e familiare delle persone e pone come limite la proporzionalità della misura.
L'approccio sempre più severo e meno timoroso nei confronti dei sorveglianti e di chi, più in generale, fa uso di nuove tecnologie per sorvegliare le persone, mostrato dalle Corti europee nelle più recenti decisioni, tra cui le sentenze nei casi *Bărbulescu* e *Digital Rights*, appare come quello preferibile in materia. Il giudice Pettiti evocava in tale senso la necessità di una «nozione europea di *deontologie statali* della sorveglianza degli individui»,[43] idea che potrebbe rilanciarsi oggi anche nei confronti dei privati, che hanno ora facilmente accesso alle nuove tecnologie di sorveglianza.
L'impresa non è impossibile. Il ruolo del Diritto deve tendere a disciplinare, in tale senso, le attività di sorveglianza che fanno uso di nuove tecnologie (e non il contrario), perché quest'ultime non conoscono limiti di fronte alle esigenze di tutela dei diritti; limiti che la legge è invece tenuta a rispettare. Se, dunque, l'invenzione di nuove tecnologie condizionano inevitabilmente l'attività normativa, anche quest'ultima ha un ruolo nell'inquadrare le prime. Se qualcuno vorrà obiettare che si tratta di una visione poco realista della questione, si potrà rispondere con una riflessione che René Cassin

[43] Cfr. *Opinion*, cit.

fece con occasione di una conferenza tenutasi a Roma quasi cinquant'anni fa, nella quale, riferendosi al ruolo del Diritto dinanzi alle realtà, affermò che è troppo comodo dire che il diritto è una semplice "mise en forme" di ciò che le realtà impongono perché, infatti, «se il Diritto subisce le realtà, esso arriva anche a crearle».[44] È sulla base di questo ragionamento che, nel suo approccio verso le nuove tecnologie, dovrebbe essere basato, a nostro avviso, il sistema europeo di tutela dei diritti umani in materia di sorveglianza segreta.

[44] Cfr. R. Cassin, *Comment protéger les droits de l'homme*, in *Com. int.*, XXV, 1970, 467. La traduzione è nostra.

La digitalizzazione della pubblica amministrazione*

Francesco Martines

Abstract

La digitalizzazione della pubblica amministrazione rappresenta una delle principali innovazioni che ha inciso sia sul piano dell'organizzazione dell'attività amministrativa sia su quello della disciplina delle singole procedure; inoltre, essa ha comportato rilevanti novità nell'ambito dei rapporti con l'utenza dei servizi amministrativi.
Il contributo, muovendo da un'analisi del contesto normativo internazionale ed europeo, mira ad approfondire la disciplina introdotta a livello interno attraverso le norme contenute nel Codice dell'Amministrazione Digitale, recentemente modificato ed integrato in attuazione della delega legislativa contenuta nella legge 124/2015.
Lo studio propone una riflessione critica destinata a mettere in evidenza non soltanto gli aspetti positivi della riforma ed i vantaggi che essa ha comportato nell'implementazione dei canoni di efficienza dell'azione pubblica, ma anche i limiti che essa reca con sé e le incognite che il cambiamento in atto ha comportato.
In ultimo, è sviluppato un focus sull'incidenza della digitalizzazione nell'ambito della materia processuale.

The implementation of ICT (Information and Communication Technologies) in the area of public administration is one of the main innovations that affect the organization of administrative activities and procedures; moreover, it has involved significant changes in the relationship with users of public services.
This paper, moving from the analysis of the international and EU legal contexts, aims to examine the Italian rules recently introduced in the Digital Administration Code, integrated by Law 124/2015.
A critical reflection is proposed about the advantages ICT in the implementation of the efficiency of public procedures, as well as the limits of the same. Lastly, the impact of ICT in the field of administrative trials is explored.

Sommario

1. Nozione di *e-government*. Il contesto internazionale ed europeo. – 2. L'uso delle ICT come strumento per la realizzazione del modello di c.d. *Open Government*. – 3. La legge 124/2015 e la riforma del CAD. – 4. Le incognite del processo di digitalizzazione. – 5. La digitalizzazione della funzione giurisdizionale.

Keywords: Codice dell'amministrazione digitale (CAD), Digitalizzazione, Amministrazione pubblica, E-government, Open data.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio anonimo, in quanto riproduce la relazione presentata dall'A. al convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno" (Messina, 26-27 maggio 2017).

1. Nozione di *e-government*. Il contesto internazionale ed europeo

Con il termine *e-government* (amministrazione digitale) si indica il processo di informatizzazione della pubblica amministrazione ossia, secondo la Comunicazione del 26 settembre 2003 della Commissione Europea, «l'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, coniugato a modifiche organizzative ed all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici ed i processi democratici e di rafforzare il sostegno alle politiche pubbliche»[1].

Nel tempo la nozione di *e-government* si è profondamente evoluta in relazione al progresso delle *Information and Communication Technologies* (ICT) che costituiscono un settore nel quale i cambiamenti sono costanti e molto rapidi. Di conseguenza, contrariamente all'inclinazione tipica del giurista (e del giuspubblicista in particolare) verso una sistematica fissazione di categorie e nozioni basilari a fondamento degli studi e delle interpretazioni del diritto positivo, *in subiecta materia* il metodo tradizionale di elaborazione scientifica ed ermeneutica, affidato alla rigorosa cristallizzazione delle nozioni fondamentali, deve cedere il passo ad un approccio connotato da elasticità, mobilità, flessibilità. Il che se, per un verso, assicura un certo dinamismo del pensiero e delle teorie, certamente coerente con le caratteristiche della c.d. "società liquida"[2], per altro verso fa sfumare - o per lo meno riduce notevolmente - i margini per conseguire l'obiettivo della certezza del diritto (o per avvicinarvisi quanto più possibile), valore finale cui ogni regolazione normativa e l'ermeneutica giuridica connessa tendono (o dovrebbero tendere).

Di recente la Commissione Europea ha adottato la Comunicazione COM(2016)/179 del 19.4.2016 con la quale ha fissato i principi di base cui deve ispirarsi l'azione per l'*e-government* per il periodo 2016-2020[3]. L'obiettivo cui deve tendere l'azione di implementazione delle nuove tecnologie nel settore dell'azione amministrativa, secondo quanto indicato dalla Commissione Europea, deve ispirarsi ai valori della massima trasparenza, efficienza ed inclusività affinchè vengano erogati «servizi pubblici end-to-end senza frontiere, il più possibile personalizzati ed intuitivi a tutti i cittadini e a tutte le imprese nell'UE».

Lo strumento per garantire la compiuta realizzazione di questi obiettivi, secondo l'impostazione della Commissione, va rinvenuto nel principio del libero accesso ai dati ed ai servizi delle amministrazioni pubbliche, sia a livello nazionale che transfrontaliero. L'accesso ai cosiddetti *Open Data* da parte di tutti coloro che abbiano un comune interesse (senza, dunque, che sia richiesta una particolare qualificazione giuridica dell'in-

[1] Comunicazione della Commissione Europea del 26 settembre 2003 "Il ruolo dell'e-governement per il futuro dell'Europa". In dottrina, fra i contributi più recenti si segnala Aa.Vv., *L'e-Government in Italia: situazione attuale, problemi e prospettive*, in *Questioni di Economia e Finanza*, Banca d'Italia, 2016; F. Bassanini, *Twenty years of administrative reforms in Italy*, in *Review of Economic Conditions in Italy*, 3/2009, 369 ss.; D. Coursey - D.F. Norris, *Models of E-Government: Are They Correct? An Empirical assessment*, in *Public Administration Review*, 3/2008, 523 ss.; M. Gascò, *New Technologies and Institutional Change in Public Administration*, in *Social Science Computer Review*, 1/2003, 6 ss.

[2] Z. Bauman, *Modernità liquida*, Bari, 2011; Id., *La società dell'incertezza*, Bologna, 2014.

[3] www.ec.europa.eu/transparency/regdoc/rep/1/2016/IT/1-2016-179-IT-F1-1.PDF

teresse medesimo) costituisce il punto di arrivo di quel percorso che dalla segretezza dell'azione amministrativa ha consentito di giungere alla totale trasparenza della stessa, sia sotto il profilo dell'attività procedimentale che della organizzazione amministrativa. Soltanto attraverso la totale apertura verso le parti interessate potrà realizzarsi un effettivo coinvolgimento delle stesse nel processo decisionale il che, fra l'altro, responsabilizzerà maggiormente le pubbliche amministrazioni in un'ottica non soltanto giuridica (aquiliana) ma anche etica (c.d. *accountability*). Tale apertura, come osserva la Commissione, contribuirà alla crescita ed alla competitività.

La Commissione europea, nel prosieguo della comunicazione citata, individua una serie di priorità strategiche da realizzarsi entro il 2020 che impegnano fattivamente tutti gli Stati membri in un'ottica di collaborazione ed impegno.

Dinanzi a tali strategie, ci si deve interrogare sulle condizioni concrete che si presentano nel nostro Paese affinchè possano realizzarsi gli obiettivi programmati.

D'altronde, gli impegni sul fronte dell'*e-government* scaturiscono non soltanto dai vincoli europei ma anche da specifici obblighi internazionali. Da ultimo, il fenomeno a livello globale è stato analizzato dalle Nazioni Unite le quali, nell'ultimo Rapporto annuale sull'*e-government* quale strumento di sviluppo sostenibile (2016)[4], hanno evidenziato un sensibile aumento dei Paesi che utilizzano strumenti informatici nella pubblica amministrazione per offrire servizi *online* ai cittadini. Inoltre, è stato evidenziato come il ricorso alle ICT può agevolare e rendere più efficiente l'attività dell'amministrazione sia nel c.d. *back office* (attività interna della pubblica amministrazione) che nel c.d. *front office* (relazione con il pubblico). Quanto al primo profilo l'amministrazione grazie alle ICT ricerca i documenti più facilmente, accede direttamente agli atti di altre amministrazioni, trasmette e riceve dati in tempo reale: può dunque esercitare le proprie funzioni istituzionali in tempi rapidi e con costi minori. Quanto al secondo profilo, il cittadino può avere costantemente a disposizione informazioni tramite una connessione ad internet senza bisogno di accedere fisicamente agli uffici, compiere in qualsiasi momento e da qualsiasi luogo attività che in precedenza presupponevano un accesso diretto presso un ufficio della pubblica amministrazione, evitare di dovere fornire informazioni già in possesso della pubblica amministrazione; il tutto, anche in questo caso, con ingente risparmio di tempo, energie e risorse.

Risponde alla realizzazione di questi obiettivi, in particolare, una delle strategie fondamentali individuate dalla Commissione Europea nella citata Comunicazione del 2016, ovvero la interoperabilità delle varie banche dati della pubblica amministrazione, da intendersi come la «capacità delle singole componenti del sistema PA di interagire orizzontalmente e verticalmente, ossia di fare rete. L'interoperabilità è infatti la capacità di due o più sistemi di connettersi fra loro e dialogare in forma automatica, scambiando informazioni e condividendo risorse»[5].

[4] *The United Nations E-Government Survey 2016: e-Government in Support of Sustainable Development, July 2016* (www.publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016).

[5] Aa.Vv., *L'e-Government in Italia: situazione attuale, problemi e prospettive*, in *Questioni di Economia e Finanza*, cit., 27.

2. L'uso delle ICT come strumento per la realizzazione del modello di c.d. *Open Government*

L'uso delle ICT è senz'altro una grande leva per la semplificazione e la riorganizzazione dei procedimenti amministrativi promuovendo un maggiore coordinamento delle competenze.

Uno dei principali problemi legati alla piena realizzazione di tali obiettivi è dato dall'ingente investimento finanziario che l'informatizzazione della pubblica amministrazione ha richiesto e richiede tuttora. Per tale ragione, la diffusione delle ICT nella pubblica amministrazione ha costituito, giocoforza, una delle ragioni alla base di un rinnovato centralismo che caratterizza l'approccio sistemico di molte delle riforme strutturali degli ultimi vent'anni.

L'ultimo rapporto ONU sullo sviluppo dell'*e-government* del 2016 ha evidenziato come la diffusione delle ICT sia alla base della piena realizzazione del modello di c.d. *Open Government*, in base al quale l'esercizio del potere pubblico deve ispirarsi a totale apertura e trasparenza favorendo la massima partecipazione dei cittadini (c.d. democrazia partecipata) e garantendo allo stesso tempo maggiori margini di controllo sul risultato finale[6]. I principi su cui si fonda l'*Open Government* sono:

- la trasparenza, finalizzata a promuovere l'*accountability* dell'amministrazione attraverso la pubblicazione delle informazioni dell'attività svolta (in questo senso, in Italia, un segnale forte è stato dato con le disposizioni relative agli obblighi di pubblicazione di cui al d.lgs. 33/2013 nonché alla disciplina sul c.d. accesso civico);
- la collaborazione inter-istituzionale che diviene volano di efficienza dell'azione complessiva dell'amministrazione, ai diversi livelli di governo (centrale e periferico).

Il modello in esame, di origine statunitense, è stato esportato a livello internazionale nel 2011 attraverso un'iniziativa multilaterale denominata *Open Government Partnership* (OGP)[7] che coinvolge oltre sessantacinque Stati nell'impegno di adottare concrete misure per la piena realizzazione a livello interno di modelli di amministrazione ispirati ai valori dell'*Open Government*. Il Governo italiano ha predisposto un proprio *Action Plan* nel 2012, successivamente aggiornato in ulteriori edizioni con modifiche ed integrazioni (da ultimo, il 20 settembre 2016, è stato approvato il Terzo Piano Nazionale

[6] F. Costantino, voce *Open Government*, in *Dig. pubbl.*, *Agg.*, Torino, 2015; E. Carloni, *L'amministrazione aperta. Regole e limiti dell'open Government*, Rimini, 2014; Id., *Amministrazione aperta e governance dell'Italia digitale*, in *Giornale dir. amm.*, 2012, 11, 1041.

[7] www.opengovpartnership.org

d'Azione 2016/2018 e, il 29 giugno 2017, l'Addendum del Terzo Piano d'Azione)[8].
L'opportunità di promuovere un'amministrazione realmente aperta, innovativa e partecipata è stata evidenziata anche in sede OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) che, nel luglio del 2014, ha adottato una raccomandazione sulle strategie di Governo digitale[9] nella quale viene tratteggiato un percorso virtuoso che valorizzi sia i vantaggi dell'utilizzo delle ICT nell'organizzazione dell'azione amministrativa sia le ulteriori ricadute che tale utilizzo porta con sé nell'ambito del rapporto con gli utenti dei servizi pubblici.
Secondo la Raccomandazione OCSE del 2014, un ruolo centrale in questo percorso è assunto dalla trasparenza, da intendersi non soltanto come accesso libero ai documenti amministrativi ma anche come *Open Data*, il che comporta che i dati resi accessibili sono altresì suscettibili di generalizzato riutilizzo da parte di operatori pubblici e privati.
Rispetto al quadro nazionale, si segnala che nel mese di ottobre 2015 l'Italia – insieme ad altri sedici Paesi – ha firmato la Carta internazionale degli *Open Data*, adottata nell'ambito della citata OGP, la quale comprende principi, azioni specifiche, orientamenti interpretativi sull'attuazione delle strategie e delle politiche di *Open Data*[10].
In maniera più incisiva, l'art. 52 del Codice di Amministrazione Digitale (d.lgs. 7 marzo 2005, n. 82, CAD) sull'accesso telematico e il riutilizzo dei dati in possesso delle pubbliche amministrazioni, così come modificato dal d.l. 179/2012, conv. in l. 221/2012, stabilisce che le amministrazioni «pubblicano nel proprio sito web (…) il catalogo dei dati, dei metadati e delle relative banche dati in loro possesso ed i regolamenti che ne disciplinano l'esercizio della facoltà di accesso telematico ed il riutilizzo, fatti salvi i dati presenti in Anagrafe tributaria». Lo stesso articolo stabilisce che «i dati e i documenti che le amministrazioni titolari pubblicano senza l'espressa adozione di una licenza si intendono rilasciati come dati di tipo aperto» (c.d. *Open Data by Default*).
Anche l'art. 68, c. 3, del CAD recante la definizione dei dati di tipo aperto è stato riscritto nel 2012 identificandone le seguenti principali caratteristiche: disponibilità dei dati in forma disaggregata; disponibilità secondo i termini di una licenza che ne consenta il riutilizzo anche per finalità commerciali; accessibilità attraverso le tecnologie dell'informazione e della comunicazione in formato aperto; disponibilità gratuita op-

[8] www. open.gov.it/terzo-piano-dazione-nazionale. Rispetto alle precedenti edizioni, il Terzo Piano di Azione si distingue per il fatto che esso è scaturito da un'ampia concertazione che ha visto coinvolte non soltanto le diverse amministrazioni pubbliche (centrali e periferiche) ma anche i soggetti privati, in particolare associazioni ed enti provenienti dal mondo universitario, dai centri di ricerca, dalle associazioni di consumatori e di categoria. L'ampio coinvolgimento dei soggetti esterni alla pubblica amministrazione può considerarsi la vera novità del Terzo Piano d'Azione che, in un'ottica di costante implementazione ed aggiornamento delle strategie, ha previsto l'istituzione di un *Open Government Forum* permanente allargato agli *stakeholders*, che si occupi periodicamente di monitoraggio e controllo del raggiungimento degli obiettivi. Le specifiche azioni del piano sono riconducibili a tre ambiti fondamentali: 1) trasparenza e *Open Data*; 2) partecipazione e *accountability*; 3) cittadinanza digitale e innovazione. Per ciascuna azione il Piano indica i soggetti responsabili, gli obiettivi prefissati, gli impegni specifici, i tempi di attuazione e i valori OGP sottesi.

[9] www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

[10] La Carta si fonda su sei principi cardine relativi ai dati che devono essere: *Open by Default*; *Timely and Comprehensive*; *Accessible and Usable; Comparable and Interoperable*; *For Improved Governance and Citizen Engagement*; *For Inclusive Development and Innovation*. Cfr. www.opendatacharter.net

pure al costo marginale effettivamente sostenuto per la riproduzione e divulgazione.
Il d.lgs. 33/2013 ha, infine, recepito la nozione di *Open Data* pur inserendola in un quadro normativo disorganico in cui la nozione di dato aperto viene confusa nella più ampia categoria della trasparenza senza che siano adeguatamente colte le differenti finalità e disciplina.

3. La legge 124/2015 e la riforma del CAD

Con l'ultima riforma strutturale della pubblica amministrazione messa in campo dal nostro legislatore (l. 7 agosto 2015, n. 124, c.d. Riforma Madia) si è cercato di imprimere un significativo impulso alla realizzazione degli obiettivi e delle strategie più recenti in punto di *e-government*.
Ai sensi dell'art. 1 della l. 124/2015 – rubricato "Carta della cittadinanza digitale" – il Governo è stato delegato ad emanare norme di modifica al CAD volte a «garantire ai cittadini ed alle imprese il diritto di accedere a tutti i dati, i documenti ed i servizi di loro interesse in modalità digitale" e «la semplificazione nell'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici».
Fra i criteri direttivi della delega spicca, per il valore innovativo rispetto a precedenti interventi di riforma ed aggiornamento del CAD, «la ridefinizione e semplificazione dei procedimenti amministrativi, in relazione alle esigenze di celerità dei tempi e trasparenza nei confronti dei cittadini e delle imprese, mediante una disciplina basata sulla loro digitalizzazione e per la piena realizzazione del principio "innanzitutto digitale" (*digital first*), nonché dell'organizzazione e delle procedure interne a ciascuna amministrazione».
La delega è stata attuata con il d.lgs. 26 agosto 2016, n. 179, che ha apportato rilevanti modifiche al testo del CAD finalizzate a realizzare un'opera di semplificazione e razionalizzazione.
Fra gli interventi più significativi si segnala:
- l'istituzione di un'Anagrafe Nazionale della Popolazione Residente (ANPR) che prenderà il posto delle anagrafi dei comuni costituendo un'unica banca dati nazionale;
- la realizzazione del Sistema Pubblico di gestione dell'Identità Digitale (SPID) che permetterà agli utenti di accedere con un unico profilo e *password* identificativa ai servizi *online* della pubblica amministrazione (art. 64 del CAD);
- l'introduzione dell'obbligo per tutte le amministrazioni di accettare i pagamenti spettanti a qualsiasi titolo attraverso strumenti di pagamento elettronico;
- la promozione della diffusione del domicilio digitale per le persone fisiche al fine di facilitare le comunicazioni con le pubbliche amministrazioni (art. 3 *quinquies* del CAD);
- la diffusione della connettività internet negli uffici e nei luoghi pubblici con *free access* per gli utenti dei servizi (art. 8 *bis* del CAD).
Le modifiche introdotte al CAD dal decreto legislativo attuativo della Riforma Madia sono tutte accomunate dall'obiettivo della semplificazione, che rappresenta un traguardo ancora ben lontano dall'essere raggiunto soprattutto nella realtà della pubblica amministrazione italiana connotata – a dispetto degli ordinamenti di altri Paesi euro-

pei – da un forte tasso di burocrazia e complessità che ostacola il conseguimento di risultati significativi in termini di sviluppo sostenibile e competitività del sistema Paese, incidendo negativamente sulla complessiva economia nazionale.
La nozione di semplificazione, connessa alla digitalizzazione, quale risultante dalle nuove norme introdotte nel CAD, risulta invero arricchita ed integrata da nuovi contenuti ed orientamenti: difatti, ai sensi dell'art. 1 lett. *dd)* e *ee)* del CAD, le pubbliche amministrazioni hanno l'obbligo di garantire i principi – di cui si è detto in precedenza – della interoperabilità e della cooperazione applicativa in forza dei quali dovrà procedersi non soltanto all'aggiornamento tecnologico ed all'acquisizione delle *digital skills* necessarie al personale in servizio, ma occorrerà altresì promuovere un'effettiva standardizzazione delle procedure, così come del resto prescritto dall'art. 41, c. 1, del CAD come modificato dalla novella del 2016. Occorrerà, dunque, elaborare dei moduli uniformi per la presentazione delle istanze da parte dei soggetti privati e delle imprese, omogeneizzare l'impostazione dei siti *web* istituzionali, procedere all'utilizzo del c.d. fascicolo elettronico, privilegiare le comunicazioni in via telematica (art. 15 del CAD)[11].
Come osservato in precedenza, questo processo di standardizzazione (irrinunciabile ove si intenda effettivamente promuovere la piena realizzazione degli obiettivi di *e-government*) determina una compressione degli spazi di autonomia organizzativa propria delle singole pubbliche amministrazioni che, giocoforza, dovranno "beneficiare" di un incisivo *imprinting* dall'alto affidato al livello di governo centrale, il che non rimarrà senza conseguenze sull'inquadramento dei rapporti fra i diversi livelli di governo territoriale.

4. Le incognite del processo di digitalizzazione

Se non può che condividersi l'impegno profuso dal legislatore e dal Governo rispetto alle strategie di *e-government* e al più generale processo di digitalizzazione dell'amministrazione pubblica, occorre porre attenzione alle difficoltà applicative che una disciplina così articolata può incontrare nel contesto reale dell'attività istituzionale delle autorità pubbliche, connotato da forti squilibri, risorse insufficienti, complessità burocratiche ed – in molti casi – anche grande arretratezza infrastrutturale e tecnologica.
La prima difficoltà è certamente legata al c.d. *digital divide*, il divario digitale che nella popolazione si registra fra coloro che conoscono ed utilizzano efficacemente gli strumenti informatici e coloro che ne restano tagliati fuori per le ragioni più diverse.
Su questo aspetto influisce senza dubbio un dato anagrafico della popolazione italiana che, per oltre il 50% è rappresentata da persone con un'età compresa fra 35 e 100 anni[12], formatasi dunque in un'epoca in cui l'accesso alla tecnologia non era diffuso come lo è oggi; ma soprattutto, pesa notevolmente sulle competenze digitali dell'italiano medio il dato che meno del 60% della popolazione ha conseguito un titolo di studio superiore alla licenza di scuola media[13] nonché la circostanza che i programmi

[11] G. Duni, *L'Amministrazione digitale*, Milano, 2008.

[12] Fonte Istat, 2017 (www.tuttitalia.it/statistiche/popolazione-eta-sesso-stato-civile-2017)

[13] Fonte Istat, 2014 (www.istat.it/it/files/2014/10/ItaliaInCifre2014.pdf)

di studio ministeriali delle scuole dell'obbligo prevedono una formazione sulle materie informatiche assolutamente inadeguata rispetto al progresso nel settore delle ICT registrato nell'ultimo ventennio.

Questi dati, che di per se stessi destano preoccupazione in quanto evidenziano un *gap* culturale difficilmente colmabile in tempi brevi (quali sono quelli cui ambirebbero le politiche di *e-government* messe in campo dalle recenti riforme), risultano addirittura allarmanti se messi a paragone dei dati analoghi di altri Paesi UE (dati Eurostat, 2017[14]) nei quali, probabilmente, politiche più illuminate di riforma dell'istruzione scolastica di base hanno favorito una rapida diffusione delle competenze necessarie per una effettiva digitalizzazione della vita pubblica.

Al fine di comprendere quanto possa incidere il *digital divide* nella realizzazione di politiche di *e-government*, appaiono eloquenti i dati riguardanti il *Digital Economy and Society Index* (DESI) reperibili sul sito *web* della Commissione Europea, aggiornati al 2017: l'Italia occupa la quart'ultima posizione (seguita da Grecia, Bulgaria e Romania) della graduatoria dei paesi europei basata sul tasso di crescita digitale; dall'analisi degli studi effettuati si evince che solo il 56% della popolazione residente in Italia dichiara di utilizzare internet (a fronte di una media europea del 72%) e che il 34% degli italiani dichiara di non avere mai utilizzato internet (a fronte di un dato medio europeo del 21%)[15].

Il CAD, invero, pone fra gli obblighi a carico delle amministrazioni la promozione di «iniziative volte a favorire la diffusione della cultura digitale fra i cittadini con particolare riguardo ai minori ed alle categorie a rischio di esclusione» (art. 8 del CAD); tuttavia, non pare che da questa previsione, ad oggi, siano derivate concrete azioni rivolte a questo fine[16].

Il tema è particolarmente delicato in quanto le pubbliche amministrazioni sono chiamate a ricercare un ottimale equilibrio fra la massimizzazione della digitalizzazione e la tutela degli interessi di tutti, ivi compresi coloro i quali a causa del *gap* sopra indicato non sono in grado di interagire telematicamente con l'autorità pubblica. Occorre cioè evitare che la promozione di politiche di *e-government* (dichiaratamente ispirate alla massima partecipazione del cittadino alla vita pubblica) finiscano paradossalmente per escludere ambiti più o meno ampi di popolazione a causa del *digital divide*. Se poi si considera che le categorie di popolazione maggiormente esposte ad una "marginalizzazione" sono le categorie deboli per eccellenza (persone indigenti, immigrati, anziani, disabili, analfabeti funzionali[17]) il rischio concreto è che i valori cui l'*e-government* si ispira

[14] www.ec.europa.eu/eurostat/statistics.

[15] www.ec.europa.eu/digital-single-market/en/desi.

[16] Si segnalano alcuni meritevoli progetti, avviati come attività integrative e sperimentali, che tuttavia mantengono ancora un carattere episodico e pionieristico; fra gli interventi più significativi si annoverano i progetti «*Programma il Futuro*» (www.programmailfuturo.it/progetto) e "*ForTic*" (www.archivio.pubblica.istruzione.it/innovazione/progetti/tic.shtml)

[17] Analfabeta funzionale, secondo un recente studio OCSE (*Further Results from the Survey of Adult Skills*, 2016), è colui che, pur sapendo leggere e scrivere, non è in grado di usare queste capacità nella vita quotidiana e che spesso non comprende i linguaggi delle nuove tecnologie. Con il 28% di analfabeti funzionali, l'Italia si colloca al penultimo posto in Europa, insieme alla Spagna, e al quartultimo nel mondo, rispetto ai 33 paesi analizzati (www.www.oecd.org/skills/skills-matter-9789264258051-en.htm).

siano clamorosamente traditi.

Sotto altro profilo, l'azione di promozione della digitalizzazione della pubblica amministrazione pone rilevanti problemi in termini di sicurezza dei dati raccolti, gestiti e custoditi dall'amministrazione.

L'ingente mole di dati che tutte le amministrazioni in tempi brevi saranno chiamate a raccogliere determinerà il necessario ricorso a sistemi tecnologici molto avanzati di cui molto difficilmente le amministrazioni dispongono, trovandosi così costrette ad esternalizzare il servizio di custodia dei dati affidandolo a società che professionalmente erogano questi servizi (c.d. *cloud computing*) nei confronti di numerosi enti pubblici e privati[18].

I dati custoditi, per l'amministrazione, dalle società di *cloud computing* saranno accumulati su *server* localizzati certamente fuori dalle sedi dell'amministrazione, con ogni probabilità collocati in altri paesi anche molto lontani. Tuttavia, la circostanza che i suddetti dati siano di rilevanza pubblicistica (in quanto comunicati nell'ambito di un procedimento amministrativo) pone non pochi dubbi in ordine ai margini di controllo che l'amministrazione potrà esercitare e, dunque, sulle garanzie di tutela rese agli utenti finali.

Tali considerazioni dovranno indurre le amministrazioni a particolari cautele nell'affidare il servizio di *cloud computing* all'esterno prevedendo rigidi protocolli di monitoraggio sull'attività svolta dal *provider* incaricato della custodia dei dati.

In quest'ottica, dunque, le amministrazioni saranno chiamate a dotarsi di personale interno adeguatamente formato (con competenze ad un tempo giuridiche e informatiche) che possa essere in grado di supportare l'attività, erogata da terzi, di protezione dei dati acquisiti. Anche da questo punto di vista il nostro Paese versa in una condizione non facile tenuto conto che l'età media dei dipendenti pubblici italiani è la più alta dei paesi OCSE[19], il che chiaramente incide sulle relative abilità informatiche possedute.

Vi è, infine, un'ultima incognita, legata in particolare agli aspetti propri dell'*Open Government*, che concerne l'effettiva idoneità della trasformazione digitale del rapporto istituzione-cittadino a coinvolgere il complesso degli interessi in gioco, consentendo dunque la più opportuna valutazione da parte delle pubbliche amministrazioni. Com'è noto è sempre più frequente il ricorso, da parte delle istituzioni, agli strumenti di *soft law* che poggiano le proprie basi su diversificate forme di consultazione pubblica in via telematica.

Tale processo implementa effettivamente gli obiettivi propri della c.d. democrazia partecipata?

L'interrogativo – a parere di chi scrive – è di particolare interesse poiché il ruolo pre-

[18] Sul tema V. Berlingò, *Il fenomeno della datafication e la sua giuridicizzazione*, in *Riv. trim. dir. pubbl.*, 2017, 641 ss.; M. Falcone, *Big data e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, ivi, 601 ss.; S. Lavertu, *Big Data and the mismeasure of public administration*, in *Public Administration Review*, 2016; N. Rogge – T. Agasisti – K. De Witte, *Big Data and the measurement of public organizations' performance and efficiency*, in *Public Policy and Administration*, 2017.

[19] L'Italia ha il più basso tasso percentuale di dipendenti sotto i 35 anni (2% contro il 18% media OCSE) e la più alta percentuale di dipendenti sopra i 54 anni (45% contro il 22% media OCSE). Cfr. OECD, *Government at a Glance*, 2017 (www.oecd-ilibrary.org/governance/government-at-a-glance-2017_gov_glance-2017-en).

valente in queste fasi di consultazione è affidato ai c.d. *stakeholders* che, sempre più spesso, sono rappresentati da grandi gruppi economici che fanno capo a società di *lobbying* capaci di raccogliere, leggere ed elaborare i dati resi "aperti" dall'amministrazione. Anche in questo caso, dunque, il rischio concreto – maggiormente avvertito in Paese come il nostro in cui si registrano disfunzioni e *gap* quali quelli sopra evidenziati – è che possano farne le spese quote di interessi pubblici (parimenti rilevanti) che non trovano espressione attraverso i rappresentanti delle diverse categorie.
A ciò si aggiunga che, nonostante non siano mancate iniziative a livello parlamentare, l'attività di *lobbying* in Italia sfugge ad una normazione di rango primario che possa assicurarne un esercizio legittimo, equo e sempre coerente con i valori costituzionali della rappresentatività ed uguaglianza.
Il quadro sopra tratteggiato, in conclusione, induce a guardare con una certa perplessità alle riforme di *e-government* "tanto al chilo" che non tengono in adeguato conto delle peculiarità del contesto territoriale, culturale e socio-economico nel quale vanno ad incidere.

5. La digitalizzazione della funzione giurisdizionale

Nell'ambito più generale del processo di digitalizzazione delle funzioni istituzionali dello Stato rientra il tema ampio del processo telematico, in particolare del Processo Amministrativo Telematico (PAT), anch'esso recentemente interessato da alcuni interventi riformatori di cui è utile dare conto per cogliere il senso complessivo del percorso di riforma in atto[20].
La digitalizzazione del PAT è stata avviata con la l. 18 giugno 2009, n. 69 che, all'art. 44, affidava al Governo la delega per il riassetto complessivo della giustizia amministrava prevedendo anche che esso contemplasse l'introduzione di «procedure informatiche e telematiche».
In attuazione della delega è stato introdotto il comunemente noto Codice del Processo Amministrativo (d.lgs. 2 luglio 2010, n. 104) che, in realtà, contiene solo poche ed isolate norme dedicate al PAT, rinviando ad una successiva regolamentazione da emanarsi a livello governativo[21].
Con d.p.c.m. 16 febbraio 2016, n. 40 è stato adottato il Regolamento recante le norme tecnico-operative per l'attuazione del PAT. L'avvio del PAT, originariamente fissato per il 1° luglio 2016, è stato posticipato al 1° gennaio 2017 al fine di procedere ad una preliminare sperimentazione. Infine, con decorrenza dal 1° gennaio 2018 il PAT è stato esteso a tutti i ricorsi, ivi compresi quelli depositati prima del 2017.
Si segnala, inoltre, che il d.lgs. 179/2016 (attuativo della Riforma Madia) ha introdotto un'importante modifica al testo dell'art. 2, c. 6, del CAD prevedendo espressamente l'applicazione delle sue norme al processo civile, penale, amministrativo, contabile e

[20] C. Giurdanella – E. Guarnaccia, *Il processo amministrativo telematico (PAT)*, Rimini, 2017.

[21] In particolare l'art. 13 dell'Allegato 2 (*Norme di attuazione*) reca norme sul processo telematico; gli artt. 39 e 136 dell'Allegato 1 (*Codice del processo amministrativo*) pongono norme in materia di comunicazioni, depositi informatici e firma digitale.

tributario in quanto compatibile e se non diversamente disposto. Si tratta di un'innovazione rilevante poiché, in passato, le disposizioni del CAD trovavano applicazione soltanto alla pubblica amministrazione in senso stretto costituendo, rispetto all'attività giurisdizionale, dei meri valori di principio.

Si ritiene, peraltro, che gli effetti prodotti dall'implementazione delle ICT nel processo giurisdizionale siano ben diversi da quelli che essa produce sull'attività di amministrazione attiva; e ciò per una serie di vincoli, la maggior parte dei quali di matrice costituzionale, che ostacolano un cambiamento strutturale e radicale del processo; oltre che in ragione della tendenziale sovranità che ciascuno Stato mantiene sulla disciplina in materia processuale, il che rende pressochè impermeabile il sistema processuale agli *input* che possono provenire dalle norme europee ed internazionali.

In altri termini, come si è avuto modo di osservare nelle precedenti pagine, l'applicazione delle nuove tecnologie al settore dell'azione esecutiva delle pubbliche amministrazioni (attraverso la diffusione dei diversi modelli di *e-government*) ha determinato o comunque determinerà delle profonde modifiche alla struttura stressa dell'attività pubblica che – in breve tempo – sfuggirà ai canoni tradizionali riguardanti, per un verso, l'organizzazione degli uffici e, per altro verso, le modalità di esercizio del potere. Lo stesso non può dirsi per quanto riguarda la funzione giurisdizionale rispetto alla quale l'applicazione di modelli digitalizzati di gestione comporterà il (mero) effetto di automazione delle procedure e degli adempimenti processuali (il deposito degli atti difensivi, la firma dei provvedimenti giudiziali, ecc.) senza intaccare lo svolgimento delle udienze, le modalità di esercizio del contraddittorio fra le parti, la maturazione delle decisioni da parte dei giudici (in composizione collegiale o monocratica)[22].

Ciononostante, l'impatto della suddetta automazione non è da sottovalutare tenuto conto degli endemici problemi di eccessiva durata che affliggono il sistema processuale italiano.

Più recentemente, con d.l. 31 agosto 2016 n. 168, conv. in l. 25 ottobre 2015 n. 197, il legislatore ha introdotto alcune modifiche al c.p.a. e soprattutto alle norme di cui all'all. 2 del d.lgs. 104/2010 concernenti il PAT. In particolare, l'art. 7 , c. 1 lett. *a)* del d.l. 168/2016 ha introdotto fra le norme di attuazione del testo codicistico una nuova disposizione (l'art. 13 *bis*) che denota un deciso impegno del legislatore affinché la digitalizzazione della funzione giurisdizionale si compia senza ulteriori indugi ed ostacoli applicativi; l'art. 13 stabilisce per il triennio 2017-2020 che ciascun Tribunale Amministrativo Regionale «se rileva che il punto di diritto sottoposto al suo esame e vertente sull'interpretazione e sull'applicazione delle norme in tema di processo amministrativo telematico ha già dato luogo a significativi contrasti giurisprudenziali […] tali da incidere in modo rilevante sul diritto di difesa di una parte, con ordinanza emanata su richiesta di parte o d'ufficio e pubblicata in udienza, può sottoporre al presidente del Consiglio di Stato istanza di rimessione del ricorso all'esame dell'adunanza plenaria, contestualmente rinviando la trattazione del giudizio alla prima udienza successiva al sessantesimo giorno dall'udienza in cui è pubblicata l'ordinanza. Il presidente del Consiglio di Stato comunica l'accoglimento della richiesta entro trenta giorni dal ricevi-

[22] Sull'argomento, M. L. Maddalena, *La digitalizzazione della vita dell'amministrazione e del processo*, in *Foro amm.*, 2016, 2535 ss.; spec. 2583.

mento, e in tal caso nell'udienza davanti al tribunale il processo è sospeso fino all'esito della decisione dell'adunanza plenaria. La mancata risposta del presidente del Consiglio di Stato entro trenta giorni dal ricevimento della richiesta equivale a rigetto. L'adunanza plenaria […] decide la sola questione di diritto relativa al processo amministrativo telematico».

L'art. 7 del d.l. 168/2016, infine, definisce alcune questioni applicative, quale ad esempio quella concernente la rilevanza delle comunicazioni effettuate ai difensori presso il domicilio digitale (che dal 1° gennaio 2018 sostituiscono del tutto quelle presso il domicilio tradizionale).

Seppur atteggiandosi in modo differente rispetto a quanto occorso nell'ambito dell'organizzazione dell'attività di amministrazione attiva, la digitalizzazione della funzione giurisdizionale – a pieno regime dal 2018 – rappresenterà comunque un cambiamento significativo del modo di svolgersi del rapporto giuridico processuale. Peraltro, molte delle incognite evidenziate con riguardo al modello di *e-government*, legate prevalentemente all'oggettiva inadeguatezza delle abilità informatiche del cittadino medio, non dovrebbero configurarsi in ambito giurisdizionale considerato che il rapporto fra l'utente del servizio giustizia e i magistrati che lo erogano è mediato attraverso il ruolo professionale del difensore, dotato delle competenze necessarie.

Informazione e comunicazione digitale nel processo di modernizzazione della pubblica amministrazione*

Anna Lazzaro

Abstract

Il percorso legislativo nazionale in materia di sviluppo del digitale nelle amministrazioni pubbliche si è sviluppato sulla spinta dell'ordinamento europeo.
Le istituzioni comunitarie hanno inteso favorire la realizzazione di una società della informazione e delle comunicazioni che si estendesse agli stati membri con l'impiego delle tecnologie, in continuo sviluppo, attraverso una serie di direttive e piani di azione che hanno reso gli interventi di adeguamento frammentati e disorganici.
Solo con il Regolamento e-IDAS del 2014, entrato in vigore nei paesi membri nel 2016, si è avviata una riforma europea più organica e che ha inciso direttamente sugli ordinamenti nazionali. Di conseguenza, gli obiettivi nazionali sono stati perseguiti con interventi che, inseriti in una politica generale europea, hanno comportato continue modifiche e aggiustamenti per la peculiarità della materia.
Il quadro attuale del nostro ordinamento diretto a modernizzare la pubblica amministrazione sotto il profilo tecnologico, pur con la recente introduzione del d. lgs. 179/2016, denota ancora un certo ritardo nell'adeguamento alle politiche di e-Europe per oggettive difficoltà, ma anche per la poca propensione ai cambiamenti sia da parte dei pubblici poteri sia della stessa società.
La creazione di una piena interazione digitale tra amministrazione e cittadini presuppone una volontà di apertura istituzionale alla società e una volontà di aprirsi alle tecnologie e a vederle come sviluppo positivo della società.

The digital national regulation development has been triggered by the European regulation. Indeed, the Community institutions aimed to promote an information and communication society. These objectives would be implemented in Member states by European directives and action plans. However, the Community institutions interventions had been fragmented and confused.
The EU eIDAS Regulation (the "Regulation") entered into force in 2016. This Regulation was key for the development of a unique framework on digital market within the territory of Member States. Indeed, not only the Regulation was directly applicable on the nation soil but also this affected directly national regulation in this respect.
National goals in digital market have been pursued throughout modifications in the National regulation landscape.
As of today, National law aims to modernize public authorities through the digitization of their services. Despite the new regulation 179/2016, modernization of public authorities is still delayed. The delay has been triggered by a difficulty of implement the e-Europe and by a lack of willpower of public authorities and society in this respect.
Digital interaction of the public authorities with the citizen requires, on one hand, the

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio anonimo, in quanto riproduce la relazione presentata dall'A. al convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno" (Messina, 26-27 maggio 2017).

willingness of the public authorities to open up to digitization, and on the other hand, the acceptance of the digitalization as a positive development for the society.

Sommario

1. L'informazione e la comunicazione delle amministrazioni ai cittadini. - 2. L'informazione amministrativa - 3. Il Codice dell'amministrazione digitale - 4. L'amministrazione digitale nella recente riforma. - 5. Principi comunitari e disciplina nazionale. - 6. Amministrazione digitale e società dell'informazione: considerazioni conclusive.

Keywords: Codice dell'Amministrazione digitale (CAD), informazione, comunicazione, nuove tecnologie, ordinamento europeo

1. L'informazione e la comunicazione delle amministrazioni ai cittadini

L'apertura delle informazioni ai cittadini, gli obblighi di comunicazione imposti alle amministrazioni al fine di rendere partecipi i privati e il processo di modernizzazione dei servizi amministrativi, che diventano accessibili facilmente e conoscibili attraverso il web, costituiscono condizioni di rinnovamento delle pubbliche amministrazioni.
L'informazione e la comunicazione sono concetti connaturati all'idea di un'amministrazione democratica in quanto partecipata e accessibile, e configurano ormai una vera e propria funzione delle amministrazioni, cui è correlato un diritto dei cittadini ad essere adeguatamente informati[1] e messi nelle condizioni di conoscere l'operato delle amministrazioni pubbliche.
Già nella disciplina del procedimento amministrativo[2], attraverso gli istituti di partecipazione e di accesso ai documenti, si delinea la posizione rilevante di coloro che hanno interesse al procedimento, attraverso il riconoscimento di determinati obblighi delle amministrazioni. Non si tratta di diffusione di informazioni generalizzata, ma di obblighi di comunicazione e informazione diretta ai soggetti specificamente interessati e individuati dalla legge, titolari non di un diritto ma di un interesse rilevante a conoscere tali comunicazioni e informazioni.
Tuttavia, la nascita della comunicazione pubblica è da considerare uno degli eventi più importanti del processo di cambiamento che ha interessato la pubblica amministrazione e la disciplina che per la prima volta nel panorama nazionale si occupa della comu-

[1] F. Manganaro - A. Romano Tassone (a cura di), *I nuovi diritti di cittadinanza: il diritto all'informazione*, Torino, 2005.

[2] Già allora certamente le scelte legislative avrebbero potuto essere più coraggiose in tema di informazioni ai cittadini, si ricorda, ad esempio, quanto auspicava la Commissione Nigro in relazione alla previsione di una fase istruttoria del procedimento aperta al pubblico.

nicazione ha avuto una portata sistemica, nonostante alcuni limiti evidenti[3].
La sua rilevanza attiene anche al fatto che l'introduzione di un nuovo modello organizzativo che tiene conto degli obblighi di informazione e comunicazione ai soggetti privati dell'operato amministrativo, irradia i suoi effetti su molte discipline, cioè su tutte le procedure che le pubbliche amministrazioni sono tenute a porre in essere e a cui sono obbligate a conformarsi.
Il cambiamento del modello organizzativo della pubblica amministrazione diventa inevitabile, tenuto conto della crescita democratica del cittadino nei confronti dei pubblici poteri, ma anche del contemporaneo sviluppo dei mezzi di comunicazione digitale.
Inoltre, anche nell'ambito del settore produttivo, il mutamento del ruolo delle amministrazioni risulta sempre più rilevante spingendo verso il cambiamento. I concetti di efficienza e di efficacia diventano, infatti, i criteri portanti dell'attività pubblica, che deve in questo modo soddisfare due imprescindibili esigenze: la compatibilità tra costi e benefici, da un lato, l'effettività e, quindi, l'effettiva realizzazione dei risultati perseguiti, dall'altro.
Risulta anche evidente l'importanza che ha avuto in questa direzione la normativa europea che, a partire dagli inizi degli anni settanta, ci ha abituati a considerare la pubblica amministrazione come un fondamentale protagonista dell'attività produttiva, in grado di condizionare lo sviluppo complessivo del paese in senso positivo o negativo, a seconda, cioè, che il suo operato agevoli, ovvero ostacoli la crescita del sistema.
Tali mutamenti, sia all'interno delle istituzioni, sia nel sociale, si accompagnano alla sempre più diffusa pervasività dell'azione amministrativa, volta a perseguire l'effettiva realizzazione dei valori collettivi, dalla salute alla privacy, dalla tutela dell'ambiente a quella del territorio, intesa l'espressione nelle sue varie accezioni (storico artistiche, paesaggistiche, ecc.), oltre ad altri valori emergenti di portata generale, collegati all'elevazione dei livelli del benessere, sia individuale, che collettivo.
Qualsiasi attività privata che risulti avere rilevanza sociale, finisce col rientrare nell'orbita, sia pure occasionale, di qualche pubblica autorità. La maggioranza delle azioni individuali finisce o direttamente o in via indiretta con l'interferire con gli interessi dei terzi.
Se questo è il modello di amministrazione che si è andato delineando e che tende sempre più a diffondersi, riesce facile constatare che il momento della comunicazione diventa uno degli aspetti fondamentali del suo nuovo modo di essere. Al pari di qualsiasi impresa che offre servizi, la pubblica amministrazione è tenuta a far conoscere alla collettività le opportunità che ciascuno di noi è in grado di ricevere, attraverso una corretta utilizzazione di ciò che rientra tra i suoi compiti istituzionali. L'impiego delle risorse pubbliche risulta in questo modo ottimizzato anche, ed in particolar modo, attraverso l'attività di comunicazione, proprio perché è questo il veicolo in grado di creare un corretto rapporto con l'utenza, con il fruitore finale, sia dei beni prodotti, che dei servizi prestati.

[3] Ci riferiamo alla l. 150/2000. Cfr. P. Marsocci, *Informazione e comunicazione istituzionale: la legge n. 150 del 2000 come un nuovo passo della riforma amministrativa*, in *Giurisprudenza di merito*, 2000, 1133 ss.; F. Merloni (a cura di), *L'informazione nelle pubbliche amministrazioni*, Rimini, 2002.

2. L'informazione amministrativa

Quando si parla di informazione amministrativa[4] è possibile distinguere l'informazione diretta ad informare determinati soggetti in ragione di un loro specifico interesse, ad esempio, in relazione ad un determinato procedimento, l'informazione che, più in generale, riguarda la collettività e che è relativa alle attività delle amministrazioni o che riguarda temi di interesse generale, e la comunicazione[5] riconducibile a quelle attività provenienti dalle amministrazioni e che vanno diffuse, con lo scambio di conoscenze con la collettività[6].

Attraverso le tre diverse tipologie, l'informazione amministrativa produce il risultato di ampliare i diritti dei cittadini, e crea uno scambio di conoscenze che determina anche una nuova forma di responsabilizzazione delle amministrazioni, obbligate a farsi conoscere.

L'esistenza di un collegamento tra il diritto ad ottenere informazioni individuali tramite il diritto di accesso e le forme di informazione generale, fu inquadrato nell'ambito di un comune "diritto alla conoscenza" all'inizio degli anni ottanta, ed entrambe le tipologie vennero comprese in quello che fu definita la "terza generazione dei diritti dell'uomo"[7].

La disciplina sull'informazione amministrativa costituisce un momento del percorso ampliativo delle forme di diffusione delle conoscenze nei confronti della generalità dei cittadini. Si comincia a prendere coscienza dell'importanza del collegamento tra documentazione amministrativa e informazione, in quanto perché si possa esercitare il diritto all'informazione, occorre che nei compiti dell'amministrazione rientri quello di ordine e coordinamento dei propri documenti e delle informazioni disponibili, affinché il privato possa essere in grado di individuare i dati e i documenti cui accedere e le informazioni da richiedere.

La l. 150/2000[8] disciplina, seppure con una certa vaghezza, una precisa funzione amministrativa che viene svolta, soprattutto, attraverso operazioni materiali, come quelle relative alla gestione dei siti Internet e alla elaborazione di messaggi pubblicitari.

Le finalità indicate all'art. 1 sono dirette a favorire la conoscenza delle disposizioni normative, illustrare l'attività delle amministrazioni, favorire l'accesso ai servizi pubblici, promuovere conoscenze su temi di rilevante interesse pubblico, favorire la semplifica-

[4] A. Meloncelli, *L'informazione amministrativa*, Rimini, 1993, 51: la cui nozione di informazione amministrativa è «dichiarazione di conoscenza oggetto di una misura trasmissiva, dichiarazione e misura sono generalmente procedimentalizzate».

[5] G. Arena (a cura di), *La funzione di comunicazione nelle pubbliche amministrazioni*, Rimini, 2001; M. De Benedetto, *Comunicazione pubblica*, in *Enciclopedia Giuridica Treccani*, Roma, 2001, 5 ss.

[6] B.G. Mattarella, *L'informazione amministrativa: profili generali*, in F. Manganaro - A. Romano Tassone (a cura di), *op. cit.*, 5; l'A. fa riferimento ad una micro-informazione, accesso individuale, e ad una macro-informazione, informazione su temi di interesse generale.

[7] G. Braibant, *Droit d'accès et droit à l'information*, in *Mélanges Charlier*, Paris, 1981.

[8] P. Marsocci, *op. cit.,* 1133.

zione e la trasparenza amministrativa, promuovere l'immagine delle amministrazioni[9].
La legge sembra, per la verità, preoccuparsi più di un assetto organizzativo dell'informazione, anziché di altri problemi, come quello della corretta informazione, dell'affidamento dei cittadini, o quello dei limiti entro i quali le informazioni fornite dalle amministrazioni le vincolino, o i problemi della tutela della riservatezza.
Infatti la legge si preoccupa soprattutto di aspetti organizzativi e dei compiti delle amministrazioni; vengono istituti l' Ufficio per le relazioni con il pubblico, la cui attività è indirizzata ai cittadini singoli ed associati (art. 8), gli Uffici stampa, la cui attività è indirizzata in via prioritaria ai mezzi di informazione di massa (art. 9), e sono introdotte le norme sul portavoce che può coadiuvare l'organo di vertice dell'amministrazione pubblica «ai fini dei rapporti di carattere politico-istituzionale con gli organi di informazione» (art. 7).
La funzione di informare proviene da determinati uffici a ciò preposti, come gli uffici stampa, i portavoce, secondo regole e criteri specifici come quelle contenute in documenti relativi alle modalità di comunicazione pubblica[10]. Si tratta di uffici che coadiuvano gli organi di indirizzo politico e sono disciplinati dalla legge come uffici di diretta collaborazione, che operano a stretto contatto con il vertice politico.
Per quanto non si possa affermare che attraverso questa disciplina si siano compiutamente affrontati i problemi connessi alla comunicazione pubblica, si comincia, comunque, ad affermare il diritto alle informazioni da parte dei cittadini, in correlazione con le posizioni delle amministrazioni di dover mettere i privati nella condizione di conoscere i modi di svolgimento delle loro attività.
La disciplina prevista dalla l. 150/2000 si ispira ai principi di pubblicità e trasparenza, relativamente alle informazioni e comunicazioni delle amministrazioni a beneficio, non solo di chi fosse direttamente coinvolto o interessato a specifici procedimenti, come avveniva nella disciplina sul procedimento, ma più in generale nei confronti di tutti i soggetti dell'ordinamento, anche al fine di consentire «conoscenze allargate e approfondite su temi di rilevante interesse pubblico e sociale» (art. 1) e promuovere la conoscenza dei servizi pubblici, in modo da favorirne l'accesso, nonché delle disposizioni normative, per facilitarne l'applicazione, confermando il ruolo di servizio assegnato alla pubblica amministrazione.
La l. 150/2000 costituisce un momento importante di un processo riformatore della pubblica amministrazione, ma lascia alla piena disponibilità delle amministrazioni la funzione di informazione, in quanto non pone obblighi per le amministrazioni e non dà strumenti ai cittadini per pretendere le informazioni.

[9] Sulle leggi in materia di informazione pubblica in altri paesi si veda: G. Palombelli, *Le informazioni pubbliche come risorsa. Profili comparati*, in F. Merloni (a cura di), *op. cit.*

[10] Dipartimento della funzione pubblica, *Manuale di stile. Strumenti per semplificare il linguaggio delle amministrazioni pubbliche,* a cura di di A. Fioritto, Bologna, 1997.

3. Il Codice dell'amministrazione digitale

Nell'ottica dello sviluppo di forme di realizzazione della trasparenza, un profilo fondamentale è costituito dall'implementazione dell'amministrazione digitale, processo che evolve in ragione del continuo sviluppo tecnologico, e che costituisce lo strumento attraverso il quale è possibile rendere conoscibile l'operato delle amministrazioni in modo immediato e attraverso un facile accesso. I processi di sviluppo della tecnologia informatica e quello di riforma delle amministrazioni che impone forme maggiori di trasparenza sono strettamente correlati.
Il d.lgs. 82/2005 (Codice dell'amministrazione digitale) già stabiliva che «le pubbliche amministrazioni nell'organizzare la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi della trasparenza».
Il Codice dell'amministrazione digitale del 2005, rappresenta una tappa importante per il processo di rinnovamento della pubblica amministrazione[11].
Con tale disciplina si avvia un processo diretto alla realizzazione di un sistema amministrativo più moderno, digitale e meno burocratizzato. Il Codice introduce un insieme di innovazioni normative che vanno ad incidere concretamente sui comportamenti e sulle prassi delle amministrazioni e sulla qualità dei servizi resi.
Il Codice dell'amministrazione digitale (CAD), si basa sul principio di effettività, in quanto si introducono misure premiali e sanzionatorie favorendo, da una parte, le amministrazioni virtuose (anche con la possibilità di quantificare e riutilizzare i risparmi ottenuti grazie alle tecnologie digitali) e sanzionando, dall'altra, le amministrazioni inadempienti; e si intende affermare l'innovazione della pubblica amministrazione, attraverso forme di incentivo alla razionalizzazione dell' organizzazione e all'informatizzazione dei procedimenti; in tal modo, le pubbliche amministrazioni ricaveranno dei risparmi che potranno utilizzare per il finanziamento di progetti di innovazione e per l'incentivazione del personale in essi coinvolto.
In particolare, si vuole fare in modo che i cittadini possano colloquiare attraverso computer e Internet con tutte le amministrazioni locali e centrali[12].
Infatti, sono state introdotte misure dirette all'utilizzo, da parte delle amministrazioni, di sistemi di comunicazione con i cittadini tramite la PEC o altre soluzioni tecnologiche equivalenti, per tutte le comunicazioni che richiedono una ricevuta di ritorno ai soggetti che preventivamente hanno dichiarato il proprio indirizzo elettronico; vengono individuati uffici responsabili dell'attività ICT; sono previsti obblighi di pubblicazione da parte delle amministrazioni centrali sui propri siti istituzionali (bandi di concorso); vengono emanate regole tecniche che possano consentire di dare piena validità alle copie cartacee e, soprattutto, a quelle digitali dei documenti informatici,

[11] Il d. lgs. 82/2005 è stato aggiornato dal d. lgs. 159/2006, e dal d. lgs. 235/2010; E. Carloni (a cura di), *Codice dell'amministrazione digitale. Commento al d. lgs. 7 marzo 2005, n. 82*, Rimini, 2005; Id., *La riforma del codice dell'amministrazione digitale*, in *Giornale di Diritto Amministrativo*, 2011, 469 ss.; F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità,* in *Diritto dell'informazione e dell'informatica*, 2, 2015, 227 ss.

[12] B. Ponti (a cura di), *Il regime dei dati pubblici. Esperienze europee e ordinamento nazionale*, Rimini, 2008, ed in particolare i contributi di P. Sucevic, P. Birkinshaw, M. Eifert, A. Cerrillo Martinez, ed E. Menichetti.

dando maggiore concretezza al processo di dematerializzazione dei documenti della pubblica amministrazione.
Le pubbliche amministrazioni in ragione della digitalizzazione dei documenti non potranno richiedere l'uso di moduli e formulari che non siano stati pubblicati sui propri siti istituzionali. Il cittadino fornirà, poi, una sola volta i propri dati all'amministrazione, in quanto sarà onere delle amministrazioni, comunque in possesso dei dati, assicurare l'accessibilità delle informazioni alle altre amministrazioni che lo richiedano.
Per evitare che il cittadino debba fornire più volte gli stessi dati, le amministrazioni titolari di banche dati predisporranno apposite convenzioni aperte, per assicurare l'accessibilità delle informazioni in proprio possesso, da parte delle altre amministrazioni.
Il d. lgs. 82/2005 è stato aggiornato, in ragione del progresso tecnologico, con il d. lgs. 159/2006 e successivamente con il d. lgs. 235/2010.
Le novità introducono un sistema di contrassegno generato elettronicamente e stampato direttamente dal cittadino dal proprio computer, per sancire la conformità dei documenti cartacei a quelli digitali, forniscono indicazioni sulla validità delle copie informatiche di documenti.
Viene prevista la gestione della conservazione dei documenti e del relativo processo da parte di un responsabile della conservazione; ogni responsabile della conservazione dei documenti può certificare il processo di digitalizzazione e di conservazione avvalendosi eventualmente di Conservatori accreditati, soggetti che ottengono da DigitPa il riconoscimento del possesso dei requisiti di sicurezza e affidabilità per effettuare il processo e la conservazione dei documenti informatici.
La PEC diventa il mezzo più veloce e sicuro per comunicare con le amministrazioni. I cittadini possono utilizzare la PEC anche come strumento di identificazione evitando l'uso della firma digitale e sono previsti strumenti di firma semplificati senza pregiudizio di sicurezza e attendibilità. Le istanze possono essere trasmesse da tutte le caselle di posta elettronica certificata rilasciate previa identificazione del titolare.
La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti (anche a fini statistici) tra imprese e pubblica amministrazione (e viceversa) avviene solo utilizzando tecnologie ICT.
Carte di identità elettronica e Carte nazionale dei servizi valgono ai fini dell'identificazione elettronica[13].

4. L'amministrazione digitale nella recente riforma

La l. 124/2015 ha delegato il governo ad emanare, tra gli altri decreti legislativi previsti nell'ambito di un'ampia riforma della pubblica amministrazione, il decreto legislativo di riforma del CAD a dimostrazione dell'esigenza di rafforzare i contenuti della discipli-

[13] Il CAD introduce alcuni strumenti (carte di credito, di debito o prepagate e ogni altro strumento di pagamento elettronico disponibile) per consentire alle pubbliche amministrazioni di riscuotere i pagamenti per via elettronica. Inoltre, permette loro di avvalersi di soggetti anche privati per la riscossione.

na, alla luce dei processi di modernizzazione e di sviluppo del diritto alle informazioni dei cittadini, e della rapidità di sviluppo delle tecnologie informatiche che impongono il continuo adeguamento normativo.

Il d.lgs. 26 agosto 2016, n. 179, recante "Modifiche e integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n.82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche"[14], prevede tra i suoi obiettivi quello di inserire le tecnologie dell'informazione e della comunicazione nei rapporti tra cittadini, imprese e pubbliche amministrazioni, tra gli strumenti per la promozione del processo di radicale riorganizzazione dell'amministrazione dello Stato, volendo attribuire rilievo e un ruolo centrale ai c.d. diritti di cittadinanza digitale (art. 1)[15].

La volontà è quella di spostare l'attenzione dal processo di digitalizzazione, ai diritti digitali di cittadini e imprese. Con la Carta della cittadinanza digitale si riconoscono direttamente diritti a cittadini e imprese, e si costituisce la base giuridica per implementare Italia Login, la piattaforma di accesso che, attraverso il Sistema pubblico d'identità digitale e l'Anagrafe nazionale della popolazione residente, permetterà ai cittadini di accedere ai servizi pubblici - e a quelli degli operatori privati che aderiranno - con un unico nome utente e un'unica *password* (prenotazioni di visite mediche, iscrizioni a scuola, pagamento dei tributi). Ciò permetterà di superare la complessità della situazione attuale per cui ogni pubblica amministrazione o ente pubblico che garantisce servizi *on-line,* richiede proprie modalità di registrazione e di utilizzo dei servizi.

Si tratta del sistema SPID (Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese) che assume un ruolo centrale in questo nuovo CAD e viene definito come un insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agid[16], secondo modalità definite con specifico decreto ministeriale, identificano cittadini, imprese e pubbliche amministrazioni per consentire loro l'accesso ai servizi in rete.

Lo SPID, quindi, è un insieme di credenziali per accedere in rete a tutti i servizi della pubblica amministrazione e a quelli degli operatori commerciali che vi aderiranno. Lo

[14] Pubblicato nella Gazzetta Ufficiale, Serie Generale n. 214 del 13 settembre 2016. Entrato in vigore il 14 settembre 2016.

[15] Secondo il nuovo decreto dal 31 dicembre del 2017 viene rivoluzionato il rapporto tra cittadini e amministrazioni pubbliche. I cittadini possono accedere ai servizi pubblici con un unico nome utente e un'unica password e possono avere un domicilio digitale con cui inviare e ricevere dalle pubbliche amministrazioni comunicazioni e documenti per via digitale.
Con la Carta della cittadinanza digitale ogni cittadino ha diritto all'identità digitale (Spid) e al domicilio digitale. Alla prima si accede con Pin unico e consente di utilizzare i servizi erogati in rete dalle pubbliche amministrazioni. Dal primo gennaio 2018 tutti i servizi online della pubblica amministrazione sono accessibili tramite Spid. Il domicilio digitale diventa l'indirizzo *on-line* con cui un cittadino può dialogare con le pubbliche amministrazioni. La moneta elettronica diventa il principale strumento di pagamento delle pubbliche amministrazioni. È eliminato l'obbligo di conservare ricevute di pagamento e bollette dei gestori dei servizi pubblici, mentre quando un ufficio pubblico non utilizza la banda la renderà disponibile ai cittadini attraverso il wi-fi. È previsto l'adeguamento del diritto interno alla nuova disciplina europea sui servizi fiduciari.

[16] Agenzia per l'Italia Digitale di cui all'art. 19 del d.l. 22 giugno 2012, n. 83, convertito, con modificazioni, dalla l. 7 agosto 2012, n. 134.

SPID consente agli utenti di avvalersi di gestori dell'identità digitale qualificati, per permettere ai fornitori di servizi l'immediata verifica della propria identità.
È chiaro, quindi, l'intento del legislatore di semplificare al massimo l'accesso ai servizi *online* dei cittadini, superando le difficoltà connesse alle carte elettroniche; ciò che può preoccupare è il pericolo "sicurezza" che incombe sempre, poiché è evidente che con tale sistema si moltiplicano le identità digitali di un cittadino, che saranno diverse per ogni servizio, e la prospettiva che ne deriva può determinare talune perplessità.
Infatti, non vi è dubbio che, per quanto necessari gli interventi di modernizzazione sotto il profilo tecnologico delle amministrazioni, non andrebbero trascurati ed eventualmente disciplinati gli aspetti relativi alle garanzie che riguardano la sicurezza dei sistemi informatici e quelli della facile diffusione di informazioni non sempre adeguatamente protette e garantite.
Il legislatore, sempre in linea di continuità con la disciplina precedente, introduce nelle definizioni di cui all'art. 1 del CAD nuove ed importanti definizioni e, in particolare, quella di identità digitale, da intendere come «rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dall'articolo 64» con chiaro rimando allo SPID; un'altra definizione riguarda il domicilio digitale, inteso come «l'indirizzo di posta elettronica certificata o l'indirizzo utilizzato da altro servizio qualificato di recapito certificato, utilizzato per le comunicazioni tra le persone fisiche e giuridiche e i soggetti di cui all'articolo 2, comma 2».
In effetti, da sempre si è sostenuto che la comunicazione del proprio indirizzo di PEC ad una pubblica amministrazione, rappresenta una vera e propria elezione di domicilio informatico e tale concetto, quindi, viene recepito a livello normativo con un'importante integrazione; difatti, si parla anche di «altro servizio qualificato di recapito certificato».

5. Principi comunitari e disciplina nazionale

La recente disciplina nazionale trae origine dal Regolamento (UE) e-IDAS n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari nel mercato interno, pubblicato nella G.U. dell'Unione Europea del 28 agosto 2014, che costituisce il più recente intervento in materia dell'Unione europea.
In effetti, l'opportunità della riforma dell'intero CAD nasce anche dalla necessità di adeguare lo stesso a questo importante regolamento comunitario noto con l'acronimo e-IDAS che sta per *electronic IDentification Authentication and Signature (ETS electronic Trust Services),* che stabilisce le condizioni per il riconoscimento reciproco in ambito di identificazione elettronica e prevede le regole comuni per le firme elettroniche, l'autentica-

zione web ed i relativi servizi fiduciari per le transazioni elettroniche[17].
I principi comunitari sono stati recepiti nel decreto di riforma del CAD ed un chiaro segnale in tal senso è rappresentato, innanzitutto, dall'adozione "in toto" di tutte le definizioni contenute nel Regolamento, con conseguente abrogazione di molte definizioni originarie del CAD.
Il Regolamento disciplina l'identificazione elettronica intesa come «il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o una persona fisica che rappresenta una persona giuridica», preoccupandosi del riconoscimento reciproco fra gli Stati membri dei mezzi di identificazione e autenticazione elettronica per accedere ad un servizio prestato da un organismo del settore pubblico *online* in uno Stato membro.
L'identificazione va distinta dalla c.d. "autenticazione" intesa come un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica.
Particolare attenzione viene rivolta ai prestatori di servizi fiduciari qualificati e non qualificati che devono rispettare determinati requisiti, assumono specifiche responsabilità in caso di danni causati con dolo o negligenza e sono sottoposti al controllo di organismi di vigilanza ed a specifiche verifiche da parte di organismi di valutazione della conformità.
Quanto alla disciplina delle firme elettroniche viene ribadito che tali modalità di firma hanno il medesimo effetto delle firme autografe e la medesima efficacia probatoria. Inoltre, trattandosi di firma elettronica qualificata viene riconosciuta in tutti gli Stati membri.
Il Regolamento introduce il concetto di sigillo elettronico da intendersi come «dati in forma elettronica acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi».
Il sigillo elettronico ha lo stesso valore giuridico e la medesima efficacia probatoria della firma elettronica, pertanto, una persona giuridica nell'ambito dei servizi pubblici potrà utilizzare il sigillo elettronico che ha la funzione di prova dell'emissione di un documento elettronico, garantendo al documento stesso la certezza dell'origine e l'integrità del contenuto, oppure utilizzandolo al fine di autenticare qualsiasi bene digitale della persona giuridica stessa, quali codici di software o server.
Altro concetto è quello della validazione temporale elettronica intesa dal Regolamento come «dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento».

[17] Il Regolamento è entrato in vigore direttamente in tutti gli Stati Membri UE, senza necessità di atti di recepimento, il 17 settembre 2014, anche se lo stesso si applica a decorrere dal 1° luglio 2016, ad eccezione delle disposizioni riportate nell'art. 52.
L'obiettivo fondamentale di questo provvedimento comunitario è quello dell'eliminazione delle barriere esistenti all'impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri almeno per l'autenticazione nei servizi pubblici. Il Regolamento, difatti, non intende intervenire riguardo ai sistemi di gestione dell'identità elettronica e relative infrastrutture istituiti negli Stati membri, ma intende garantire che per accedere ai servizi *online* transfrontalieri offerti dagli Stati membri, si possa disporre di un'identificazione e un'autenticazione elettronica sicura.

Sono poi previsti i servizi di recapito certificato che consentono la trasmissione di dati tra terzi per via elettronica e forniscono prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e proteggono i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate.
Il Regolamento introduce importanti innovazioni come l'obbligo per le amministrazioni ad accettare pagamenti attraverso servizi elettronici, la previsione del principio *Digital first* che ha indotto il nostro paese all'adozione del processo telematico, l'obbligo per i pubblici uffici di rendere disponibile la connessione ad Internet tramite wi-fi, il principio dell'*open data* che comporta il pieno accesso alle informazioni pubbliche.

6. Amministrazione digitale e società dell'informazione: considerazioni conclusive

Tutto il percorso legislativo nazionale in materia di sviluppo del digitale nelle amministrazioni pubbliche si è sviluppato sulla spinta dell'ordinamento europeo.
Le istituzioni comunitarie hanno inteso favorire la realizzazione di una società della informazione e delle comunicazioni che si estendesse agli stati membri con l'impiego delle tecnologie, in continuo sviluppo, attraverso una serie di direttive che hanno posto vincoli in materia di firma digitale (1999/93CE), di tutela della privacy (2002/58/CE)[18], di commercio elettronico (2000/31/CE), procedendo attraverso le linee guida ed eventualmente consentire azioni correttive in ragione della continua evoluzione del settore.
Le scelte europee di sviluppo dell'e-Europe incidono sulla vita socio politico economica dei cittadini attraverso la costruzione di modelli di amministrazione pubblica in grado di fornire un funzionale e ottimale accesso elettronico ai servizi pubblici sfruttando le potenzialità delle innovazioni tecnologiche.
Caratteristica del percorso di sviluppo a livello europeo è stata, forse inevitabilmente, considerata la continua evoluzione delle tecnologie innovative, una serie di interventi settoriali e frammentati introdotti nei paesi membri attraverso piani d'azione e direttive[19]. Solo con l'entrata in vigore del Regolamento e-IDAS del 2014 si è avviata una riforma europea più organica e che ha inciso direttamente sugli ordinamenti nazionali. Di conseguenza, gli obiettivi nazionali sono stati perseguiti con interventi[20] che, inseriti in una politica generale europea, hanno comportato continue modifiche e aggiustamenti per la peculiarità della materia.

[18] Recentemente si veda il Regolamento (UE) n. 2016/679 sulla protezione delle persone fisiche con riferimento alla tutela dei dati personali, cfr. S. Sica - V. D'Antonio - G. M. Riccio, *La nuova disciplina europea sulla privacy*, Padova, 2017; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016; L. Bistolfi - E. Pelino - C. Bolognini, *Il Regolamento Privacy europeo*, Milano, 2016; con riferimento alla situazione precedente al Regolamento cfr. G. Finocchiaro, *Privacy e tutela dei dati personali*, Bologna, 2012.

[19] C. Leone, *Il ruolo del dritto europeo nella costruzione dell'amministrazione digitale*, in *Rivista italiana di Diritto Pubblico Comunitario*, 2014, 867 ss.

[20] Nel nostro paese, oltre che nel CAD, sono previste disposizioni di adeguamento alle direttive europee in materia di digitalizzazione nel d.lgs. 5/2012, nel d.lgs. 83/2012, nel d.lgs. 179/2012 e nel d.lgs. 69/2013.

Va detto che il quadro attuale del nostro ordinamento denota ancora un certo ritardo nell'adeguamento alle politiche di e-Europe per le oggettive difficoltà, ma anche per la poca propensione ai cambiamenti sia da parte dei pubblici poteri sia della stessa società.

La creazione di una piena interazione digitale tra amministrazione e cittadini presuppone una volontà di apertura istituzionale alla società e dall'altra parte una volontà di aprirsi alle tecnologie e a vederle come sviluppo positivo della società. Altro fattore che incide negativamente sulla modernizzazione tecnologica, può essere considerata la poca fiducia nelle istituzioni che produce una evidente difficoltà per il cittadino di accedere con tranquillità alle informazioni e ai servizi telematici.

Qualche considerazione infine sulla imposizione di obblighi nel dialogo tra amministrazione e cittadini. Infatti, è possibile ritenere che l'uso obbligato delle tecnologie non significa solo modernità e progresso e, di conseguenza, le modalità tradizionali non possono ancora essere abbandonate. Il diritto dei cittadini ad avere servizi moderni e innovativi può non voler significare compressione del diritto di dialogare con modalità tradizionali, talvolta ritenute più efficaci.

E in ogni caso alla preoccupazione di intensificare i servizi telematici dovrebbe corrispondere una formazione della collettività diffusa e la generale possibilità di accedere ad Internet in modo libero e gratuito[21].

[21] S. Rodotà, *Una Costituzione per Internet?*, in *Politica del diritto*, 2010, 337 ss.; G. Finocchiaro - F. Delfini, *Diritto dell'informatica*, Torino, 2014; M. Nisticò - P. Passaglia (a cura di), *Internet e Costituzione*, Torino, 2014; M. Betzu, *Regolare Internet*, Torino, 2012; G. De Minico, *Diritti, Regole, Internet*, in www.costituzionalismo.it, 2, 2011, 15 ss,; T.E. Frosini, *Tecnologie e libertà costituzionali*, in *Diritto dell'informazione e dell'informatica*, 2003, 487 ss; Id., *Access to internet as fundamental right,* in *Italian journal of public law*, 2013, 226 ss.

Saggi

L’art. 21 ha settant’anni

I delitti contro il sentimento religioso: tra incriminazione dell'opinione e tutela della libertà di manifestazione del pensiero*

Fabio Basile

Abstract

I delitti contro il sentimento religioso, presenti nel nostro codice penale, sono prevalentemente strutturati quali "reati d'opinione". Ciò rende opportuno verificare se e a quali condizioni essi possano essere ritenuti compatibili con il fondamentale diritto, riconosciuto dalla Costituzione (art. 21), di manifestare liberamente il proprio pensiero. Il presente contributo ripercorre la giurisprudenza, ordinaria e costituzionale, che ha affrontato tale questione, dando altresì conto dell'evoluzione legislativa che i delitti in parola hanno conosciuto dal 1930 ad oggi.

The crimes against religious sentiment, provided by the Italian Criminal Code, are mainly framed as "crimes of opinion". Therefore, it should be ascertained whether and how those crimes are compatible with the exercise of freedom of expression, guaranteed as a fundamental right by Art. 21 of the Italian Constitution. The paper provides an overview of the jurisprudence – of ordinary courts and the Constitutional Court – and of the legislative evolution since 1930s about the crimes against religious sentiments.

Sommario

1. Premessa: il vilipendio quale "reato d'opinione". – 2. L'evoluzione dei delitti contro il sentimento religioso. – 3. (*Segue*): la riforma del 2006. – 4. La sentenza della Corte costituzionale n. 188 del 1975. – 5. L'esercizio del diritto di libera manifestazione del pensiero quale causa di giustificazione (art. 51 c.p.). – 6. Le più recenti applicazioni della giurisprudenza di legittimità. – 7. Chiusa.

Keywords: Religione, Vilipendio, Libertà di pensiero, Papa, Confessione religiosa

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

1. Premessa: il vilipendio quale "reato d'opinione"

I delitti contro il sentimento religioso[1], presenti nel nostro codice penale – un corpo di delitti di rara applicazione giurisprudenziale (soprattutto in tempi recenti), ma di rilevantissimo valore simbolico[2] – sono tuttora prevalentemente strutturati quali "reati d'opinione"[3].

Con la sola eccezione delle fattispecie di cui all'art. 405 c.p. (c.d. *turbatio sacrorum*) e all'art. 404 co. 2 c.p. (così come riformulato nel 2006: offese a una confessione religiosa mediante danneggiamento di cose), l'elemento centrale di tali delitti è, infatti, costituito dal "vilipendio", e il "vilipendio" è espressione di un'opinione: un'opinione di disprezzo e di dileggio[4], ma pur sempre un'opinione.

Risulta, pertanto, giocoforza porsi il problema della compatibilità dei delitti in parola con il fondamentale diritto, riconosciuto dalla Costituzione (art. 21), di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione.

2. L'evoluzione dei delitti contro il sentimento religioso

Degno di nota è, peraltro, il fatto che i delitti contro il sentimento religioso abbiano

[1] Per mera comodità del lettore, si riporta, nella formulazione originaria, il testo degli artt. 402-406 e 724 c.p., cui faremo più volte riferimento nel presente scritto:

Art. 402 - *Vilipendio della religione dello Stato*: «Chiunque pubblicamente vilipende la religione dello Stato è punito con la reclusione fino a un anno».

Art. 403 - *Offese alla religione dello Stato mediante vilipendio di persone*: «1. Chiunque pubblicamente offende la religione dello Stato, mediante vilipendio di chi la professa, è punito con la reclusione fino a due anni. 2. Si applica la reclusione da uno a tre anni a chi offende la religione dello Stato, mediante vilipendio di un ministro del culto cattolico».

Art. 404 - *Offese alla religione dello Stato mediante vilipendio di cose*: «1. Chiunque, in un luogo destinato al culto, o in un luogo pubblico o aperto al pubblico, offende la religione dello Stato, mediante vilipendio di cose che formino oggetto di culto, o siano consacrate al culto, o siano destinate necessariamente all'esercizio del culto, è punito con la reclusione da uno a tre anni. 2. La stessa pena si applica a chi commette il fatto in occasione di funzioni religiose, compiute in luogo privato da un ministro del culto cattolico».

Art. 405 - *Turbamento di funzioni religiose del culto cattolico*: «1. Chiunque impedisce o turba l'esercizio di funzioni, cerimonie o pratiche religiose del culto cattolico, le quali si compiano con l'assistenza di un ministro del culto medesimo o in luogo destinato al culto, o in un luogo pubblico o aperto al pubblico, è punito con la reclusione fino a due anni. 2. Se concorrono fatti di violenza alle persone o di minaccia, si applica la reclusione da uno a tre anni».

Art. 406 - *Delitti contro i culti ammessi nello Stato*: «Chiunque commette uno dei fatti preveduti dagli articoli 403, 404 e 405 contro un culto ammesso nello Stato è punito ai termini dei predetti articoli, ma la pena è diminuita».

Art. 724 - *Bestemmia e manifestazioni oltraggiose verso i defunti*: «Chiunque pubblicamente bestemmia, con invettive o parole oltraggiose, contro la divinità o i simboli o le persone venerati nella religione dello Stato, è punito con l'ammenda da lire cento a tremila [...]».

[2] Così, per tutti, P. Siracusano, *Commento agli artt. 402-406*, in M. Ronco-B. Romano (a cura di), *Codice penale ipertestuale*, IV ed., Torino, 2012, 1765 ss.

[3] Per la riconducibilità dei delitti contro il sentimento religioso nella (controversa) categoria dei "reati d'opinione", e per l'illustrazione di tale categoria, v., tra gli scritti più recenti, L. Alesiani, *I reati d'opinione. Una rilettura in chiave costituzionale*, Milano, 2006, 105 ss.

[4] Dottrina unanime; v. per tutti P. Siracusano, *I delitti in materia di religione*, Milano, 1983, 119; S. Prosdocimi, voce *Vilipendio (reati di)*, in *Enciclopedia del diritto*, Milano, 1993, vol. XLVI, 738.

conservato fino a oggi la predetta struttura di "reati d'opinione", nonostante i tanti rivolgimenti che li hanno interessati: il superamento del principio confessionistico; i plurimi interventi della Corte costituzionale; infine la riforma operata dalla l. 24 febbraio 2006, n. 85 ("Modifiche al Codice penale in materia di reati d'opinione").

Conviene, quindi, sia pur in estrema sintesi, ripercorrere la loro evoluzione legislativa e giurisprudenziale, al fine di meglio comprendere le attuali disposizioni incriminatrici di cui agli artt. 403, 404 e 405 c.p., e valutare i possibili punti di (perdurante) attrito delle stesse con l'art. 21 Cost.

Ebbene, nel loro impianto codicistico originario i delitti in parola – cui possiamo aggiungere, ai fini delle presenti riflessioni, anche la contravvenzione di bestemmia – offrivano una "tutela privilegiata", sia dal punto di vista qualitativo che dal punto di vista quantitativo, alla religione cattolica[5]: da una parte, infatti, le fattispecie di cui all'art. 402 c.p. ("Vilipendio della religione dello Stato") e all'art. 724 co. 1 c.p. ("Bestemmia") incriminavano soltanto le offese alla religione cattolica; dall'altra, l'art. 406 c.p. comminava una pena più lieve qualora i fatti di cui agli artt. 403-405 c.p. fossero stati commessi a danno di culti diversi da quello cattolico; nessuna tutela penalistica, infine, era offerta ai culti c.d. "non ammessi", vale a dire non riconosciuti dallo Stato né in modo esplicito (per effetto della l. 1159/1929 o in base a trattati internazionali o ancora, a partire dal 1984, in base a intese), né implicito (mediante atti statali di approvazione di ministri di culto o di erezione di enti con finalità religiosa).

Tale impianto originario costituiva il frutto della deliberata scelta dei compilatori del Codice penale del 1930 di dare rilievo, a livello di legislazione penale, al c.d. "principio confessionistico", vale a dire al riconoscimento della religione cattolica apostolica romana quale "religione dello Stato". In tal modo, infatti, il legislatore fascista intendeva, da una parte, esaltare la (da poco raggiunta) Conciliazione tra Stato italiano e Santa Sede e, dall'altra, sottolineare valori religiosi che potessero stimolare le energie del popolo italiano e fungere da fattore di unità morale della nazione[6].

Il superamento del principio confessionistico – implicitamente già avvenuto con l'emanazione della Costituzione e, esplicitamente, col Protocollo addizionale all'Accordo con la Santa Sede del 18 febbraio 1984, di modifica dei Patti lateranensi, ratificato con la l. 121 del 1985[7] – non aveva, tuttavia, provocato l'automatica caducazione dei delitti in parola: secondo la dottrina e la giurisprudenza assolutamente prevalenti, infatti, questi erano rimasti pienamente in vigore, in quanto la formula "religione dello Stato" sarebbe stata mero tramite linguistico per indicare, anche dopo il superamento del

[5] Sul punto, v. per tutti, N. Marchei, *"Sentimento religioso" e bene giuridico. Tra giurisprudenza costituzionale e novella legislativa*, Milano, 2006, 50 ss.

[6] Sul punto, v. per tutti G. Casuscelli (a cura di), *Nozioni di diritto ecclesiastico*, Torino, 2009, 245 ss. In proposito, v. pure quanto rilevato dalla stessa Corte costituzionale (C. Cost., 20 novembre 2000, n. 508): il sistema originario dei reati in materia di religione «si spiega per il rilievo che, nelle concezioni politiche dell'epoca, era riconosciuto al cattolicesimo quale fattore di unità morale della nazione»; la religione cattolica, pertanto, «oltre ad essere considerata oggetto di professione di fede, era assunta a elemento costitutivo della compagine statale e, come tale, formava oggetto di particolare protezione anche nell'interesse dello Stato».

[7] Cfr. F. Stella, *Il nuovo concordato tra l'Italia e la Santa Sede: riflessi di diritto penale*, in *Jus*, 1, 1989, 97 ss.

principio confessionistico, la religione cattolica[8].
Tale perdurante, e immutata, vigenza rendeva, tuttavia, ormai intollerabile il privilegio concesso, in sede penale, alla religione cattolica rispetto alle altre religioni. A tale privilegio, pertanto, reagirono, nei primi decenni dell'era repubblicana, non solo la dottrina, ma anche i giudici di merito, i quali sollevarono dinanzi alla Corte costituzionale una serie di eccezioni di legittimità, intese a rimuovere, alla luce degli artt. 3, 8, 19 e 20 Cost., gli effetti discriminatori prodotti dalla disciplina allora contenuta negli artt. 402-406 e 724 c.p. a scapito delle religioni diverse da quella cattolica.
In replica alle suddette eccezioni, tuttavia, in una prima fase la Corte costituzionale – facendo leva su un criterio quantitativo-sociologico di cui si presumeva l'idoneità a giustificare la tutela privilegiata riservata alla religione cattolica, quale religione della "maggioranza degli Italiani" – lasciava sopravvivere, con l'avallo della Cassazione, l'impianto originario del Codice Rocco[9].
A partire dal 1995, invece, la Corte costituzionale – stante anche la perdurante inerzia del legislatore, più volte invano stigmatizzata dal giudice delle leggi – con una serie di sentenze che hanno investito tutti i reati in parola, ha provveduto a rimuovere tali effetti discriminatori:
- sia quelli qualitativi: la tutela riservata alla sola religione cattolica dall'art. 402 c.p. è venuta integralmente meno[10]; quella di cui all'art. 724 c.p. è stata, invece, estesa anche ai culti acattolici[11];
- sia quelli quantitativi: le differenze di pena, previste originariamente dagli artt. 403, 404 e 405 c.p. rispetto alle ipotesi di cui all'art. 406 c.p., sono state, infatti, eliminate[12].

3. (*Segue*): la riforma del 2006

Infine, il legislatore del 2006, con la l. n. 85 di riforma dei reati d'opinione (che ha interessato, oltre ai delitti in parola, numerose altre disposizioni del codice penale, incriminatrici di delitti contro la personalità dello Stato), ha preso sostanzialmente atto del nuovo assetto dei delitti contro il sentimento religioso, risultante dai summenzionati, plurimi interventi della Corte costituzionale e, con una sorta di operazione di ripulitura lessicale (che ha investito sia il testo, sia le rubriche delle norme in esame), ha provveduto a cancellare ogni riferimento alla religione dello Stato/religione cattolica, e ha abrogato l'art. 406 c.p., che faceva riferimento ai culti acattolici, divenuto ormai

[8] Per i doverosi riferimenti di dottrina e giurisprudenza, sia consentito rinviare a F. Basile, *Commento agli artt. 403 ss.*, in E. Dolcini-G. Marinucci (a cura di), *Codice penale commentato*, Milano, 2015, 1827 ss.

[9] In tal senso, v. le pronunce C. Cost. 30 novembre 1957, n. 125; 30 dicembre 1958, n. 79; 31 maggio 1965, n. 39; 27 febbraio 1973, n. 14; 8 luglio 1975, n. 188 (sulla quale, v. però anche *infra*, par. 4); 23 aprile 1987, n. 147; 28 luglio 1988, n. 925; infine, 16 febbraio 1989, n. 54.

[10] C. Cost., 20 novembre 2000, n. 508, che ha dichiarato l'illegittimità dell'art. 402 c.p.

[11] C. Cost., 18 ottobre 1995, n. 440, che ha dichiarato l'illegittimità dell'art. 724 c.p., limitatamente alle parole «o i Simboli o le Persone venerati nella religione dello Stato». La contravvenzione di bestemmia è stata successivamente depenalizzata (d.lgs. 507/1999).

[12] In relazione all'art. 403 c.p., C. Cost., 29 aprile 2005, n. 168; in relazione all'art. 404 c.p., C. Cost., 14 novembre 1997, n. 329; infine, in relazione all'art. 405 c.p., C. Cost., 9 luglio 2002, n. 327.

superfluo[13].

Oltre a questo intervento di tipo "cosmetico", tuttavia, la riforma del 2006 ha introdotto (tra l'altro) due fattori di novità sostanziale, senz'altro rilevanti nella prospettiva della compatibilità con l'art. 21 Cost. dei "nuovi" delitti contro il sentimento religioso: in primo luogo, infatti, il legislatore ha previsto all'art. 404, c. 2 c.p. una nuova fattispecie di reato (il danneggiamento di cose attinenti al culto), all'interno della quale la dimensione di "reato d'opinione" appare oggi sfumata a favore, invece, di una prevalente dimensione di reato di danno patrimoniale alle cose (tant'è che si parla, in proposito, di vilipendio "reale"); in secondo luogo, e soprattutto, il legislatore del 2006 ha scelto di rinunziare alla pena detentiva per tutti i reati d'opinione, compresi, ovviamente, anche i vilipendi di cui agli artt. 403 e 404, c. 1, c.p., i quali sono ora puniti con una assai modesta, quasi risibile, pena pecuniaria (la reclusione è, invece, comminata per il predetto nuovo delitto di cui all'art. 404, c. 2, c.p., oltreché per la *turbatio sacrorum* di cui all'art. 405 c.p.).

Ma ancor più rilevante, nella prospettiva qui indagata dei rapporti con l'art. 21 Cost., è stato quanto il legislatore del 2006 "non ha fatto" (con scelta più o meno consapevole):

- il legislatore del 2006, infatti, "non" ha ripristinato il delitto di vilipendio "diretto" della religione (di cui al vecchio art. 402 c.p., già dichiarato incostituzionale nel 2000), come pure sarebbe stato in teoria possibile fare, ovviamente previa sua estensione a tutte le religioni[14]. Ciò comporta la definitiva non-punibilità, oggi, del vilipendio della religione che non passi per il tramite di un'aggressione a persone (art. 403 c.p.) o cose (art. 404, c. 1, c.p.): la religione in sé (o "le" religioni in sé), con i suoi dogmi e fondamenti, non assurge più a oggetto autonomo di tutela penale[15]. È, quindi, per sempre scomparsa dalla nostra legislazione penale la figura forse più "odiosa" di reato d'opinione in materia di religione, tramite la quale, in passato, si era talora giunti a punire – emblematica, in tal senso, la vicenda di Pier Paolo Pasolini e del suo cortometraggio "La Ricotta"[16] – anche il dissenso provocatorio, la critica radicale, la satira dissacrante verso i "contenuti" della religione (che, peraltro, allora era solo la religione cattolica);
- il legislatore del 2006 "non" ha, poi, preso posizione alcuna circa il bene giuridico tutelato dai "nuovi" delitti di cui agli artt. 403-405 c.p.: e questo silenzio è senz'altro interpretabile come assenso a quell'orientamento, che risultava ormai dominante nella dottrina e nella giurisprudenza pre-riforma, secondo cui il bene giuridico tutelato dai delitti in parola è il "sentimento religioso", e non già la religione quale "bene di civiltà". Se, infatti, il legislatore fascista del 1930, attraverso gli artt. 402-405 e 724 c.p., aveva

[13] D. Pulitanò, *Laicità e diritto penale*, in *Rivista italiana di diritto e procedura penale*, 1, 2006, 81.

[14] N. Marchei, *"Sentimento religioso" e bene giuridico. Tra giurisprudenza costituzionale e novella legislativa*, cit., 190; P. Siracusano, *Commento agli artt. 402-406*, cit., 1765.

[15] M. Pelissero, *Osservazioni critiche sulla legge in tema di reati di opinione; occasioni mancate e incoerenze sistematiche (II)*, in *Diritto penale e processo*, 2006, 1201; F. Giunta, *Verso un rinnovato romanticismo penale? I reati in materia di religione e il problema della tutela dei sentimenti*, in AA.VV., *Studi in onore di Mario Romano*, Napoli, 2011, vol. III, 1546.

[16] Condannato in primo grado (Trib. Roma, sez. IV, 7 marzo 1963), Pasolini veniva assolto in appello, ma la sentenza di assoluzione era poi annullata dalla Cassazione su ricorso del procuratore generale, con una sentenza (Cass. pen., sez. III, 24 febbraio 1967, n. 328, *CED* 104261) la quale, tuttavia, dichiarava estinto il reato per amnistia.

inteso tutelare la religione (cattolica) in sé, quale valore culturale e sociale, patrimonio di dogmi e principi[17], dopo l'avvento della Costituzione la dottrina e la giurisprudenza, invece, si impegnarono nella ricerca di un bene giuridico per questi reati che risultasse "compatibile" con il nuovo volto – laico, secolarizzato e pluralista – dell'Italia repubblicana; e tale bene fu infine individuato nel "sentimento religioso", inteso come una sorta di corollario del diritto, costituzionalmente riconosciuto, di libertà di religione[18].
Nel silenzio del legislatore del 2006, tale approdo può senz'altro essere mantenuto fermo anche oggi[19], sicché non residua più alcun dubbio sul fatto che gli attuali delitti di cui agli artt. 403-405 c.p. tutelino un bene di rango costituzionale, all'occorrenza bilanciabile col diritto di libera manifestazione del pensiero di cui all'art. 21 Cost.
Dopo il 2006 – quale effetto intenzionale e, in buona parte, anche preterintenzionale della riforma – possiamo, quindi, constatare che i punti di attrito tra i delitti di cui agli artt. 403-405 c.p. e l'art. 21 Cost. si sono indubbiamente smussati.

4. La sentenza della Corte costituzionale n. 188 del 1975

Un contributo assai rilevante al processo, descritto nelle precedenti righe, di ridefinizione del bene giuridico protetto – passato dalla "religione bene di civiltà" al "sentimento religioso" – è stato sicuramente fornito dalla sentenza della Corte costituzionale n. 188 del 1975, con cui il giudice delle leggi, per la prima e finora unica volta, ha sindacato la legittimità costituzionale dei delitti in parola alla luce dell'art. 21 Cost.
Con tale sentenza, in particolare, la Corte, facendo ricorso alla c.d. "teoria del bilanciamento" tra interessi o valori costituzionali in conflitto, ha escluso la fondatezza di un'eccezione di incostituzionalità, sollevata in relazione all'art. 403 c.p.
A tal fine la Corte è partita da una premessa fondamentale: il bene giuridico tutelato dall'art. 403 c.p. è il «sentimento religioso, quale vive nell'intimo della coscienza individuale e si estende anche a gruppi più o meno numerosi di persone legate tra loro dal vincolo della professione di una fede comune», e tale bene «è da considerare tra i beni costituzionalmente rilevanti, come risulta da una lettura coordinata degli artt. 2, 8 e 19 Cost., e come risulta indirettamente confermato anche dal primo comma dell'art. 3 e dall'art. 20 Cost.».
A questo punto si è fatta strada la conclusione, nel ragionamento della Corte, secondo cui il delitto di vilipendio di cui all'art. 403 c.p., proprio perché posto a tutela di un bene di rilevanza costituzionale, può «legittimamente [...] limitare l'ambito di operatività dell'art. 21 Cost.».

[17] Fondamentale in tal senso lo studio di P. Siracusano, *I delitti in materia di religione*, cit., 11 s.

[18] Per i doverosi riferimenti di dottrina e giurisprudenza, sia consentito rinviare nuovamente a F. Basile, *Commento agli artt. 403 ss.*, cit., 1831 ss.

[19] Va solo precisato che – considerato l'insistito riferimento, operato dagli attuali artt. 403-405 c.p., alle "confessioni religiose", considerata altresì la procedibilità d'ufficio di questi delitti, e avuto riguardo, infine, alle connotazioni spazio-temporali che collocano i vari fatti di reato in esame in una dimensione schiettamente superindividuale – il sentimento religioso da essi tutelato non pare possa coincidere col sentimento religioso individuale, bensì solo col sentimento religioso collettivo, e segnatamente col sentimento religioso dei fedeli che si riconoscono in una determinata confessione religiosa.

Tale conclusione, tuttavia, viene subito corredata dalla Corte con una fondamentale precisazione: occorre circoscrivere «la figura della condotta vilipendiosa [...] entro i giusti confini, segnati, per un verso, dallo stesso significato etimologico della parola (che vuol dire "tenere a vile", e quindi additare al pubblico disprezzo o dileggio), e, per altro verso, dalla esigenza [...] di rendere compatibile la tutela penale accordata al bene protetto dalla norma in questione [art. 403 c.p.] con la più ampia libertà di manifestazione del proprio pensiero in materia religiosa, con specifico riferimento alla quale non a caso l'art. 19 Cost. anticipa, in termini quanto mai espliciti, il più generale principio dell'art. 21 Cost. È evidente, ad esempio, a tacer d'altro, che non sussisterebbe quella libertà di far "propaganda" per una religione, come espressamente prevede e consente l'art. 19 Cost., se chi di tale diritto si avvale non potesse altrettanto liberamente dimostrarne la superiorità nei confronti di altre, di queste ultime criticando i presupposti o i dogmi».

E al fine di circoscrivere la condotta vilipendiosa «entro i giusti confini», la Corte rimarca che il vilipendio non va confuso né con la discussione su temi religiosi, così a livello scientifico come a livello divulgativo, né con la critica e la confutazione pur se vivacemente polemica; né, infine, con l'espressione di radicale dissenso da ogni concezione richiamantesi a valori religiosi trascendenti, in nome di ideologie immanentistiche o positivistiche o altre che siano. Per contro, sempre secondo la Corte, costituiscono vilipendio, e sono «pertanto esclusi dalla garanzia dell'art. 21 Cost. (e dell'art. 19 Cost.)», la contumelia, lo scherno, l'offesa, per dir così, fine a sé stessa, che costituisce a un tempo ingiuria al credente (e perciò lesione della sua personalità) e oltraggio ai valori etici di cui si sostanzia e alimenta il fenomeno religioso, oggettivamente riguardato.

5. L'esercizio del diritto di libera manifestazione del pensiero quale causa di giustificazione (art. 51 c.p.)

Dopo la sentenza del 1975 e, a maggior ragione, dopo la riforma del 2006 (coi suoi effetti intenzionali e preterintenzionali sopradescritti), la questione della legittimità dei delitti contro il sentimento religioso rispetto all'art. 21 Cost. non pare essere più stata affrontata dalla Corte costituzionale[20].

Sembrerebbe, quindi, non esistere (o non esistere più) un contrasto, frontale e assoluto, dei delitti in parola con l'art. 21 Cost., di proporzioni tali da reclamarne l'espulsione dal nostro ordinamento con efficacia *erga omnes*.

Nei procedimenti che hanno ad oggetto questi delitti, invece, il richiamo al diritto alla libera manifestazione del pensiero continua a essere assai frequente nella differente prospettiva di giustificare, per il tramite dell'art. 51 c.p., la condotta tenuta, nel caso di specie, dal singolo imputato.

Un tale approccio è, ad esempio, stato seguito nel 2001 dal Tribunale di Latina, chia-

[20] Segnaliamo solo un'ordinanza del 1989 (n. 479), con cui la Corte ha ritenuto manifestamente inammissibile una questione di legittimità, genericamente e confusamente motivata con riferimento anche all'art. 21 Cost., sollevata dal pretore di Orvieto nell'ambito di un procedimento che vedeva imputata del reato di cui all'art. 403 c.p. una giovane donna che aveva attaccato sul retro della sua auto un adesivo riportante la scritta: «Wojtyla? No, grazie!».

mato a decidere della punibilità, ai sensi dell'art. 403 c.p., di un imputato che aveva pubblicato online tre vignette "animate" dal seguente contenuto:
1) «*Perché al clero fa paura il gay pride?*: vignetta in cui si vede un alto prelato che subisce un atto di sodomizzazione e che all'inizio resta indifferente, ma al momento della completa penetrazione da parte del partner ne trae piacere»;
2) *«La pagina dei fans di pope'n'poppe*: vignetta in cui si vede un'immagine animata di una ragazza bionda dal cui seno esce la testa del Papa. La spiegazione del gioco – consistente nel combattere contro il Pontefice per toccare la giovane donna – è la seguente: "Il sogno di tutti è agguantare degli splendidi seni, ma spesso risalgono in superficie pudori inconsci radicati in noi da anni di bombardamento pseudo-spirituale cattolico. Così ecco il Papa, simbolo di tutto questo, che ci si avventa contro per impedirci un sano piacere materiale"»;
3) *«Il cursore animato del Papa che si masturba*, inserito nella sezione *gadgets* del sito»[21].
Rispetto alle prime due vignette il Tribunale di Latina ritiene che esse esprimano, sia pur nella loro grossolana irriverenza, un "messaggio": una critica satirica della posizione assunta dalle gerarchie ecclesiastiche nei confronti dell'omosessualità e, più in generale, del desiderio sessuale. Per tale motivo esse sarebbero "coperte" dalla causa di giustificazione dell'esercizio di un diritto (art. 51 c.p.) e, segnatamente, del diritto di satira, che rinviene il suo fondamento nell'art. 21 Cost.
Rispetto, invece, alla terza vignetta, il Tribunale di Latina esclude che nella stessa sia ravvisabile un qualche «elemento di irrisione costruttiva, direttamente o indirettamente riconducibile nell'alveo della libera manifestazione del pensiero, perché finalizzata alla gratuita mostra di un aspetto della vita sessuale del Pontefice», e pertanto la fa ricadere al di fuori della causa di giustificazione dell'esercizio del diritto di satira (salvo poi comunque non punire l'imputato in quanto questi avrebbe agito senza dolo di vilipendio)[22].
Con tale decisione il Tribunale di Latina si allinea, peraltro, ad un orientamento diffuso in dottrina e giurisprudenza, secondo cui non godrebbero dell'ombrello protettivo offerto dall'art. 21 Cost. quei fatti di vilipendio non costituenti in alcun modo manifestazione di pensiero, come, ad esempio, l'insulto fine a se stesso, l'esplosione verbale informe, inidonea a trasmettere informazioni, valutazioni o altro atteggiamento spirituale, nonché quei fatti di vilipendio che, pur esprimenti un pensiero, travalichino, per la loro volgarità o turpitudine, il limite del buon costume.
L'invocazione del diritto alla libera manifestazione del pensiero (art. 51 c.p. in combinato disposto con art. 21 Cost.) non è, invece, valsa ad Oriana Fallaci per evitare, nel 2005, il rinvio a giudizio per il reato di cui all'art. 403 c.p. per avere la stessa usato, all'interno del suo libro "La forza della ragione", espressioni offensive nei confronti dell'Islam e dei suoi fedeli, dal momento che, ad avviso del G.U.P., tali espressioni risultavano inserite in un contesto che rivelava sentimenti di avversione e disprezzo verso

[21] Cfr. Trib. Latina, 7 giugno 2001, in *Dir. Eccl.*, II, 2002, 99 ss., da cui è ripresa la descrizione delle tre vignette.

[22] Per maggiori ragguagli su tale vicenda giudiziaria, può vedersi, volendo, F. Basile, *Sentimento religioso e libertà di satira: riflessioni a partire da Charlie Hebdo. La pubblicazione delle dodici vignette satiriche sull'Islam costituisce reato (in Italia)?*, in *Notizie di Politeia*, XXXI, 2015, 77 s.

ogni manifestazione proveniente da tutte le popolazioni di religione islamica (senza distinguere tra moderati ed estremisti) e volutamente dirette a disegnarne una immagine temibile, connotata non soltanto da sanguinaria ostilità verso il mondo occidentale, ma anche da costumi retrivi e spregevoli[23]. Il processo, come è noto, poi non si celebrò per la sopravvenuta morte nel 2006 della giornalista-scrittrice, sicché non sapremo mai se, all'esito del dibattimento, a suo favore sarebbe stato alla fine riconosciuto, in funzione scriminante (art. 51 c.p.), l'esercizio del diritto alla libera manifestazione del pensiero[24].

6. Le più recenti applicazioni della giurisprudenza di legittimità

Dopo la riforma del 2006 le applicazioni giurisprudenziali degli artt. 403 ss. c.p., soprattutto in sede di legittimità, si sono ancor più diradate, ma non del tutto estinte[25].
Tra le più recenti, possiamo segnalare una sentenza della Cassazione del 2015, relativa al caso di un settantaduenne, imputato del delitto di cui all'art. 403 co. 2 c.p. (offese ad una confessione religiosa mediante vilipendio di un suo ministro di culto) per aver esposto, in pieno centro a Milano, un trittico da lui stesso realizzato, formato da tre fotocopie in bianco e nero, stampate su tela, delle dimensioni di 170x70 centimetri, raffiguranti, rispettivamente, il Pontefice Benedetto XVI, un pene con testicoli, e il segretario personale del Pontefice, mons. Ganswein, con sotto la didascalia «Chi di voi non è culo scagli la prima pietra».
Secondo la difesa, il trittico sarebbe un'opera artistica, da interpretare esclusivamente quale manifestazione, sia pur cruda e volgare, di un dissenso in chiave critica, ironica e satirica, verso l'opinione espressa dalle gerarchie ecclesiastiche sull'omosessualità: la condotta dell'imputato risulterebbe quindi giustificata, per il tramite dell'art. 51 c.p., dal diritto di libera manifestazione del pensiero.
La Cassazione (e prima di lei i giudici di merito), per contro, ritiene che il trittico esposto – sia per la collocazione in sequenza delle tre immagini, sia per la didascalia posta a

[23] G.U.P. Bergamo, ord. 16 maggio 2005, pubblicata per estratto in *Quaderni di diritto e politica ecclesiastica*, 2006, 1029 s.

[24] Va, peraltro, aggiunto che grazie all'art. 21 Cost. la Fallaci non venne, invece, rinviata a giudizio per l'altro reato contestatole nel medesimo procedimento, vale a dire il reato di istigazione all'odio razziale ed etnico: come si legge nell'ordinanza del G.U.P. di Bergamo appena citata, infatti, «la configurabilità del reato di cui all'art. 3 della legge n. 654 del 1975 è esclusa dalla finalità dell'argomentazione, tesa esclusivamente a provocare la presa di coscienza del pericolo per l'Europa conseguente ad una massiccia immigrazione dei musulmani: come tale essa costituisce estrinsecazione della libertà di pensiero, garantita dall'art. 21 Cost.».

[25] Oltre ai due casi che tra breve commenteremo, segnaliamo anche Cass. pen., sez. III, 15 settembre 2015, n. 41821, *CED* 265497: condanna dell'imputato per il delitto di offese a una confessione religiosa mediante danneggiamento di cose (art. 404, c. 2 c.p.), per aver questi deturpato le pareti di una chiesa leccese con scritte offensive nei confronti del Pontefice Benedetto XVI; Cass. pen., sez. III, 8 settembre 2016, n. 3072: condanna degli imputati per il delitto di *turbatio sacrorum* (art. 405 c.p.) per avere gli stessi impedito e turbato una funzione religiosa del culto cristiano evangelico pregando ad alta voce fino al punto da coprire la voce dei celebranti e degli altri fedeli ed insultando e minacciando reiteratamente i celebranti e gli altri fedeli presenti. In tali due applicazioni, tuttavia, non viene in rilievo il profilo della libera manifestazione del pensiero.

loro corredo, sia per il significato che a tale didascalia potevano attribuire agevolmente tutti i passanti – costituisca una chiara allusione a presunti rapporti omosessuali, peraltro non consentiti dal voto di castità, tra il Pontefice e il suo assistente: altro che opera artistica, quindi, ma solo una rappresentazione «indecorosa ed offensiva nell'accezione dell'uomo medio». Con la propria condotta, pertanto, l'imputato avrebbe «violato il limite dovuto al rispetto della devozione altrui, ingiustamente messo a repentaglio da una manifestazione che, lungi dall'essere meramente critica di costumi sessuali non consentiti a ministri del culto, appare costituire una mera contumelia, scherno e offesa fine a sé stessa».

Il Pontefice Benedetto XVI risulta, suo malgrado, preso di mira anche nel caso giudicato dall'ultima e più recente sentenza di Cassazione che vogliamo qui ricordare, del 2017, relativa a cinque persone le quali organizzavano una sorta di *flash mob* ad un angolo del sagrato di una chiesa di Lecce, dove collocavano, in posizione ben visibile, un cartellone raffigurante sullo sfondo una sagoma costituita dall'immagine di Papa Ratzinger e, in primo piano, un bersaglio costituito da una serie di cerchi concentrici con l'indicazione di punteggi vari, riportante in calce la scritta: «1.000 punti, caramelle, preservativi, vino e ostie sconsacrate se centri quel buco di culo da cui quotidianamente vomita fiumi di merda». Su un siffatto bersaglio lanciavano, quindi, numerose freccette colorate.

Chiamati a rispondere del delitto di cui all'art. 403 co. 2 c.p., per aver offeso la confessione religiosa cattolica mediante vilipendio del Pontefice, gli imputati a loro difesa invocavano (tra l'altro) l'art. 21 Cost. in funzione scriminante (art. 51 c.p.): con la loro condotta essi avrebbero voluto esprimere una critica all'allora Pontefice in quanto persona, a causa delle posizioni dal medesimo assunte in tema di omosessualità e abusi sui minori, e non già offendere il sentimento religioso degli appartenenti alla confessione cattolica mediante un attacco al suo massimo rappresentante.

Secondo la valutazione delle corti di merito, condivisa dalla Cassazione, invece, «non solo il contenuto del cartellone, le azioni intraprese sullo stesso (il lancio di freccette), il luogo ove tale *flash mob* era stato organizzato risultano oggettivamente, e senza equivoci, idonei e volti a "svilire" e ferire il sentimento religioso cattolico, ma è proprio nei motivi di ricorso, laddove i ricorrenti hanno adombrato le ragioni di tale loro contestazione (per le posizioni assunte dal Papa nei confronti dei gay ed altre), che emerge, con vivida chiarezza, che l'attacco violento e volgare al Papa era rivolto allo stesso in quanto Capo della Chiesa cattolica, e, quindi, in quanto il contenuto delle dichiarazioni e dei messaggi del Papa era in grado di orientare i fedeli e di raggiungere il sentimento religioso degli stessi».

In questa sentenza, peraltro, la Cassazione richiama proprio la decisione n. 188 del 1975 della Corte costituzionale sopra illustrata, e si pone nel solco della stessa per ribadire, da un lato, che il delitto di cui all'art. 403 c.p. costituisce «una limitazione di operatività dell'art. 21 Cost.»; dall'altro, che tale limitazione non scatta quando non di mero vilipendio si tratti, bensì di «discussione, scientifica o meno, sui temi religiosi, di critica, o di espressione di dissenso dai valori religiosi per l'adesione ad ideologie atee o di altra natura, ovvero di confutazione, anche con toni accesi, dei dogmi della fede».

7. Chiusa

L'indicazione fornita dalla Corte costituzionale già nel 1975, e da ultimo ripresa dalla Cassazione nel più recente dei casi di cui abbiamo notizia, costituisce, a nostro modesto avviso, una formula sostanzialmente corretta per trovare il delicato punto di equilibrio tra il diritto alla libera manifestazione del pensiero e il rispetto dovuto al sentimento religioso dei fedeli di una confessione religiosa.
Si tratta, tuttavia, di una formula di difficile applicazione concreta e dagli esiti assai incerti, in quanto la prassi giudiziaria ci mostra che i contorni dei due valori da soppesare alla ricerca del punto di equilibrio in realtà non risultano quasi mai ben delineati e stagliati, e si prestano, quindi, ad ondivaghe valutazioni discrezionali.
Sotto le ceneri, la problematica compatibilità dei delitti in parola con il fondamentale diritto, riconosciuto dalla Costituzione (art. 21), di manifestare liberamente il proprio pensiero, continua, quindi, ad ardere, e potrebbe in ogni momento avvampare soprattutto in un periodo, come l'attuale, in cui la religione (quella cattolica, quella islamica, quella ebraica ...) sembra offrire spesso, quasi sempre suo malgrado, il pretesto per innescare conflitti[26].

[26] Sul recente incremento dei conflitti su base religiosa nelle società occidentali, e sulle cause di tale incremento, v. C. Cianitto, *Quando la parola ferisce. Blasfemia e incitamento all'odio religioso nella società contemporanea*, Torino, 2016, 3 ss. e, volendo, la recensione a tale libro, di F. Basile, *Recensione*, in *Diritto Ecclesiastico*, 2015, 335 ss.

Saggi

Fake news, pluralismo informativo e responsabilità in rete

Le *fake news* sui social network: un'analisi economica*

Vincenzo Visco Comandini

Abstract

Il contributo approfondisce i profili economici – domanda, offerta e loro equilibri – delle fake news sui social networks, analizzando le diverse ragioni della loro diffusione e gli effetti negativi che queste producono sul benessere collettivo, fra cui la perdita di credibilità dei media e la capacità dei cittadini di prendere decisioni politiche consapevoli e informate. I possibili interventi di politica, finalizzati a contenere il fenomeno, per essere efficaci richiedono una decisa azione di autoregolazione da parte dei gestori delle piattaforme digitali, che rischiano di vedere significativamente ridotti gli investimenti pubblicitari.

The paper discusses the economics of the fake news on social networks, including their supply, demand, and equilibria. The reasons of their diffusion among social media, as well as negative consequences on both democracy and media's reputation loss are scrutinized. Possible policies aimed at fighting social backslashes of the fake news require to be harmonized with digital platform's measures, since social networks risk a strong drop in advertising expenditure.

Keywords: Fake news, Disinformazione, Post-verità, Social network, Phishing

1. Introduzione

Questo lavoro[1] approfondisce i profili economici delle *fake news*, i meccanismi attraverso cui queste riescono ad alterare e distorcere le opinioni degli utilizzatori, in particolare sui *social network*, e gli effetti negativi che queste producono sul benessere collettivo e sul funzionamento della democrazia.

Genesi, efficacia e meccanismi di diffusione delle *fake news* sono analizzati attraverso lo studio degli equilibri che si generano nell'interazione della loro domanda e offerta. Il concetto di equilibrio – che sperimentiamo quotidianamente quando siamo in fila alle casse del supermercato alla ricerca di quella più breve, osservando che esse, appunto

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

[1] Una precedente versione è stata preparata per il gruppo di studio Astrid *Comunicazione e diffusione delle informazioni sui social* coordinato da F. Pizzetti, pubblicata su *Astrid Rassegna* n. 273, 16, 2017.

in equilibrio, tendono ad essere di uguale lunghezza[2] - applicato alle *fake news* mostra come queste possano alterare, anche in modo decisivo, il normale funzionamento dei mercati dell'informazione e della politica.

Allcott e Gentzkow[3] definiscono le *fake news* come qualsiasi articolo contenente notizie deliberatamente false che può trarre in inganno i lettori. Tale definizione, basata sui due caratteri chiave di autenticità e finalità[4] che identificano la presenza di falsità verificabili, include anche articoli originariamente apparsi su siti web satirici ma confondibili con fatti reali, specie se letti isolatamente sui *feed* di Twitter o Facebook.

Le *fake news* non sono certo un fenomeno nuovo, ma oggi sono diventate ben più rilevanti e socialmente pericolose con l'avvento dei social network (d'ora in poi, SN), le cui reti si sono sviluppate in modo impressionante. A livello globale, a settembre 2017 Facebook disponeva di ben 2 miliardi di utilizzatori mensili, Whatsapp di 1,3 mld, Twitter di 328 milioni (fonte: Statista). Nel 2016, il 62% degli adulti statunitensi ha letto notizie sui SN, contro il 49% nel 2012 (fonte: journalism.org). Le *fake news* trovano sui SN un terreno particolarmente fertile di diffusione, perché l'utente trova informazioni già preconfezionata e sintetizzate che può subito commentare con i propri amici con cui è connesso. Il legame fra uso dei SN e presenza di *fake news* ha diverse ragioni, sia economiche che politico-culturali.

La prima ragione è che, grazie a Internet, le barriere all'ingresso nell'industria dei media si sono ridotte quasi a zero, essendo oggi tecnicamente molto semplice creare siti web e, se il numero dei contatti ricevuti è sufficiente, ricavarne utili con la pubblicità. Quando una *fake news*, originariamente pubblicata su un certo sito, è discussa e creduta vera o interessante fra i componenti di un SN, lo stesso sito, se si genera l'effetto virale di diffusione dell'informazione, riceve una notevole quantità di visite che consente al suo gestore di realizzare profitti.

La seconda ragione è l'accentuata polarizzazione politica dell'elettorato, osservata in tutto il mondo occidentale, in cui prevale la tendenza degli appartenenti ad un certo schieramento politico o ideologico a sviluppare forti sentimenti negativi nei confronti degli avversari. Sui SN la polarizzazione è un attributo tipico associato alle discussioni fra utenti su questioni civili o culturali quali, ad esempio la medicina ufficiale e quella alternativa. Quattrociocchi e Vicini[5] hanno analizzato le interazioni di 2,3 milioni di visitatori di siti italiani di narrazioni di scienza alternativa, messi a confronto con quelle di altrettanti utenti di siti classificati come favorevoli alla scienza ufficiale. Le interazioni all'interno del gruppo sulla scienza alternativa risultano più numerose - gli utenti sono più partecipi e attivi - rispetto a quelle registrate nel gruppo di scienza ufficiale, ma entrambi i gruppi appaiono chiusi e polarizzati l'uno rispetto all'altro, senza alcun confronto reciproco.

---

[2] La similitudine è di G. Akerlof - R. Shiller, *Phishing for Phools. The Economics of Manipulation and Deception*, Princeton and Oxford, 2015, 1 ss.

[3] H. Allcott - M. Gentzkow, *Social Media and Fake News in the 2016 Election*, in *Journal of Economic Perspectives*, 31:2, 2017, 211 ss.

[4] K. Shu - A. Sliva - S. Wang - J. Tang - H. Liu, *Fake News Detection on Social Media: A Data Mining Perspective*, in *ACM SIGKDD Explorations Newsletter*, August 2017.

[5] W. Quattrociocchi - A. Vicini, *Misinformation. Guida alla società dell'informazione e della credulità*, Milano 2016.

Chi esprime tali sentimenti negativi è più esposto alle *fake news*, in quanto è indotto a ritenere vera qualsiasi informazione che metta in cattiva luce o denigri gli esponenti avversari. Bakshy, Messing e Adamic[6] mostrano come le amicizie su Facebook tendano ad aggregarsi per gruppi ideologicamente omogenei: negli Stati Uniti la quota degli amici di un utente che appartengono ad uno schieramento politico opposto al suo sono solo il 20% fra i democratici e il 18% fra i repubblicani.

Le cause della polarizzazione della politica sono molteplici, alcune delle quali inerenti i meccanismi di formazione della classe politica, come mostra l'analisi di Sinclair[7] per gli Stati Uniti dove l'ideologia diventa lo strumento della polarizzazione. Più in generale, si può ritenere che la riduzione di benessere della classe media, tradizionale fulcro dei sistemi democratici, generata sia dal progresso tecnologico nei servizi (suo tipico campo d'occupazione), sia dalla globalizzazione dell'economia, abbia reso elettoralmente meno attraente per i politici l'uso dei consueti strumenti del dialogo e della mediazione degli interessi, che richiede accordi, realismo, condivisione di idee o obiettivi. I politici trovano invece sempre più spesso vantaggioso, a fini elettorali, utilizzare nelle loro comunicazioni sui SN la leva ideologica che, generando emozioni, tende a polarizzare le opinioni e a sviare il dibattito dai fatti reali, creando spazio per racconti preconfezionati e quindi anche, nei casi più estremi, *fake news*. E' stato osservato che in Italia, anche a causa della crisi finanziaria dei partiti politici che non godono più di alcun contributo pubblico, nelle elezioni i manifesti elettorali vengono sempre più spesso sostituiti dai SN[8], attraverso cui i politici cercano di attrarre consenso[9] specie per i cittadini che mostrano una crescente disaffezione per la politica. Per i politici più disinvolti, le *fake news* costituiscono quindi un nuovo strumento a basso costo, finalizzato a raggiungere selettivamente gli elettori meno istruiti.

La terza ragione è che i SN si sono rivelati uno strumento molto efficace per diffondere notizie false. È stato recentemente stimato che più di un milione di tweet sono derivati dalla nota *fake news Pizzagate*, i cui ideatori sostenevano l'esistenza di una cospirazione per tenere nascoste le email di John Podesta, il manager della campagna della Clinton, hackerati e successivamente diffusi da *WikiLeaks*.[10] Gli utenti dei SN, se cercano informazioni politico-sociali, hanno quindi un'elevata probabilità di leggere articoli di notizie allineate con la propria appartenenza politica o ideologica, e di incontrare storie false, che però interpretano come vere perché concordanti con il loro pensiero.

La quarta ragione ha a che fare con il web e la sua modalità prevalente di finanziamento, la pubblicità. Su Internet, grazie soprattutto ai motori di ricerca e ai SN, la distinzione fra informazione vera e propria – il contenuto cercato dall'utente – e informazione pubblicitaria tende a farsi meno netta, fino in alcuni casi a scomparire. In questo caso,

---

[6] E. Bakshy - S. Messing - L. A. Adamic, *Exposure to Ideologically Diverse News and Opinion on Facebook, Science* 348(6239), 2015, 1130 ss.

[7] B. Sinclair, *Party Wars: Polarization and the Politics of National Policy Making*, Oklahoma City, 2006.

[8] S. Scherer, *In Italian election campaign, Facebook, Twitter replace posters, piazzas, Yahoo! News*, 1 March 2018.

[9] Cfr. Openpolis, *A caccia di voti con le sponsorizzazioni social*, 26 febbraio 2018.

[10] Secondo Pizzagate, le email avrebbero in realtà contenuto messaggi in codice su traffici umani scambiati da una rete di pedofili comprendente noti ristoranti negli Stati Uniti e alcuni membri del partito democratico. Il Dipartimento di Giustizia è dovuto intervenire per dichiarare la notizia completamente falsa e priva di fondamento. Cfr. Wikipedia Pizzagate Conspiracy Theory, 2017.

l'obiettivo dei gestori dei servizi e degli inserzionisti non è di ingannare i consumatori, ma di rendere loro più rilevante e meno fastidiosa possibile la pubblicità. Non a caso gli algoritmi che trovano i contenuti cercati dall'utente sono gli stessi che selezionano la pubblicità a lui dedicata. Ciò non di meno l'effetto ottenuto, se aumenta l'efficacia delle inserzioni sul web, superando di molto quelle sulla carta stampata o anche sulla TV, crea però un fraintendimento nel consumatore, che non è sempre in grado di distinguere fra informazione e pubblicità. Nelle inserzioni *contextual display* (quelle su Facebook o YouTube) quest'effetto è amplificato sia dall'elemento emozionale inserito nel messaggio pubblicitario, sia dal fatto che, a differenza dei motori di ricerca generalisti, gli utenti cercano contenuti personali (storie, notizie e profili di altri utenti) e spettacoli (video, musica, film, documentari, dibattiti, ecc.), che sono in realtà forme d'intrattenimento aggregatrici di audience. Le *fake news* utilizzano il medesimo meccanismo per diffondersi: leggendole il consumatore, anche se ha dubbi sulla loro autenticità, divertendosi è portato a condividerle con la propria cerchia di amici, esattamente come quando vediamo un film che ci è piaciuto (o non ci è piaciuto) e lo consigliamo (o sconsigliamo) agli amici. Le *fake news* rappresentano quindi anche una forma estrema di *infotainment*[11], e di conseguenza possono avere un certo valore commerciale. In un recente seminario tenutosi alla Sapienza Università di Roma[12], uno dei maggiori creatori di fake ha confermato che i lettori sono irresistibilmente attratti dagli argomenti su cui hanno i nervi scoperti, che commentano estremizzando ancor più il loro contenuto e diffondendolo sui SN, spesso per puro divertimento.

La quinta ragione è il vistoso calo di fiducia che i cittadini dei paesi sviluppati mostrano nei confronti dei grandi media, in America in modo più accentuato fra i repubblicani rispetto ai democratici (nel 2016 il 50% dei democratici dichiarava di avere fiducia nei media, contro solo il 15% dei repubblicani, fonte: *Gallup*), in Italia fra la destra e il M5S rispetto alla sinistra. Una recente indagine del Pew Research Center ha rilevato che negli Stati Uniti, dove le *fake news* sono un argomento fortemente divisivo - il Presidente Trump ha annunciato provocatoriamente la proclamazione dei "*Fake news Awards*" da lui stesso selezionati - solo il 56% dei cittadini si fida dei media[13]. La riduzione della fiducia nei media rende i cittadini più incerti e più facilmente catturabili da strategie d'ingannevolezza (o *deception*), basate sulla diffusione di concetti ambigui che mescolano deliberatamente elementi di verità e falsità. Non a caso il termine post-verità (*Post-Truth*), originariamente definito da Keyes[14], è stato eletto dall'Oxford *Dictionary*

[11] L'esempio più eclatante di confusione mista a divertimento generata da una *fake news* in Italia è la pagina su Facebook pubblicata durante la campagna elettorale del 2012 e subito diventata virale, attribuita all'inesistente senatore Cirenga, in cui si sosteneva che il Parlamento aveva appena approvato una legge da lui proposta (con 257 voti favorevoli e 165 astenuti), che stanziava 134 mld€ in favore dei deputati che non sarebbero stati rieletti. In coda alla pagina era chiaramente indicato trattarsi di uno scherzo: «E' solo colpa del popolo caprone che l'ha votata ma che ha soprattutto condiviso questa immane boiata falsa che solo dei boccaloni come voi potevano reputare vera», ma ciò non ha impedito un diluvio di commenti seri e indignati da parte dei suoi lettori. Cfr. W. Quattrociocchi – A. Vicini, *op. cit.*, 29 ss.

[12] *Il re delle fake news in cattedra alla Sapienza: «Ma non ci ho mai guadagnato, mi interessa l'aspetto educativo»*, Repubblica.it, 1 marzo 2018.

[13] Cfr. N. McCarthy, *Where People Think The News Is Accurate, Statista*, 17 January 2018.

[14] R. Keyes, *The Post-Truth Era: Dishonesty and Deception in Contemporary Life*, New York 2004.

parola dell'anno 2016. La post-verità è un'affermazione ambigua che non essendo né verità né del tutto falsa, crea un ambiente ricettivo per le *fake news*. Queste ultime sono deliberatamente costruite per confondere i lettori, e ciò pone seri problemi tecnici e semantici per individuarle. Il contenuto delle *fake news* è diverso dalle notizie ordinarie sia per argomento, stile e tipo di piattaforma utilizzata, e tenta di distorcere la verità con una pluralità di stili linguistici, mentre contemporaneamente prende in giro le notizie vere, volutamente presentate come dubbie. Al fine di supportare una tesi non basata su fatti, l'autore di *fake news* usa tipicamente un'evidenza vera, posta però all'interno di un contesto falso[15].

La sesta ragione è il meccanismo di diffusione e condivisione delle informazioni sui SN, messo in luce nel lavoro seminale di Lerman, Yan e Wu[16], peculiare e molto diverso rispetto a quello dei media tradizionali. Sui SN, la maggioranza degli utenti tende a fidarsi più della cerchia di amici di cui fa parte e a credere ciò che questi riferiscono, meno delle notizie diffuse dagli altri grandi media. Ciò genera un meccanismo perverso – la cosiddetta illusione della maggioranza – che fa apparire ai loro occhi come prevalente e condivisa da gran parte della propria cerchia un'opinione, anche la più assurda, espressa in realtà da una ristretta minoranza, solo perché chi la sostiene è molto ben collegato con loro e col resto della rete.

Nel secondo paragrafo le *fake news* sono analizzate all'interno della più generale strategia dell'ingannevolezza che sembra caratterizzare molti settori dell'economia e della società civile, messi a rischio dai politici che adottano l'approccio della post-verità. Nel terzo è descritto e discusso il meccanismo di illusione della maggioranza sui SN. Nel quarto paragrafo vengono identificate le principali caratteristiche dell'offerta (chi le produce e perché) e della domanda (come sono percepite e utilizzate dai consumatori) delle *fake news*, alcune delle quali distintive rispetto agli altri beni d'informazione presenti sul mercato. Il quinto paragrafo analizza gli effetti negativi che le *fake news* possono produrre sul benessere sociale e sulla democrazia, mentre nel sesto sono presentati i risultati di uno studio che ha provato a stimarne gli effetti sulle recenti elezioni presidenziali negli Stati Uniti.

Il settimo paragrafo discute i possibili interventi di politica, nessuno dei quali, preso isolatamente, sembra in grado di contrastare efficacemente gli effetti negativi delle *fake news*. E' piuttosto dal versante degli incentivi di mercato, accompagnato da misure di stimolo ad un maggior coordinamento fra tutti i soggetti interessati, che possono provenire soluzioni in grado di minimizzare i danni sociali da queste provocati. Seguono le conclusioni.

2. L'economia dell'ingannevolezza

Nel loro libro *Phishing for phools*, Akerlof e Shiller[17] descrivono e analizzano tutte le

[15] K. Shu - A. Silva - S. Wang - J. Tang - H. Liu, *op. cit.*

[16] K. Lerman - X. Yan - X. Wu, *The Majority Illusion in Social Networks*, USC Information Sciences Institute, California, 17 February 2016.

[17] G. Akerlof - R. Shiller *Phishing for Phools*, *op. cit.*, 163 ss.

situazioni in cui un certo soggetto, il pescatore (o *fisherman*) compie azioni per cui i pescati (o *phools*) si comportano in modo da perseguire il suo interesse e non il loro. "*Phool*" è un individuo che, per qualsiasi ragione, viene ingannato e catturato con successo dal pescatore[18]. Ci sono due tipi di cattura: quella informativa e quella psicologica, oggi largamente applicate a mercati diversi, come la finanza, il tabacco e l'alcool, il *marketing*, le proposte d'investimento, la pubblicità e, naturalmente, la politica. Il primo tipo di cattura deriva dall'asimmetria informativa fra pescatore e pescato, quella psicologica dal sapiente uso da parte del pescatore di concetti, fatti e racconti preconfezionati che suscitano nel pescato emozioni, spesso non percepite come tali, che lo fanno finire nella rete.

Gli economisti tendono a ricondurre il malfunzionamento di un certo mercato alla presenza di esternalità non compensate o a un'iniqua distribuzione del reddito: secondo il pensiero economico tradizionale le inefficienze riscontrate, anche quelle dei mercati dell'informazione, sarebbero risolvibili intervenendo su queste due cause. Akerlof e Shiller, invece, ritengono che, a causa della presenza e della pervasività delle strategie d'inganno, non si possano separare in modo chiaro i mercati che funzionano da quelli che non funzionano: tutti, anche quelli più competitivi, sono soggetti a rischi di *phishing*, perché l'ingannevolezza inerisce con i caratteri dell'uomo reale. La scienza economica fa fatica a comprendere che l'inganno e il raggiro sono sistematici e non episodici.[19] I due premi Nobel fanno l'analogia con il cancro: solo in alcuni limitati casi è causato da agenti esterni come virus, batteri o sostanze cancerogene (cui è effettivamente possibile porre rimedio con appropriati vaccini, terapie o politiche di risanamento ambientale), mentre nella stragrande maggioranza dei casi è attivato da fattori endogeni, gli stessi che ci fanno stare in salute. Il cancro sviluppa una mutazione delle nostre cellule che, come quelle sane, dispongono anch'esse di difese contro gli attacchi esterni. Le cellule cancerose sono molto resistenti agli attacchi, perché nel cancro la nostra fisiologia benigna si estende alle cellule maligne. Ecco l'analogia con l'ingannevolezza e le *fake news*: applicate ai mercati che teoricamente funzionerebbero bene se tutti fossero pienamente informati, colpiscono inesorabilmente quelli che fra noi sono ingenui e/o disinformati.

L'ingannevolezza nel mercato dell'informazione, di cui le *fake news* rappresentano l'applicazione più estrema, è un fenomeno legato alla natura dell'emozione che una certa notizia suscita in chi parla, scrive, ascolta o legge. Se dal lato dell'offerta – chi genera e diffonde la notizia – si nasconde una deliberata strategia di *phishing*, la domanda ne viene inevitabilmente condizionata, spesso in modo decisivo. Akerlof e Shiller insistono sul concetto di equilibrio, diverso se i mercati sono soggetti o meno a strategie d'inganno.

La fattispecie che qui ci interessa approfondire è l'effetto delle strategie d'ingannevo-

[18] Il termine "*fish*", coniato nel 1996 dall'Oxford *English Dictionary* in riferimento al web, denotava originariamente solo i comportamenti fraudolenti on-line. Akerlof e Fisher ne allargano la denotazione a tutti i comportamenti d'ingannevolezza dei soggetti economici e politici.

[19] Fanno eccezione R. Coase, *The market for goods and the market for ideas*, in *American Economic Review*, vol. 64, 2, papers and proceedings, 384 ss., e O. Williamson, *The Economic Institutions of Capitalism. Firms, Markets, Relational Contracting*, New York, 1986, tr. it. *Le istituzioni del capitalismo*, Milano, 1987, che hanno indagato l'opportunismo nella regolazione dei mercati e nelle relazioni contrattuali.

lezza sulla politica, simile anche se non identica a quello che esse creano sui mercati dei beni e servizi. La teoria economica della democrazia, originariamente formulata da Downs[20], sostiene che in politica esiste un equilibrio paretiano nelle competizioni elettorali, di cui l'elettore mediano è l'ago della bilancia. L'elettore mediano è il soggetto rappresentativo posto al centro della distribuzione delle preferenze dei cittadini per una certa politica, ad esempio la riduzione delle tasse. Alla sua sinistra ci sono coloro che, con intensità crescente man mano che ci si sposta a sinistra, non desiderano tagliare le tasse perché non vogliono ridurre la spesa pubblica; alla sua destra coloro che, sempre con intensità crescente, vogliono invece ridurre insieme tasse e spesa pubblica. Due candidati, uno di sinistra e l'altro di destra, si fronteggiano nella competizione elettorale. Entrambi cercano di includere nei loro programmi quello preferito dall'elettore mediano: chi dei due schieramenti ne ottiene il consenso, raggiunge la maggioranza dei voti e vince le elezioni. La ricerca dell'appoggio dell'elettore mediano consiste nel sottile bilanciamento dei suoi interessi da includere nel programma elettorale, tutti in gran parte conosciuti e decisivi per vincere. Il programma scelto e le preferenze dell'elettore mediano costituiscono quindi il punto d'equilibrio delle competizioni elettorali.

L'analisi di Downs è basata sull'ipotesi di perfetta informazione, che non vale mai nel mondo della post-verità. Se entra in gioco l'inganno, secondo Akerlof e Shiller cambiano le strategie dei candidati, che possono trovare conveniente accrescere in modo voluto quella degli elettori, proponendo messaggi semplici, banali e confondenti che però suscitano in loro emozioni. Gli elettori, così come i consumatori, sono catturabili anche psicologicamente attraverso storie preconfezionate, come quella, descritta dai due autori, del candidato repubblicano del Iowa al Senato che nello spot televisivo elettorale compare sul trattore a rasare il proprio prato, come un vicino qualsiasi: lo spot non parla mai di programmi elettorali, ma genera nell'ascoltatore emozioni e meccanismi di identificazione con il candidato attraverso un racconto costruito ad arte[21]. Così l'inganno modifica l'equilibrio paretiano, perché allontana i programmi dei candidati dalle preferenze dell'elettore mediano.

In sostanza, le *fake news* e, più in generale, le strategie d'ingannevolezza, sostituiscono gli elettori con i consumatori, e la classe politica con le imprese[22]. La sostituzione è resa possibile dal doppio ruolo del cittadino che come elettore dovrebbe esprimere consensi politici razionali basati sulle informazioni disponibili, ma come consumatore di queste stesse informazioni è in realtà esposto alle strategie di marketing utilizzate

[20] A. Downs, *An Economic Theory of Political Action in a Democracy*, in *Journal of Political Economy*, vol. 65, 1957, 135 ss.

[21] Akerlof e Snower hanno studiato l'importanza della narrazione *phishing* sul consenso politico. Il caso da loro analizzato è la manipolazione negli anni Venti da parte del partito comunista sovietico, ottenuta attraverso il racconto, risultato convincente per il popolo russo, che attribuiva alla mancanza di collaborazione dei *kulaki* (i piccoli proprietari di terre) la responsabilità della carestia, che causò milioni di morti. La vera ragione della carestia, invece, era dovuta al fallimento del sistema pianificato centralmente che non prevedeva alcun incentivo alla produzione, perché il prodotto eccedente la quota assegnata veniva semplicemente requisito, così che tutti producevano solo il minimo necessario, e un qualsiasi fattore esterno impediva di raggiungere l'obiettivo prefissato dallo stato. Cfr. G. Akerlof - D. Snower, *Bread and Bullets*, *CESIFO working paper* no. 5747, category 13: Behavioural Economics, February 2016.

[22] Oxera, *The policy of truth? Deception in markets and in public policy*, *Oxera Agenda*, April 2017.

dalle imprese che le producono. Queste, facendo leva su elementi psicologici diversi dalla razionalità, generano in lui sentimenti, reazioni e apprezzamenti tipici del consumatore di prodotti. I politici, spiazzati nel loro ruolo tradizionale di aggregatori di consenso basato sulla mediazione degli interessi, diventano a loro volta consumatori perché acquistano servizi d'informazione emozionali, potenzialmente attraenti per il loro elettorato, da imprese specializzate che ne sostituiscono implicitamente la funzione.[23] Questo schema interpretativo predice che i politici che hanno fatto in passato, o fanno attualmente, uso di strumenti d'ingannevolezza fra cui le *fake news*, tenteranno sia di occultare le prove dei loro acquisti sia di difenderne i produttori, specie se finanziati da soggetti terzi. E' questo, ad esempio, il caso delle interferenze russe rilevato in occasione di elezioni e referendum in alcuni paesi occidentali.

La strategia elettorale vincente del candidato pescatore con elettori pescabili, spiegano Akerlof e Shiller, è basata su tre distinti momenti: 1) pubblicamente, il candidato formula programmi e proposte cui il tipico elettore è sensibile e ben informato 2) sui temi in cui l'elettore è male informato - tipicamente quelli che interessano i finanziatori della sua campagna e i gruppi d'interesse organizzato di cui cerca di ottenere il consenso - il candidato li appoggia di fatto senza però diffonderne la notizia tra il suo elettorato; 3) utilizza i finanziamenti ricevuti dai gruppi d'interesse che l'appoggiano per aumentare la sua popolarità fra la popolazione generale disposto a votarlo perché apprezza le sue storie preconfezionate (rasa il prato in TV).

Il candidato pescatore può usare efficacemente anche la tecnica estrema dell'*hate speech*. Questo strumento, definibile come qualsiasi discorso o scritto abusivo o minaccioso che esprime pregiudizi contro un gruppo particolare in base alla razza, religione o orientamento sessuale, suscita in chi l'ascolta forti emozioni, soprattutto se di basso livello culturale, e funziona se il candidato pescatore lo adatta selettivamente al suo elettorato, già predisposto a recepirlo. Ad esempio, attribuire ai migranti africani o mediorientali la causa del terrorismo e la diffusione di malattie è un tipico *hate speech phishing* che, rinforzando le convinzioni degli elettori già maldisposti verso gli stranieri immigrati, sottende una relazione di complicità, emozione e reciprocità tra pescatore e pescato, accomunata da forti sentimenti negativi preconcetti contro i migranti e gli stranieri.

Il meccanismo della cattura si accresce all'aumentare del grado di apprezzamento e di fiducia del consumatore/elettore per un certo media. Il web, almeno fino ad oggi, non seleziona contenuti, non cura il controllo redazionale, non offre servizi di *fact-checking*, ossia procedure di controllo e segnalazione della veridicità dell'informazione e della sua fonte. All'utente è stato fino ad oggi demandato il compito di verificare l'attendibilità di ciò che legge. I SN, dove le notizie sono preconfezionate e sintetizzate, riducono di molto i costi di ricerca del consumatore, ma quest'ultimo, così facilitato, non si rende conto di essere stato selezionato o ghettizzato nella fornitura della notizia, e finisce per incontrare i propri simili, trasformando il SN in uno specchio che alimenta e rafforza le polarizzazioni[24]. Sul web s'incontra la verità che già si conosce, e si evitano le occasioni

[23] Un esempio italiano di tale inversione dei ruoli è Casaleggio & Associati che gestisce e governa i siti del M5S.

[24] C. Sunstein, *Why Nudge? The Politics of Libertarian Paternalism*, Yale 2014.

di confronto con ciò che non si conosce o che non ci somiglia. Favorendo gli scambi tra gruppi, i SN tendono a polarizzare le opinioni e gli estremismi[25].

3. I meccanismi di diffusione delle informazioni sui social network

La tendenza degli utenti dei SN a segregarsi per gruppi ideologicamente omogenei non è un fenomeno casuale, bensì una conseguenza della struttura delle loro reti di amici. Gli utenti dei SN, stante la diffusa ignoranza sui fatti del mondo reale, tendono a fidarsi di ciò che sostiene l'amico appartenente alla loro cerchia, perché lo ritengono erroneamente più informato di loro. Ciò favorisce la formazione di opinioni, spesso assurde, condivise dalla cerchia di amici, che a tutti appaiono sostenute da una maggioranza che in realtà non è tale. Quest'effetto è stato definito da Lerman, Yan e Wu[26] *il paradosso dell'amicizia*.

Il paradosso dell'amicizia dipende dal fatto che in media, gran parte della gente ha meno amici di quanti non ne abbiano questi ultimi. Nonostante che questa affermazione non abbia alcun senso logico, è in realtà ampiamente utilizzata in diversi contesti, ad esempio dagli epidemiologici per scoprire la diffusione precoce di un'epidemia. Il paradosso suggerisce di monitorare i contatti e gli amici di un certo individuo, perché questi hanno maggiore probabilità di avere contatti con terzi, non solo quindi di ammalarsi ma soprattutto di infettare gli altri. Un altro esempio del paradosso è quello del consumo di alcool. Se i forti bevitori di alcolici sono anche molto conosciuti e popolari, la maggioranza dei cittadini che in qualche modo li conosce si convince erroneamente che i propri amici bevano più di loro.

Il meccanismo del paradosso è oggi applicato con successo da alcune tecniche di marketing sui SN, fra cui il cosiddetto *social shopping*, in cui le aziende che investono in pubblicità cercano di stimolare una discussione fra un gruppo di amici su certi prodotti o servizi, di cui questi scambiano le loro esperienze di consumo. Il social shopping fa aumentare del 25% il numero di ordini sul carrello per gli acquisti on-line e di ben il 50% del valore medio dell'ordine[27].

Un punto critico del paradosso emerge quando viene utilizzato per prendere decisioni politiche, perché genera il meccanismo che Lerman, Yan e Wu chiamano l'illusione della maggioranza, un problema per la democrazia che nei prossimi anni – si pensi ai meccanismi di scelta dei candidati sul web del M5S in Italia - potrebbe diventare molto serio.

Per spiegarlo si consideri, come esempio, una rete di SN composta da 13 individui (mostrata nelle fig.1 e 2).

---

[25] A. Nicita, *E' possibile il libero scambio nel mercato della verità?,* in *Il Foglio*, 13 gennaio 2017.

[26] K. Lerman – X. Yan - X., Wu, *op. cit.*

[27] S. Guo - M. Wang - J. Leskovec, *The Role of Social Networks in Online Shopping: Information Passing, Price of Trust, and Consumer Choice, ACM Conference on Electronic Commerce 2011*, arXiv:1104.0942v1, 2011.

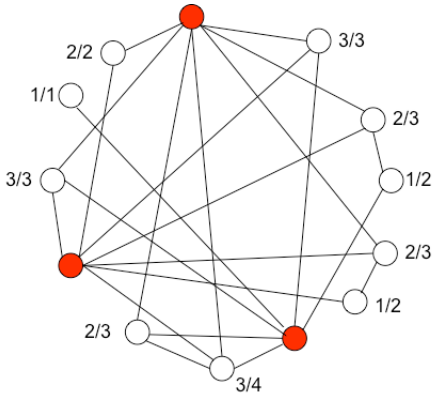


Figura 1 – esempio di rete non selettiva di social network

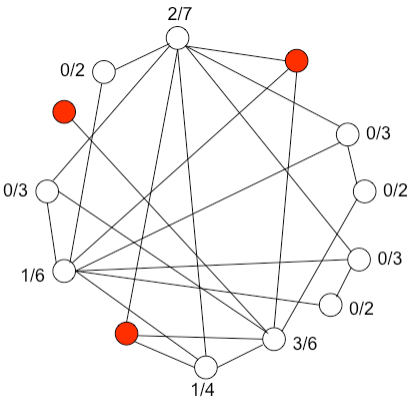


Figura 2 – esempio di rete selettiva di social network

La fig. 1 presenta il caso in cui tre soggetti *attivi* (segnati in rosso), ossia quelli che diffondono una certa informazione sulla rete del SN, poniamo ad esempio un falso e ingiustificato allarme sui rischi della vaccinazione contro il morbillo che causerebbe l'autismo, dispongono anche di molti legami con gli altri membri. Questi soggetti sono in grado di influenzare gli altri dieci (in bianco nella figura, cosiddetti *inattivi*) che hanno meno legami con il resto della rete e che ritengono vera l'informazione diffusa solo se chi glie l'ha trasmessa ha un contatto diretto con loro. Ad esempio il soggetto in alto a destra è inattivo e dispone solo di tre legami con altri membri del SN, stabiliti esclusivamente con soggetti attivi. A lui in particolare, ma anche ad altri tre soggetti nelle medesime condizioni di dipendenza dalle informazioni diffuse dagli attivi, la falsa informazione sulla dannosità della vaccinazione per il morbillo appare vera perché sostenuta dalla maggioranza dell'intero *network*, anche quando in realtà non lo è.

La rete descritta nella fig. 1 è definibile come *non selettiva*, perché i tre soggetti attivi, pur rappresentando solo il 23% (sono 3 su 13) dei membri della rete del SN, controllano il 77% (20 su 26) dei legami complessivi degli inattivi. Ciò consente loro di condizionare l'opinione di ben 9 membri. Pertanto, sia all'interno che all'esterno della rete, il loro messaggio, che sappiamo essere in realtà fake, appare espresso dalla maggioranza del SN.

Poniamo ora il caso che i soggetti attivi nella diffusione della *fake news* non siano più quelli del caso precedente, ma altri tre (fig. 2, segnati in rosso). In questo caso gli attivi, avendo pochi legami, controllano solo il 18% (7 su 38) di quelli totali e quindi non riescono a raggiungere la maggioranza dei consensi. Se diffondessero una falsa informazione non verrebbero creduti dalla maggioranza, perché la rete è diventata ora *selettiva*. Tutto dipende dal numero dei legami posseduto dai soggetti attivi.

Proviamo ora a vedere cosa succede se, tornando al caso della fig. 1 con gli attivi che raccolgono la maggioranza dei consensi, i tre soggetti passivi (che nella fig. 2 sono invece attivi) cambiano opinione sui presunti rischi della vaccinazione perché, ad esempio, si sono informati presso le autorità sanitarie o i centri epidemiologici dell'evidente falsità scientifica di tale tesi e dei pericoli per la salute pubblica che essa comporta. Diventando anch'essi attivi, cercano di diffondere la corretta informazione sul SN. Tuttavia, dispongono di pochi legami perché la rete è per loro selettiva, e quindi, pur essendo portatori di informazione (peraltro corretta) non riescono ad influenzare in modo decisivo la maggioranza degli aderenti alla rete. Ipotizzando che essi riescano a

convincere gli altri soggetti inattivi con cui hanno legame diretto, ma non quelli che in precedenza avevano diffuso la falsa notizia dei pericoli della vaccinazione: riescono a far cambiare opinione solo ad un altro soggetto (quello posto più in basso della rete), conquistando solo il 16% (3 su 19) dei legami degli inattivi. Le corrette informazioni sono così comprese e accettate da una minoranza degli aderenti, solo 4 su 13, pari al 31,7%. Gli altri membri, ignari dei fatti e condizionati dagli attivi con molti legami, continuano a credere che ci siano seri rischi connessi alla vaccinazione del morbillo.
Da questo esempio emerge chiaramente l'importanza strategica per chi diffonde informazioni su un SN, compresi quindi i produttori di *fake news*, di conoscerne ex-ante la struttura della sua rete, in modo da condizionarne la diffusione. Il reperimento e la gestione dei Big Data diventano così gli strumenti con cui si può dominare il consenso degli utenti sui SN. Questi ultimi sono particolarmente a rischio di credere alle *fake news*, come indicano i dati della seguente tab.1, che mostra come negli Stati Uniti le visite ai siti di *fake news* provengano in misura prevalente (41,8%) dai SN, a fronte solo del 10% per quelle ricevute dai maggiori siti di news. Chi riesce a condizionare i SN con una certa *fake news*, ottiene una cassa di risonanza (*l'echo chamber*) che finanzia e accresce i siti dove questa è stata creata.

Tab. 1 Visite dei siti d'informazione negli Stati Uniti per fonte
- valori percentuali medi pesati per il n. di visite mensili -

	visite dirette sul sito	visite da link terzi	visite dai motori di ricerca	visite dai social media
Siti importanti di news (n=690)	48,7%	10,6%	30,6%	10,1%
Siti di fake news (n=65)	30,5%	5,7%	22,0%	41,8%

fonte: Alexa (da Allcott e Gentzkow, 2017)

4. I produttori di *fake news*

È importante capire chi sono le imprese che producono *fake news* e perché lo fanno. *BuzzFeed* e *the Guardian* hanno scoperto che più di 100 siti che hanno pubblicato *fake news* rivolte al mercato statunitense erano tutti gestiti da adolescenti residenti in una piccola città, Veles, in Macedonia[28]. Il sito *Endingthefed.com*, responsabile di quattro fra le più popolari *fake news* su Facebook, è stato creato e gestito da un rumeno[29]. L'azienda americana *Disinfomedia* è proprietaria di molti siti di *fake news*, e impiega circa 20 dipendenti che producono notizie false[30].

[28] S. Subramanian, *Inside the Macedonian Fake-News Complex*, in *Wired*, 15 February 2015.

[29] T. Townsend, *The Bizarre Truth Behind the Biggest Pro-Trump Facebook Hoaxes*, Inc., 21 November 2016.

[30] L. Sydell, *We Tracked Down a Fake-News Creator in the Suburbs. Here's What We Learned*, in *National Public Radio*, 23 November 2016.

BuzzFeed ha recentemente svolto uno studio su 60 siti italiani e diverse pagine Facebook di proprietà di Web365, società a conduzione familiare, composta secondo il suo proprietario da sei persone più un team di giornalisti[31]. La pagina Facebook del principale sito del network di Web365 - Direttanews.it - conta circa 3 milioni di Like, e secondo il software di analisi *CrowdTangle* ha ottenuto nell'ultimo anno più di 5 milioni di condivisioni dei suoi articoli[32].

Le motivazioni a produrre *fake news* possono essere economiche, ideologiche o psicologiche.

Dal punto di vista economico, l'obiettivo dei produttori di notizie false è realizzare profitti con la pubblicità rivolta a chi va sui loro siti web. Ad esempio gli adolescenti di Veles, che hanno prodotto *fake news* sia a favore di Donald Trump che di Hillary Clinton, in occasione delle elezioni presidenziali del 2016 hanno guadagnato decine di migliaia di dollari[33]. Paul Horner ha dichiarato di aver creato *fake news* a favore di Trump per ricavare profitti nonostante sostenesse di essere personalmente un suo oppositore[34].

La seconda motivazione è ideologica. Alcuni produttori di *fake news* sostengono di aver iniziato la loro attività per aiutare Trump[35], altri per combattere con tutte le armi disponibili lo schieramento politico avversario. Il New York Times[36] cita rapporti che mostrano come la Russia abbia creato numerosi falsi siti e gruppi su SN per diffondere storie false in occasione delle elezioni presidenziali. Nell'epoca del web e dei SN, chi si sente politicamente schierato rischia di attivare, anche involontariamente, meccanismi di disinformazione su notizie di cui ignora l'origine.

La terza motivazione è di ordine psicologico. Quattrociocchi e Vicini[37] spiegano che il *meme*, abbreviazione del termine greco *mímēma*, imitazione, ovvero un pezzo di informazione che si replica come i virus passando da un utente all'altro, si diffonde attraverso la condivisione e i Like ed è sempre a rischio di eccessiva semplificazione, che tende a renderlo inesatto. La diffusione di un *meme* è un'azione che ha una profonda motivazione narcisistica in chi l'ha pubblicato. Quest'ultimo riceve una gratificazione psicologica crescente all'aumentare dei Like e delle richieste di condivisione ricevuti, che aumenta ulteriormente se il *meme* è una fake, perché il *phishing* ha funzionato.

I produttori di *fake news* presentano due caratteristiche distintive rispetto ai tradizionali fornitori di informazioni. La prima è che non fanno investimenti per produrre notizie

---

31 C. Brunelli, *Dalle fake news al copia-e-incolla, il network italiano delle bufale*, in *La Repubblica*, 21 novembre 2017.

32 La strategia comunicativa di Web365 è di attrarre click attraverso titoli sensazionalistici come «*Incredibile. 10 minuti e il tumore sparisce*», che mescolano articoli, post e *fake news* facendo leva sui sentimenti anti-immigrati ("Germania, la Merkel parla e gli immigrati hanno in mano la città" "Birmingham, la città più islamizzata si prepara per il Natale") e sulla presunta censura dei principali mass media (molte fake provengono da una pagina intitolata "Quello che i TG non dicono").

33 S. Subramanian, *op. cit.*

34 C. Dewey, *Facebook Fake-News Writer: I Think Donald Trump is in the White House because of Me*, in *The Washington Post*, 17 November 2016.

35 T. Townsend, *op. cit.*

36 New York Times, *Fake news and the Internet Shell Game*, in *New York Times*, 28 November 2016.

37 W. Quattrociocchi - A. Vicini, *op. cit.*

accurate, così che il loro prodotto è, il più delle volte, avulso da fatti accertati. La seconda è che non tentano di costruirsi una buona reputazione, ma solo massimizzare i guadagni derivanti dai click ricevuti nel brevissimo periodo sulla singola falsa notizia. Queste aziende attraggono domanda (ossia click) sia perché i consumatori non sono in grado di distinguere fra notizie di qualità e notizie false, sia perché costruiscono volutamente *fake news* ritagliate per fornire utilità psicologica ai consumatori che appartengono allo specifico gruppo o schieramento politico o ideologico a cui sono rivolte. Di fronte ad eventuali censure o chiusure di siti o pagine postate da parte dei gestori delle piattaforme, sono in grado di rispondere rapidamente sia creando subito nuovi siti o post, sia modificando sottilmente i contenuti fake posti come titolo di una notizia o fatto veri[38] attraverso il tipico uso di un linguaggio scurrile che però suscita indignazione o anche semplice divertimento.

Ciò significa che ci troviamo di fronte ad un bene d'informazione spesso apprezzato e che ha un suo proprio mercato: come la prostituzione o la droga, vietarlo o classificarlo come falso o illegittimo non impedisce che non venga consumato comunque, anzi il semplice divieto rischia di rinforzare falsi convincimenti nei consumatori. Finora i gestori dei SN, inizialmente impreparati ad identificare le *fake news* anche perché beneficiari del traffico addizionale, appaiono oggi riluttanti a diffondere informazioni sui ricavi pubblicitari di tale segmento distorto del mercato. Non sono infatti disponibili dati (che pure sarebbe facile ricostruire) sull'ammontare dei fatturati generati dai produttori di *fake news*, e le evidenze empiriche esistenti rimangono necessariamente confinate all'aneddotica e a singoli casi.

5. Domanda e offerta delle *fake news*

Gentzkow, Shapiro e Stone[39]hanno costruito un modello economico teorico sulla domanda e offerta di informazioni per spiegare i comportamenti dei soggetti (consumatori che si informano, politici candidati, media) di cui ci interessa capire l'applicazione rispetto alle *fake news*. Il punto centrale del loro modello, peraltro originariamente identificato da Mullainathan e Shleifer[40], è che i consumatori presentano nella loro funzione di utilità due parametri diversi, fra loro in conflitto: da un lato l'incentivo personale a ottenere dai media informazioni corrette e complete, dall'altro il beneficio psicologico derivante dal trovare confermate dalle notizie ricevute le loro opinioni personali, spesso basate su preconcetti e semplificazioni in un mondo sempre più difficile da interpretare.

I media tradizionali vogliono fornire informazioni di elevata qualità – raccontare i fatti in modo oggettivo e imparziale - per attrarre consumatori in modo da ottenere una

[38] Ad esempio, l'azienda Web365 ha ripreso completamente la notizia pubblicata da *La Repubblica* «*Pensioni, la Cgil boccia anche l'ultima proposta del governo: Mobilitazione il 2 dicembre*», cui ha aggiunto come titolo introduttivo «*Camusso sfancula gentiloni sulle pensioni*».

[39] M. Gentzkow - J. Shapiro - D. Stone, *Media Bias in the Marketplace: Theory,* in S. Anderson - J. Waldfogel - D. Stromberg (eds.) *Handbook of Media Economics*, vol. 1B, Chap. 14, Amsterdam 2016.

[40] S. Mullainathan - A. Shleifer, *The Market for News*, in *American Economic Review,* 95:4, 2005, 1031 ss.

buona reputazione. Tuttavia, essi possono derogare a tale comportamento virtuoso quando i loro lettori o ascoltatori ricevono informazioni frammentarie sullo specifico fatto di loro interesse. In tal caso faticano ad identificare i fatti reali selezionandoli fra l'enorme mole di notizie disponibili, e quindi finiscono col preferire non i media che nella situazione di informazione chiara, completa e circostanziata godono di buona reputazione, ma quelli che, come i SN, pubblicano informazioni semplici e preconfezionate che confermano le loro opinioni personali, da cui traggono, come già osservato, un significativo beneficio psicologico. Il modello di Gentzkow, Shapiro e Stone spiega che in equilibrio, quando domanda e offerta con tali caratteristiche si incontrano, si genera un certo ammontare di informazioni volutamente distorte.

Recenti contributi dell'economia comportamentale mostrano che il meccanismo decisionale dell'individuo utilizza, spesso contemporaneamente, due diversi sistemi cognitivi:[41] il primo (che chiamiamo sistema 1) è quello razionale, conscio, costruito su regole e procedure, ma lento nella sua applicazione; il secondo (sistema 2) è quello intuitivo, basato sulle nostre sensazioni (istinti, riflessi, modi di essere), spesso inconscio, ma anche rapido. Se nelle decisioni usassimo esclusivamente il sistema 1 non riusciremmo ad affrontare il mondo, perché per risolvere gran parte dei problemi quotidiani abbiamo bisogno di scelte rapide e di scorciatoie (chiamate anche *euristiche*). Tuttavia, il sistema 2 è soggetto a distorsioni. Fino ad oggi si assumeva che il mercato dell'informazione fosse basato sul sistema mentale 1, quello razionale, sia da parte dei produttori di notizie, vincolati al rispetto di poche e semplici regole deontologiche, sia dei consumatori, che sceglierebbero le notizie usando il loro lato razionale. La moltiplicazione delle *fake news* mostra invece che i consumatori, favoriti dai bassi costi di ricerca, scelgono sui SN le notizie usando il loro lato emotivo, così che anche l'offerta tende ad adeguarsi alla mutata domanda. Il problema è ulteriormente aggravato dalla presenza, comune fra gli utenti dei SN, di un meccanismo mentale noto in psicologia, il cosiddetto *realismo naïve*, che li porta a ritenere come unica e vera la loro percezione della realtà, mentre quella degli altri sarebbe quasi sempre disinformata, irrazionale o distorta[42].

6. Gli effetti delle *fake news* sulla collettività

La presenza di *fake news* sul mercato delle informazioni ha diverse implicazioni negative sul benessere sociale. I consumatori che confondono notizie false e vere si creano opinioni personali non accurate, che riducono le esternalità sociali positive, fra cui in primo luogo la capacità dei cittadini di utilizzare l'informazione per selezionare in occasione di elezioni candidati di elevata onestà e competenza. Inoltre, come osservato da Thaler e Sunstein[43], lasciare al cittadino la libertà di cambiare la propria opinione in relazione all'accuratezza delle notizie ricevute dai media è un valore sociale importante

[41] R. Thaler, *Misbehaving: The making of behavioural economics*, chapter 4, London 2015.

[42] A. Ward - E. Ross - T. Reed - E. Turiel - T. Brown, *Naive realism in everyday life: Implications for social conflict and misunderstanding*, in E. S. Reed - E. Turiel - T. Brown (eds.) *Values and knowledge*, Mahwah, 1997, 103 ss.

[43] R. Thaler - C. Sunstein, *Libertarian Paternalism*, in *American Economic Review*, 93, 2003, 175 ss.

da preservare e difendere. Tale valore è completamente annullato dall'interazione fra *fake news* e visione politica polarizzata, che rende più difficile la condivisione fra i cittadini su quali siano i problemi sociali più importanti da affrontare e quali gli strumenti da adottare per risolverli.

Proprio l'incapacità del consumatore di distinguere notizie vere da quelle false quando è esposto alle *fake news*, lo rende facilmente disposto ad accettare credenze false o distorte. Tuttavia, non è solo l'informazione ad essere distorta dalle *fake news*, bensì anche il modo con cui il consumatore interpreta e risponde agli stimoli del mondo reale: lo allontana dalla ragione per avvicinarlo al fuoco delle passioni negative, come rabbia, paura, indignazione perché le notizie false vengono esplicitamente create per confonderlo e spingerlo verso i politici più abili a catturarne il consenso e a rafforzarne lo scetticismo nei confronti degli altri media, che subiscono un effetto di spiazzamento, specie fra i giovani[44]. È stato rilevato che la *fake news* più popolare su Facebook sulla campagna presidenziale del 2016 ha avuto una diffusione per contatti raggiunti di gran lunga superiore a quella della più importante notizia vera pubblicata sui principali media tradizionali[45].

Fra i sentimenti negativi stimolati dalle *fake news* c'è l'indignazione che, come osservato da Santambrogio[46], è una reazione per un torto o un'ingiustizia subìti, cui è associata l'idea di malafede da parte di chi li ha commessi. Ci si indigna solo con chi commette scientemente un'ingiustizia spacciandola per un alto ideale. Stimolare con false notizie l'indignazione in politica implica quindi un abbassamento del livello di autocontrollo del target insieme alla squalificazione degli avversari politici, accusati di imbrogliare le carte. E' uno strumento molto efficace nell'odierna competizione politica, simile e complementare alla strategia della post-verità, che non a caso ha dato il nome ad un partito in Spagna che ha avuto un notevole successo elettorale. Ma non è nuovo, e per questo è socialmente ancora più pericoloso, perché nascosto in una memoria collettiva che potrebbe sempre riemergere. Il suo antenato storico, infatti, era la capacità di demagoghi, governanti o personaggi pubblici di aizzare la folla contro un certo avversario, spingendola talvolta anche al suo linciaggio.[47] Gli *hate-speech* di oggi sul web innescati da fake, fanno riferimento proprio all'idea di una possibile giustizia sommaria, in cui lo Stato non esiste. Scatenando nei pescati i peggiori istinti, li soddisfa virtualmente, ma li predispone anche a passare all'azione.[48]

Il pericolo delle *fake news* non è percepito in modo simile nei diversi paesi. Nella fig. 3 è mostrata, per dieci paesi, la percentuale di coloro che si mostrano fortemente o solo incidentalmente preoccupati della difficoltà di distinguere sul web il vero dal falso (fonte: indagine BBC World 2017). Negli Stati Uniti e nel Regno Unito, dove le *fake news* han-

[44] J. Wakefield, *Social media 'outstrips TV' as news source for young people*, in *BBC News*, 15 June 2016.

[45] Wikipedia, *Fake news,* 2017.

[46] Cfr. M. Santambrogio, *L'odio degli indignati da fake news*, in *Il Sole 24 Ore, Domenica*, 3 settembre 2017

[47] Ancora nella tranquilla Olanda di fine Seicento, gli orangisti riuscirono, con opportuni racconti *fake*, a far linciare da una folla inferocita il matematico Johan de Witt, che per vent'anni aveva governato il paese con grande senso di tolleranza e moderazione.

[48] É questa, probabilmente, una delle possibili concause della recente tentata strage a Macerata di cittadini di colore presi a caso.

no indubbiamente condizionato, probabilmente in modo non decisivo ma comunque avvertibile, la compagna presidenziale e il referendum sulla Brexit, la percentuale dei cittadini seriamente preoccupati dai contenuti falsi apparsi sul web è inferiore a quella del Brasile, Grecia, Francia e Spagna, dove le fake non sono (ancora) state esplicitamente utilizzate per condizionare le elezioni. Russia, Cina e Turchia, dove sussistono serie limitazioni alla libertà d'informazione e a gravi forme di violenza nei confronti dell'opposizione, il pericolo è attualmente percepito solo da una minoranza di cittadini.

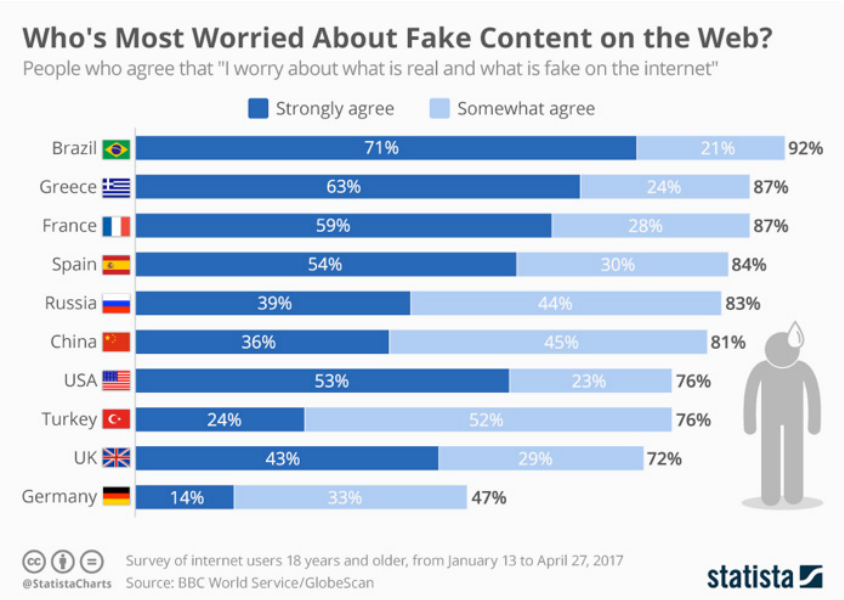


FIGURA 3 I TIMORI DEI CONTENUTI FAKE SUL WEB DEI CITTADINI DI 10 PAESI

Gli italiani, non compresi nel campione dell'indagine BBC, sono particolarmente esposti ad essere ingannati dalle *fake news*, perché la loro capacità di comprensione e analisi dei testi scritti è particolarmente bassa, come misurato dal tradizionale studio OCSE multipaese del 2013[49], in cui l'Italia è all'ultimo posto nella graduatoria fra i paesi esaminati. Su una scala da 1 a 5, ben il 42% degli italiani risulta al livello 2, che indica una capacità di navigare sul web e trovare le informazioni collegandone due o più parti, ma di fare inferenze solo di basso livello, e addirittura il 27,7% non sa fare neanche questo (è al livello 1).

Fra i colpiti dalle *fake news* c'è anche l'industria pubblicitaria, preoccupata dagli effetti negativi prodotti da queste e dalle frodi pubblicitarie sulle decisioni di investimento degli inserzionisti nei media digitali[50]. Il 2016 ha registrato un incremento del traffico sul web, in parte dovuto alle elezioni presidenziali americane, ma anche alle *fake news*. La presenza diffusa di notizie false comporterà – stimano gli analisti - un atteggiamento più prudente da parte degli investitori nella spesa sugli spazi pubblicitari dei siti web, e un aumento dei costi per garantire agli utenti maggiore qualità delle inserzioni, che non

[49] OECD (2013) OECD Skills Outlook 2013, Books, OECD iLibrary.

[50] R. Katz, *Russia, an Ad Conundrum. Study finds distrust of social ads in wake of political fracas*, in *eMarketer*, 21 November 2017.

tutti sembrano disposti a pagare: ne risentiranno inevitabilmente i ricavi pubblicitari, che si aggiusteranno al ribasso. Se non saranno prese misure adeguate, l'industria pubblicitaria si aspetta uno spostamento degli investimenti verso i media non digitali. Non è quindi solo la democrazia ad essere distorta dalle *fake news*, ma anche la competizione intermediale, perché l'industria digitale più innovativa, che ha trovato nel modello di business pubblicitario la fonte di finanziamento del web, appare ancora impreparata di fronte alla loro imprevista e larga diffusione.

7. L'influenza delle *fake news* sui risultati elettorali delle elezioni presidenziali USA e le interferenze sulle elezioni 2018 in Italia

Alla luce dell'importanza politica e sociale delle *fake news*, alcuni commentatori hanno sostenuto che, se queste non avessero avuto un'ampia diffusione, Donald Trump, indubbiamente favorito rispetto a Hillary Clinton grazie al più elevato numero di fakes in suo favore, non sarebbe divenuto Presidente degli Stati Uniti[51]. Il timore di interferenze nelle elezioni si è estesa in diversi paesi fra cui il Regno Unito in occasione del referendum sulla Brexit, ed oggi anche alle elezioni politiche in Italia.

Allcot e Gentzkow[52] hanno provato a misurare l'impatto delle *fake news* sui risultati elettorali. A tal fine hanno costruito un complesso set d'informazioni, comprendente un data base con le 156 più importanti *fake news* relative alle elezioni (41 a favore di Clinton, 156 pro-Trump) con le relative condivisioni ricevute su Facebook, un'indagine online su 1200 soggetti intervistati nei tre mesi precedenti le elezioni, e una seconda indagine successiva alle elezioni, sempre online su 1208 soggetti, in cui si chiedeva se l'utente ricordasse alcune fra le più importanti *fake news* pubblicate, mescolate con altre sia vere sia specificamente inventate per l'indagine e quindi mai apparse sui media (queste ultime con la funzione di placebo). In questa seconda indagine venivano poste alcune domande sulle caratteristiche demografiche (età, sesso, livello d'istruzione, razza/etnia, classe di reddito), politiche (affiliazione politica prima della campagna 2016, voto alle elezioni presidenziali), di consumo delle informazioni (tempo dedicato a leggere, ascoltare o vedere in tv informazioni sulle elezioni e in particolare sui SN, fonti d'informazione utilizzate).

Dall'indagine campionaria è emerso che solo il 13,8% degli intervistati ha utilizzato i SN come fonte d'informazione primaria per le elezioni (tab.2)[53].

[51] H. Parkinson, *Click and Elect: How Fake news Helped Donald Trump Win a Real Election*, in *The Guardian*, 14 November 2016; M. Read, *Donald Trump Won because of Facebook*, in *New York Magazine*, 9 November 2016; C. Dewey, *op. cit.*

[52] H. Allcott - M. Gentzkow, *Social Media and Fake news in the 2016 Election*, in *Journal of Economic Perspectives* 31(2), 2017, 211 ss.

[53] I dati della tab. 2 differiscono in modo significativo da quelli della precedente tab. 1 relativamente ai SN. Tale differenza sembra riflettere proprio la maggiore concentrazione delle *fake news* sui SN rispetto a quella rilevata e/o percepita sugli altri media.

Tab. 2 Principale fonte d'informazione utilizzata dai cittadini negli Stati Uniti nella campagna presidenziale 2016

Fonte d'informazione	
TV via cavo	23,5%
Network televisivi nazionali	19,2%
Siti web	14,8%
TV locali	14,5%
Social Networks	13,8%
Stampa	8,0%
Radio	6,2%

Usando la differenza fra notizie vere, *fake news* e notizie placebo, Allcot e Gentzkow hanno stimato il tasso di esposizione dei consumatori alle *fake news*: mediamente ogni cittadino americano durante il periodo elettorale ha letto 1,14 *fake news* apparse sul web (siti e/o SN). Utilizzando un modello statistico probit, i due autori hanno verificato se siano rilevabili differenze fra repubblicani e democratici nel credere ad una *fake news* o a notizie vere[54].

I repubblicani hanno un tasso di risposta corretta più alto dei democratici sulle notizie vere, ma credono anche di più alle *fake news*[55]. I democratici sembrano invece più scettici nei confronti delle notizie in generale. Questo risultato non cambia se si introducono altre variabili esplicative quali l'età, il livello d'istruzione e il tempo speso per informarsi sui media (predittori di un'elevata probabilità di risposta giusta), o i SN come principale fonte d'informazione, i cui utenti hanno contemporaneamente alta probabilità di rispondere correttamente se la notizia è vera ma anche alta probabilità di ritenere vera una *fake news*.

La conclusione cui giungono Allcot e Gentzow è molto prudente: nonostante un avvertibile effetto delle *fake news* sulle opinioni dei consumatori, non sembra aver influito se non in modo marginale sull'esito delle elezioni, per almeno tre motivi. Il primo è che l'esposizione alle *fake news* è quantitativamente simile a quella di una serie addizione di spot elettorali, che spostano il voto per meno dello 0,02%[56]. Il secondo è che l'analisi svolta non ha potuto tenere conto del contenuto specifico di ogni singola notizia falsa e della sua specifica capacità di confondimento: non tutte le *fake news* sono uguali. Il terzo è che l'accentuata polarizzazione, già presente nell'elettorato, fa si che chi è pescato con una notizia falsa, essendo comunque predisposto ideologicamente in un senso o

[54] I primi hanno una maggiore probabilità di ritenere vera la *fake* che Obama non è nato negli Stati Uniti, i secondi che Bush è stato complice con l'attentato dell'11 settembre. Cfr. D. Cassino - K. Jenkins, *Conspiracy Theories Prosper: 25% of Americans Are "Truthers"*, Fairleigh Dickinson University's Public Mind Poll, 17 January 2013.

[55] In Italia è stato rilevato un fenomeno simile: gli elettori di centro-destra e quelli del M5S sono più esposti e credono di più alle *fake news* di quelli di centro-sinistra. Cfr. I. Diamanti, *Fake news sul web, metà degli italiani si sente beffata*, in *La Repubblica*, 17 dicembre 2017.

[56] J. Spenkuch - D. Toniatti, *Political Advertising and Election Outcomes*, *CESifo Working Paper Series*, 5780, 2016.

nell'altro, ha verosimilmente già deciso per chi votare.[57] Ovviamente, chi utilizza i SN come principale o unica d'informazione, diventa il target mirato delle *fake news*, specie se giovane e con basso livello d'istruzione, perché per lui la probabilità di trovare opinioni diverse dalle sue nel ristretto e segregato gruppo di amici è minima, ed è mal disposto a fidarsi delle informazioni dei media tradizionali.

Se l'influenza delle *fake news* sulle elezioni politiche americane è ancora argomento aperto di discussione, forti evidenze provenienti dagli studi più recenti mostrano che queste concorrono direttamente a polarizzare l'opinione pubblica. Non sarebbero dunque solo una conseguenza della polarizzazione, ma al contrario una sua causa scatenante. Un recente studio svolto dall'Internet Institute dell'Università di Oxford nei tre mesi precedenti il discorso 2018 del Presidente Trump sullo stato dell'Unione evidenzia, infatti, una netta diversità nel tasso d'isolamento e nella vicinanza rispetto ai siti di *fake news* fra gli ultraconservatori sostenitori di Donald Trump e il resto degli utenti classificati da algoritmi di AI in gruppi d'affiliazione politica. I risultati dello studio, definito dal *Financial Times*[58] ad oggi il più completo ed esaustivo sul rapporto fra *fake news* e SN, sono sintetizzati nella fig. 4.

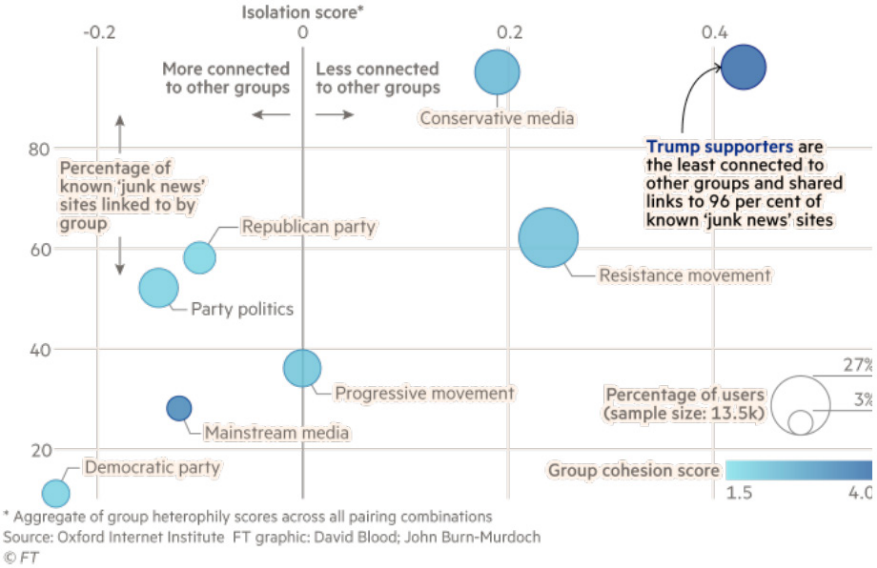


FIGURA 4 DIMENSIONE, TASSO D'ISOLAMENTO E DISTANZA DAI SITI DI *FAKE NEWS* DEI GRUPPI DI AFFILIAZIONE POLITICA SU TWITTER NEI TRE MESI PRECEDENTI IL DISCORSO DI TRUMP SULL'UNIONE

Ciascun gruppo d'affiliazione politica è analizzato lungo due dimensioni. La dimensione orizzontale (*isolation score*) definisce quanto ciascun gruppo è collegato o dialoga con gli altri. Il gruppo più isolato in assoluto sono i sostenitori di Trump, seguito dai movimenti di resistenza (come *Occupy*) e dagli utenti dei media conservatori. La dimensione verticale, invece, definisce il tasso di link con cui ciascun gruppo risulta collegato con

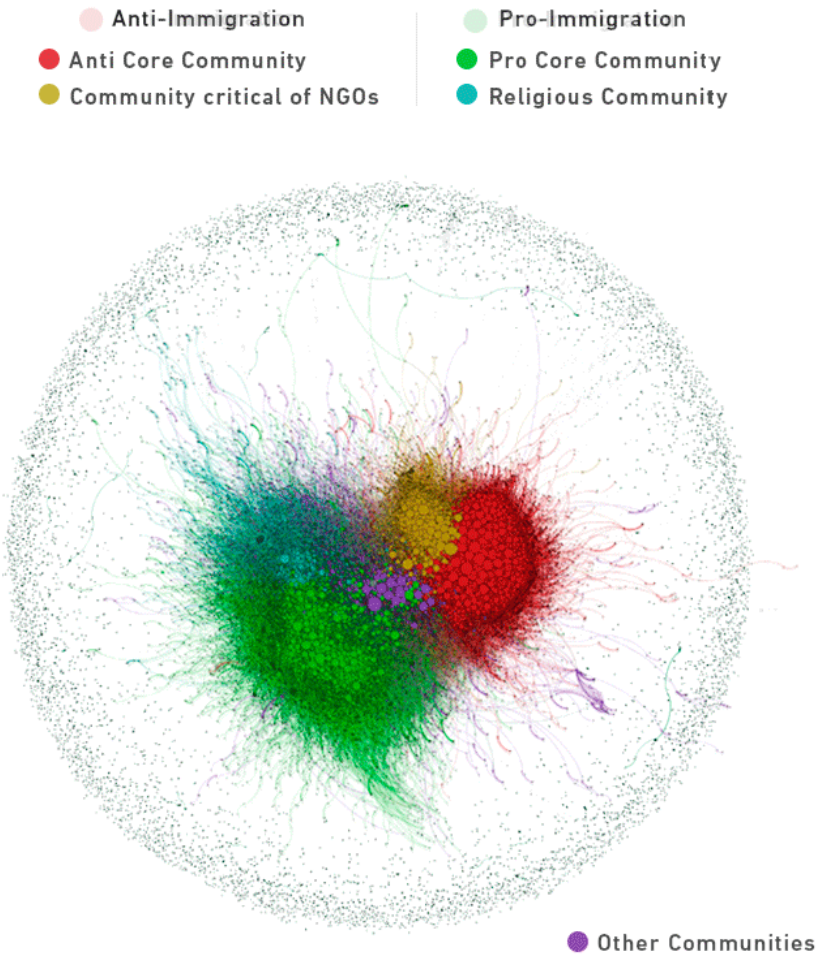
[57] Quest'opinione è condivisa da Alexander Nix, CEO di Cambridge Analitica, società di psicografica che ha lavorato per la campagna elettorale di Donald Trump. Cfr. M. Butcher, *Cambridge Analytica CEO talks to TechCrunch about Trump, Hillary and the future*, in *Techcrunch.com*, 6 November 2017.

[58] Hard right dominates use of fake US news, Oxford study finds, in FT, 11 February 2018.

noti siti di junk news (che includono *fake news*, notizie sensazionalistiche, estremiste, cospirative, commenti mascherati, ecc.). Qui di nuovo i sostenitori di Trump sono il gruppo più collegato a tali siti: il 96% ne condivide i contatti, mentre fra i democratici il collegamento è addirittura inferiore a 20%. Questo fenomeno suggerisce che nei periodi non elettorali le *fake news* vengono utilizzate per rafforzare, quasi esclusivamente nello schieramento conservatore, l'identità polarizzata ed autoreferenziale dei suoi appartenenti. Lo schieramento democratico/progressista, invece, sembra subire il loro effetto negativo senza riceverne alcun beneficio in termini di consenso.

Uno studio, condotto dalla società di ricerca Alto che utilizza un software simile a quello di Google indicizzando per rilevanza i contenuti e le fonti nelle discussioni[59], ha recentemente analizzato, nel periodo 1 febbraio-31 luglio 2017, più di 1 milione di commenti generati da 98 mila utenti di Twitter che discutono sull'immigrazione in Italia. Anche in questo caso si conferma la polarizzazione estrema del dibattito, in cui gli utenti anti-immigrati, inferiori per numero rispetto a quelli pro-immigrati (17mila contro 35mila), risultano però molto più attivi (in media 26,5 contro 5,4 tweet per utente). La fig. 5 visualizza i dati sulle opinioni polarizzate degli utenti sul tema, con due comunità contrarie agli immigrati, due favorevoli, e un 15% di indecisi.

FIGURA 5 VISUALIZZAZIONE DELLE INTERAZIONI FRA GRUPPI D'OPINIONE SULL'IMMIGRAZIONE IN ITALIA



[59] www.alto-analytics.com/en_US/the-construction-of-anti-immigration-messages-in-italy/

La narrativa scambiata dagli anti-immigrati, rilanciando la classica associazione immigrazione-insicurezza-crimini-terrorismo (cui si aggiungono in alcuni casi teorie cospirative), ha avuto come fonti d'informazione, oltre a notizie locali, soprattutto i siti Sputnik Italia e Russia Today, le cui notizie fake o pseudo propagandistiche ("Nel 2065 la quota di immigrati potrebbe rappresentare il 40% della popolazione totale", "Bill Gates esorta a salvare l'Europa dagli immigrati", "Immigrazione, meglio essere senza cuore che perdere la propria Patria") sono state rilanciate dal 90,4% agli utenti anti-immigrati[60]. Le evidenze dell'interferenza russa risultano quindi confermate.

8. Cosa fare?

Il problema è quindi come intervenire sulle *fake news* con adeguati strumenti, capaci di aiutare i consumatori a inferire con corrette informazioni i veri fatti del mondo. Il politico che utilizza la strategia della post-verità adotta una retorica che sottostima le evidenze oggettive e un linguaggio che lo avvantaggia, costruito unicamente sul proprio interesse, in conflitto con quello di lungo periodo dei cittadini. Questo comportamento è molto simile a quello delle aziende che confondono i consumatori con una sofisticata strategia di arbitraggio, consistente nell'invogliarli ad accettare subito un'offerta allettante che però implica alti costi successivi che il consumatore scopre solo in ritardo, quando è ormai vincolato dentro la relazione contrattuale e non gli è più conveniente uscirne (è quindi *locked-in*). In equilibrio, tutte le imprese finiscono con l'adottare questa strategia che sfrutta l'ingenuità del consumatore, e quindi il classico rimedio antitrust è rendere questa strategia illegale. In politica, però, ciò non è possibile perché, come già osservato da Coase[61], economisti, giuristi, editori e politici hanno sempre sostenuto che il mercato della libera espressione delle idee, a differenza di quello dei beni e servizi, non presenta i tipici fallimenti di mercato perché il cittadino è il miglior giudice di ciò che trova sui media. Secondo Coase, invece, è un paradosso ritenere che l'intervento pubblico sia inutile e sbagliato nel mercato delle idee ma desiderabile in quello dei beni e servizi. Entrambi i mercati, pur essendo soggetti a rischi di opportunismo o di decisioni interessate da parte dei regolatori, richiedono misure *ad hoc* se si è in presenza di fallimenti di mercato, in special modo se, come nel nostro caso, le distorsioni sono dovute ad asimmetria informativa.

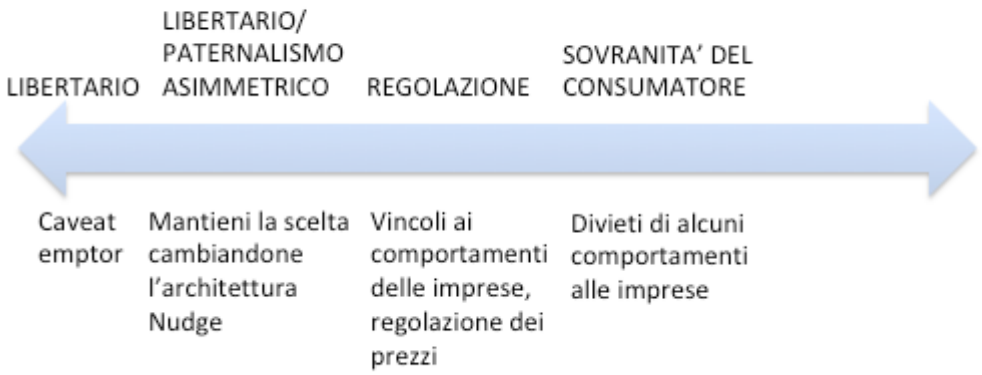
La post-verità spinge il cittadino-elettore a capovolgere il suo normale processo di scelta politica. Se sono un elettore razionale, cerco prima di pesare le evidenze che mi arrivano dalle informazioni reali sul mondo (fase descrittiva), per poi sviluppare la mia posizione rispetto all'offerta politica (fase normativa, che implica la creazione di un'idea su *come le cose dovrebbero andare*). Nel mondo della post-verità, invece, gli elettori sono spinti direttamente ad apparentarsi ad uno schieramento politico, per poi sceglie-

[60] Alto ha rilevato anche la presenza di falsi *fact-checker*: sul sito anti-immigrazione Vox News è scritto che la fonte delle informazioni dei post è verificabile cliccandoci sopra, ma i link rimandano sempre o ad altri siti anti-immigrati (fra cui principalmente "Tutti I Crimini degli Immigrati", di cui Vox News è emanazione) o alle pagine Facebook di associazioni politiche come Casa Pound.

[61] R. Coase, *op. cit.*

re i fatti che lo confermano, ignorando quelli che lo mettono in dubbio (distorsione della fase descrittiva). Un altro modo di vedere il problema è che la post-verità orienta i cittadini ad utilizzare in politica il loro lato emotivo (sistema 2) e ad escludere quello razionale (sistema 1). Il linguaggio adottato diventa lo strumento rilevante per generare la distorsione: si stimola il lato emotivo degli elettori usando termini semplici come *grande*, *cattivo*, *noi*, *loro*, ecc., escludendo domande su *cosa pensano* di un certo problema, spesso complesso e dagli esiti incerti, e sostituendole con quelle che chiedono loro *come si sentono* rispetto a quello stesso problema. Anche la ripetizione di un messaggi[62], indipendentemente dalla sua verità, implica che esso è creduto vero, perché nella nostra mente la familiarità si associa con la verità[63]. Il problema è ulteriormente complicato dalla presenza sui SN di due tipiche figure di utenti, sempre più frequenti nei ceti sociali tormentati dalla disoccupazione o inoccupazione, i cosiddetti *troll* e i *debunker*.[64]
Oxera[65] ha classificato i diversi strumenti disponibili lungo un'ideale linea d'intensità crescente d'intervento regolatorio (fig. 6).

FIGURA 6 LO SPETTRO DEGLI INTERVENTI SULLE FAKE NEWS



Fonte: Oxera (2017)

Lo schema proposto ricalca il ventaglio degli strumenti utilizzati nella regolazione pubblica dei mercati quando falliscono perché soggetti ad asimmetria informativa, comprendenti interventi sia sulla domanda che l'offerta.
A sinistra dello spettro la filosofia libertaria classica che, giudicando le *fake news* semplicemente fatti che accadono normalmente nella realtà[66], ritiene non necessario alcun

[62] Ad esempio, twittare continuamente storie nuove innesca il cosiddetto meccanismo della *disponibilità a cascata*, che fa apparire come certi, importanti e frequenti eventi che in realtà non lo sono. Cfr. T. Kuran - C. Sunstein, *Availability Cascades and Risk Regulation*, in *Stanford Law Review*, 51:4, 1999, 683 ss.

[63] W. Moons - D. Mackie - T. Garcia-Marques, *The impact of repetition-induced familiarity on agreement with weak and strong arguments*, in *Journal of Personality and Social Psychology*, 96:1, 2009, 32 ss.

[64] I primi cercano deliberatamente la facile rissa verbale con commenti compulsivi e provocatori, i secondi agiscono da smascheratori seriali, opposti e simmetrici rispetto ai primi, pretendendo ossessivamente di ristabilire con il loro intervento la realtà delle cose. Entrambi interagiscono con le *fake news* in modo opportunistico, aumentando la confusione nei lettori che ne leggono i commenti o post. Cfr. W. Quattrociocchi - A. Vicini, *op. cit.*

[65] Oxera, *op. cit.*

[66] V. Zeno-Zencovich, *Fake news, un falso problema perché non esistono 'notizie vere'*, in *Key4Biz*, 28 novembre 2017.

tipo d'intervento (*Caveat emptor,* ovvero ci pensi il consumatore a tutelarsi). Il mercato delle informazioni sarebbe quindi in grado di autoregolarsi[67]. Questa sembra essere l'opinione, non espressa ma di fatto supportata, da Donald Trump che ne ha verosimilmente beneficiato ai fini elettorali, anche se probabilmente in modo non decisivo.
Spostandoci sulla destra segue il paternalismo libertario asimmetrico, proposto da alcuni economisti comportamentali,[68] che ritiene che quando i consumatori - in questo caso anche elettori - non agiscono nel loro interesse perché soggetti a distorsioni causate dalle emozioni che governano le loro scelte, siano da preferirsi interventi soft (*nudges*, o "aiutini") che alterano le opzioni disponibili senza cambiare la loro libertà di scelta: i soggetti che si comportano in modo irrazionale vengono aiutati, con piccoli interventi mirati, a prendere decisioni più consapevoli, ma si lascia piena libertà agli altri. Peraltro, il paternalismo libertario si avvale dei medesimi concetti della post-verità: giudica inevitabili le distorsioni cognitive connesse alle emozioni generate dalle informazioni e richiede l'adozione di misure di contro-inganno, della stessa natura delle *fake news*. Il problema è che, proprio su queste ultime non c'è accordo fra i decisori pubblici, comprese le autorità di regolazione, su quali debbano essere tali interventi selettivi, e se questi possano essere realmente efficaci.
Al centro del ventaglio delle opzioni troviamo l'approccio economico tradizionale, che considera le *fake news* e la disinformazione da queste generata una tipica forma di fallimento di mercato, che richiede gli interventi tipici utilizzati nella regolazione ex-ante ed ex-post. Tale approccio è concettualmente condiviso da Pollicino[69], secondo cui la protezione dei cittadini europei contro le *fake news*, accordata dall'art. 10 della Convenzione Europea e dall'art. 11 della Carta dei Diritti Fondamentali dell'Unione Europea, enfatizzando la dimensione passiva di essere informati in modo pluralistico, crea spazi per interventi pubblici in un mercato, come quello di Internet, caratterizzato da numerosi fallimenti di mercato.
Gli interventi di regolazione nel mercato delle idee non possono però essere trattati allo stesso modo di quelli adottati nel mercato dei beni e servizi – già nel 1974 Coase[70] metteva in guardia contro tale semplificazione – perché nel nostro caso le azioni antitrust sulla sola offerta potrebbero non essere né necessarie né sufficienti. Un tipico errore di questo tipo è la tesi sostenuta dal sito Vox[71], secondo cui le *fake news* sarebbero una conseguenza della dominanza monopolistica di Google e Facebook negli algoritmi di ricerca. Tali piattaforme, pur non essendo direttamente interessate a diffonderle, non avrebbero però incentivi sufficienti ad individuarle, filtrarle correttamente o ad escluderle: un mercato delle ricerche più competitivo, secondo tale interpretazione, amplierebbe verosimilmente l'offerta con nuovi algoritmi capaci di selezionarle e combatterle. L'intervento proposto da Vox presenta due serie debolezze. La prima è che

[67] Per una critica a tale tesi, fondata sull'antinomia fra scarsità di tempo a disposizione del consumatore per informarsi e quasi illimitata disponibilità di informazioni sul web, cfr. O. Pollicino, *Fake news, Internet and Metaphors (to be handled carefully*) in *questa Rivista*, 2017, 23 ss.

[68] R. Thaler - C. Sunstein, *op. cit.*

[69] O. Pollicino, *op. cit.*

[70] R. Coase, *op. cit.*

[71] Vox, *Why "fake news" is an antitrust problem*, 23 November 2017.

propone interventi sulla sola offerta, mentre i problemi sociali più seri delle *fake news* riguardano la domanda. La seconda è che considera gli algoritmi di ricerca i principali responsabili della loro diffusione, ipotesi smentita dai dati della precedente tab.1, secondo cui solo il 22% dei contatti ricevuti dai siti di notizie false derivi da risultati dei motori di ricerca, contro il 41,8% dei SN. In realtà, la funzione di ricerca assume un ruolo funzionale ed economico molto diverso a seconda del tipo di piattaforma. Costituisce il cuore del business nel mercato delle ricerche generaliste (Google, Yahoo! e Bing) dove la competizione è interamente basata sulla bontà ed efficacia dei risultati ottenuti dagli utenti collegati alla pubblicità, altrettanto efficace.[72] Al contrario, sui SN come Facebook o Twitter o sui portali specializzati come Amazon, Ebay, EDreams o YouTube, la funzione di ricerca è soprattutto uno strumento pratico messo a disposizione dell'utente per aiutarlo a trovare ciò che cerca, essendo la competizione in tali mercati incentrata non sulla ricerca, ma sulle modalità di fruizione dei contenuti (su Facebook, facilità di trovare gli amici e ciò che questi scrivono, sui portali specializzati gli specifici prodotti o servizi domandati). Intervenendo con azioni ex-post antitrust solo sugli algoritmi – che non sono di per sé responsabili della diffusione delle *fake news* – la proposta, oltre ad essere inefficace, finisce inevitabilmente per distorcere la competizione intermediale.

Preoccupati dai rischi di riduzione della rilevanza delle inserzioni pubblicitarie dovute alla presenza di *fake news* Google, Microsoft e Facebook hanno recentemente annunciato la fornitura di servizi di *fact-checking*. Nel weekend del 17 dicembre 2017 Google ha aggiornato le linee guida che i siti web devono rispettare per essere mostrati in Google News, il suo servizio d'informazione. D'ora in poi i siti di notizie «non devono rappresentare in modo fuorviante, travisare o nascondere informazioni sulla proprietà o sulla finalità principale e non devono intraprendere attività coordinate allo scopo di ingannare gli utenti». Come esempio Google cita «i siti che rappresentano in modo ingannevole o nascondono il proprio Paese di origine e sono rivolti agli utenti di un altro Paese sulla base di false premesse».

Tuttavia il problema non può certo dirsi risolto, perché le procedure di *fact-checking* assumono che il consumatore sia razionale e disponibile a farsi rieducare. Infatti, molti utenti dei SN, nonostante i *warning,* continuano a leggere le *fake news*, rinforzando anzi le loro convinzioni circa una generale e pervasiva distorsione ingannevole del mondo dell'informazione, da cui credono erroneamente di uscire ghettizzandosi ancora più sui SN[73]. Pennycook e Rand[74] giungono alle medesime conclusioni. Essi hanno osservato, attraverso esperimenti svolti su campioni di più di settemila consumatori, che l'aggiun-

[72] Cfr. V. Visco Comandini, *Google e i mercati dei servizi di ricerca su Internet*, in *Mercato Concorrenza Regole*, 2013, 541 ss.

[73] Cfr. B. Nyhan - J. Reifler, *When Corrections Fail: The Persistence of Political Misperceptions*, in *Political Behavior*, 32:2, 2010, 303 ss. I due autori hanno svolto un esperimento su un campione di studenti di orientamento politico conservatore. Ai soggetti veniva richiesto di leggere *fake news* che includevano sia una tesi ingannevole espressa da un politico, sia la stessa tesi corredata dall'indicazione che si trattava di un falso. I risultati hanno mostrato che la presenza dell'indicazione spesso non riduce l'errata percezione ma anzi l'accresce. Quando una nuova informazione contraddice l'opinione già formatasi nella mente dei soggetti, questi semplicemente la sovracompensano con contro-argomentazioni.

[74] G. Pennycook - D. Rand, *Assessing the effect of "disputed" warnings and source salience on perceptions of fake news accuracy*, SSRN-id3035384, 15 September 2017.

ta di un avviso (*tag*) con il logo dell'editore su di un certo articolo, che dichiara controversa la veridicità della notizia in esso contenuta, non ha alcun impatto sull'accuratezza dei giudizi espressi dai consumatori che l'hanno letto. Al contrario, si rileva la presenza di un effetto di "fiducia implicita" da parte dei sostenitori di Trump e dei giovani con meno di 26 anni, che fa loro sembrare le *fake news* non contrassegnate dal tag sempre credibili e accurate. L'etichetta posta accanto ad una *fake news*, che indubbiamente è una forma di *nudge* (aiutino), non sembra educare il consumatore a sviluppare un atteggiamento critico, ma anzi in presenza di accentuata polarizzazione lo abitua ancor più a non porre la necessaria attenzione a distinguere e selezionare il vero dal falso.

Più decisi gli interventi annunciati recentemente da Facebook per impedire che soggetti esterni provino ad inquinare la democrazia interferendo sui normali processi democratici. Facebook dal gennaio 2018 offrirà ai suoi iscritti un nuovo strumento per scoprire se negli ultimi mesi hanno seguito, verosimilmente senza rendersene conto, i falsi account creati dalla *Research Agency Internet* tra gennaio 2015 e agosto 2017, periodo in cui gruppi vicini al governo russo avevano tentato di manipolare l'opinione pubblica in vista delle elezioni presidenziali comprando pubblicità sul SN di *Menlo Park*[75]. Una simile indagine è in corso anche sul referendum per la Brexit[76].

Facebook sembra essersi reso pienamente conto degli effetti potenzialmente dannosi delle *fake news* sul proprio business: ha recentemente deciso[77] di ridurre l'esposizione passiva dei suoi utenti alle notizie del suo servizio *News Feed*, riducendone i *link* e i video e aumentando lo spazio delle conversazioni fra utenti. Facebook ha anche implementato un nuovo servizio di fact-checking all'inizio del 2017[78], basato su 4 aree di intervento: 1) migliorare e rendere più semplice e trasparente la valutazione degli utenti che segnalano la presenza di bufale sul suo portale, 2) collaborare attivamente con le organizzazioni terze specializzate in fact-checking che hanno sottoscritto il *Poynter's International Fact Checking Code of Principles*,[79] 3) migliorare l'informazione degli utenti che desiderano condividere una determinata notizia, 4) escludere dalla pubblicità i siti di false informazioni o di pubblicità occulta. La procedura adottata da Facebook prevede di inviare tutte le news sospette (perché segnalate da utenti sulla base di riscontri ragionevoli) all'organizzazione competente per territorio e/o lingua aderente al codice dei principi definito da *Poynter's International*, che viene incaricata di valutarne l'autenticità. Se quest'ultima le identifica come fake, la notizia viene: i) contrassegnata come controversa, ii) collegata ad un link che spiega le ragioni di tale classificazione, iii) pubblicata ugualmente su *News Feed*, ma ponendola sempre agli ultimi posti sulla pagina, iv) esclusa dai servizi pubblicitari. Agli utenti che desiderano ugualmente condividerla con i propri amici la notizia appare comunque etichettata come controversa.

Una procedura simile, ma in cui il compito di identificazione di una *fake news* è demandato ad un team dedicato di esperti del Centro Nazionale Anticrimine Informatico

[75] F. Vendrame, *Facebook, più trasparenza sulle attività russe*, in *Webnews*, 23 Novembre 2017.

[76] *Facebook investigates Russian meddling in British politics*, in *Financial Times*, 18 January 2018.

[77] Cfr. C. Newton, *Facebook's startling new ambition is to shrink. A wild reversal comes to the News Feed*, in *The Verge*, 14 January 2018.

[78] Cfr. A. Mosseri, *News Feed FYI: Addressing Hoaxes and Fake news*, in *Facebook newsroom*, 15 December 2016.

[79] Nel gennaio 2018, 44 organizzazioni risultavano aver adottato il codice.

per la Protezione delle Infrastrutture Critiche (CNAIPIC) del Ministero dell'Interno, è stata avviata nel gennaio 2018 dal Ministro dell'Interno del governo italiano, con l'obiettivo di limitare possibili distorsioni nelle elezioni politiche di marzo[80]. Una volta accertata attraverso il software OSINT (*Open Source Intelligence*) la deliberata falsità di una notizia, la Polizia Postale provvede a diffondere l'informazione sul SN dove questa è stata pubblicata.

Se dal lato della domanda l'intervento pubblico non può quindi essere di tipo coercitivo, dal lato dell'offerta, una volta accertata la natura offensiva o di fake di una notizia, è tecnicamente possibile ottenere dal gestore delle piattaforme generaliste o social la chiusura dei siti che l'hanno divulgata, ma spesso si tratta di una misura inefficace. È proprio ciò che è accaduto in Italia, dove Facebook, sulla base di richieste motivate, ha chiuso alcuni account collegati a Web365, ma il gestore di questo network ha reagito prontamente aprendo nuovi post o siti in cui le notizie fake erano abilmente mescolate con fatti sensazionali o notizie vere. Tuttavia, c'è chi ritiene che affidare ad algoritmi l'individuazione di *fake news* rischia di trasformare chi li gestisce in un improprio "arbitro della verità"[81]. Quest'osservazione, corretta in un astratto mondo di costi di transazione nulli, apre un dilemma cui la politica e le istituzioni debbono fornire una risposta. Da un lato, infatti, senza l'uso di algoritmi l'individuazione delle *fake news* è in pratica impossibile, dall'altro i tempi lunghi di una procedura di accertamento affidata a tribunali o ad autorità pubbliche, la rendono certamente inefficace, perché in questa fattispecie la velocità di risposta è requisito essenziale per combattere il fenomeno. Come indica la sperimentazione di Facebook sopradescritta, affidare l'individuazione di notizie volutamente ingannevoli ad organismi tecnici terzi indipendenti, le cui pratiche siano validate come conformi a criteri certi, univoci e trasparenti, fra cui in primo luogo il sopraricordato codice dei principi di *Poynter's International*, appare, più che una soluzione definitiva, una scorciatoia che si spera risulti efficace nella repressione delle *fake news*.

Una diversa strategia, rispettosa dei meccanismi di mercato, è di rafforzare, con adeguati incentivi, l'alleanza fra tutti i soggetti che hanno interesse a combattere le *fake news*. Le agenzie pubblicitarie sui media digitali, come già osservato, sono seriamente preoccupate per i suoi effetti negativi, e temono che la loro presenza pervasiva riduca di molto l'efficacia e la rilevanza (per l'utente) delle inserzioni pubblicitarie *contextual display* mostrate sui siti che le pubblicano, con il rischio di un circolo vizioso che vede sempre più *fake news* pubblicate, associate ad una sempre più bassa rilevanza delle inserzioni mostrate. La migliore strategia, secondo i pubblicitari ma anche dei detentori dei diritti di proprietà intellettuale interessati a combattere le contraffazioni sul web, sembra essere quella della *whitelist*, ossia di una sorta di bollino blu assegnato ai siti che godono di una sufficiente reputazione nel fornire informazioni di qualità non false o prodotti non contraffatti, mentre l'opzione simmetrica della *blacklist* (lista dei siti "cattivi" da escludere) non sembra funzionare bene, proprio perché, come spiegato al par. 4, i siti di fakes operano nel brevissimo periodo e cambiano continuamente di nome.

[80] Cfr. L. Garofalo, *Fake news, a certificare la 'verità' la Polizia Postale*, in *Key4biz*, 19 gennaio 2018.

[81] Cfr., *Garante Privacy, l'algoritmo non può decidere sulle fake news, intervista ad Antonello Soro*, in *Key4biz*, 27 novembre 2017.

Tali interventi iniziano ad essere finanziati da fondi pubblici: il Pentagono trasferirà al *Global Engagement Center* (Gec) del Dipartimento di Stato 40 milioni di dollari per finanziare azioni volte a ridurre l'impatto della propaganda e della disinformazione operate da attori statali. Una di queste iniziative è la creazione di un Information *Access Fund* per sostenere partner pubblici e privati che lavorano per denunciare e contrastare la propaganda e la disinformazione di nazioni straniere. Alle sovvenzioni, potranno accedere gruppi della società civile, fornitori di contenuti multimediali, organizzazioni non governative, centri di ricerca e sviluppo, società private e istituzioni accademiche.
E' però necessario un maggiore coinvolgimento, non limitato al *fact-checking*, dei grandi portali come Facebook o Google, le cui metriche di misurazione dell'efficacia utilizzate sono considerate dai pubblicitari insufficienti a tenere conto di questo nuovo fenomeno. I grandi gestori dei SN temono una riduzione dei profitti dovuta ai rilevanti costi legati agli interventi contro le *fake news*. Facebook ha dichiarato che le *fake news* provenienti dai siti di (dis)informazione legati alla Russia hanno raggiunto ben 150 milioni di utenti[82]. Per combatterle prevede di assumere 10 mila nuovi addetti, raddoppiando così il numero degli addetti preposti alla sicurezza, ma scontentando i propri azionisti. Facebook e Google, nel vendere pubblicità di prodotti e servizi, fronteggiano sempre l'alternativa fra mostrare più o meno inserzioni pubblicitarie sulle loro pagine. Se mostrano più inserzioni, i loro ricavi crescono ma diminuisce la rilevanza di queste ultime, se le limitano a quelle rilevanti ottengono meno ricavi, ma mantengono alta la loro reputazione[83]. La scelta fra massimizzazione dei ricavi nel breve o nel lungo periodo – il classico problema dell'uovo e della gallina - è finora sempre stata quella di privilegiare la seconda, perché la reputazione è fattore cruciale nella competizione fra piattaforme. Fino ad oggi, però, si trattava di inserzioni relative a prodotti e servizi, non di link a siti d'informazione, da cui esse traggono profitti solo dalle inserzioni sui siti indicizzati. Come già osservato, queste piattaforme, che nell'immediato hanno beneficiato delle *fake news* in termini di maggiore traffico, rischiano di subire nel medio periodo un calo di investimenti pubblicitari. E' quindi verosimile ipotizzare che, non ostante gli elevati costi e i mugugni degli azionisti, gli *Over-the-Top* adegueranno alla strategia di lungo periodo gli algoritmi di ricerca e la pubblicazione di inserzioni pubblicitarie sui siti dubbi, e quindi cercheranno le soluzioni più adeguate al problema delle *fake news*.
Un'altra possibile misura sono le campagne informative di educazione dei cittadini, comprese le scuole, finalizzate ad aiutarli a riconoscere la sopraffazione generata dalla strategia comunicativa della post-verità. Ma anche questo strumento, chiaramente paternalistico, richiede un disegno molto attento, che in ogni caso potrebbe non essere efficace. Riprendendo l'esempio del mercato dei servizi, le campagne d'informazione e di alfabetizzazione ai servizi finanziari rivolte ai consumatori non sembrano essere in grado di modificarne i loro comportamenti distorti o irrazionali[84].
Un ulteriore strumento, a cavallo fra la sovranità del consumatore e il paternalismo classico, è la promozione di norme sociali che favoriscono comportamenti corretti nella comunicazione politica. Nel caso della post-verità, il problema si sposta sulle

[82] H. Kuchler, *Facebook counts the cost of post-truth politics*, in *Financial Times*, 27 November 2017.

[83] H. Varian, *The Economics of Internet Search*, in *Rivista di Politica Economica*, 2007, 177 ss.

[84] Oxera, *Financial (il)literacy: do consumer education programmes work?*, *Agenda*, March 2008.

azioni dei politici e sulla legittimità dei metodi che usano nelle campagne elettorali e per comunicare con i cittadini. Nel Regno Unito, un'opzione raccomandata dal *Committee on Standards in Public Life* (CSPL) è un accordo preventivo fra i partiti per l'adozione di un codice deontologico sull'informazione elettorale[85]. Tuttavia la Commissione elettorale britannica ha segnalato numerose difficoltà connesse con la sua implementazione, perché quest'organo non ha intenzione di trasformarsi in un giudice della verità, che potrebbe minare la sua indipendenza. La CSLP si è effettivamente espressa sui pericoli delle *fake news* e sulla scarsa attitudine delle istituzioni a censurare i comportamenti dei politici che le utilizzano, ma non è a oggi ancora chiaro se intende promuoverne una revisione completa, fissando standard e raccomandazioni precise.

Il mondo digitale ha oggi un problema di fondo, legato alla mancanza di trasparenza sulle notizie. Nelle grandi imprese di media che producono informazioni e notizie è possibile accertare chi ne è l'autore, e se qualcuno ritiene che queste siano false, distorte o inaccurate, è sempre in grado di risalire facilmente all'editore responsabile. Nei SN e nei grandi aggregatori come Google, invece, la provenienza ultima dei contenuti diffusi e l'algoritmo che decide cosa noi vediamo e cosa non vediamo, sono del tutto opachi. Per questa ragione la politica sta oggi tentando di intervenire con strumenti legislativi che, almeno nelle intenzioni dei proponenti, dovrebbero porre rimedio a questo problema. Tuttavia, alcuni osservatori, scettici sulla loro efficacia, ritengono si tratti più di un'operazione di marketing politico (far vedere all'opinione pubblica che il governo si occupa delle *fake news*) che di misure realmente in grado di combattere gli effetti negativi della post-verità[86].

Una proposta di legge presentata al Senato americano, *l'Honest Ads Act*, intende obbligare le piattaforme a raccogliere documenti che individuino i soggetti che stanno dietro le campagne di pubblicità politica. Tale misura regolatoria, richiedendo l'intervento umano, è però dispendiosa in termini di risorse impiegate. Facebook, Twitter e Google, preoccupate, come già osservato, per un aumento esponenziale dei costi che potrebbe incidere sulla loro redditività, stanno facendo pressioni per limitarne l'applicazione alle sole campagne politiche, che taluni vorrebbero allargare a tutte le inserzioni pubblicitarie sul web.

Una proposta di legge del tutto simile è stata recentemente presentata in Italia dal deputato Anzaldi.[87] La proposta prevede l'obbligo, per ogni sito internet accessibile al pubblico che raccolga pubblicità o finanziamenti superiori a centomila euro, di indicare in modo chiaramente visibile nella pagina iniziale titolari, proprietari e finanziatori, diretti o indiretti, indipendentemente dalla forma societaria utilizzata. Due punti di questa proposta, soprattutto informativi, non sono però chiari. Da un lato la proposta non fornisce i dati necessari a valutare se il limite finanziario previsto per attivare la misura è appropriato al fine di includere i principali siti di *fake news* e/o disinformazione. Dall'altro non presenta alcuno studio sugli effetti che tale misura dovrebbe avere

[85] Committee on Standards in Public Life, Culture, Media and Sport, *Select Committee Inquiry "Fake news"*, submission by the Committee, March 2017.

[86] H. Kuchler, *Facebook counts the cost of post-truth politics*, *op. cit.*

[87] Proposta di legge n. 4573 "Disposizioni in materia di conoscibilità degli assetti proprietari e dei soggetti finanziatori dei siti internet", presentata alla Camera dei Deputati il 5 luglio 2017.

sul comportamento dei consumatori, se cioè questi, una volta che leggono il nome del finanziatore (che non è da escludere sia un prestanome) accanto alla notizia supposta falsa, rinuncino o meno a condividerla o a trasformarla in *meme* virale.
La Germania ha recentemente approvato una legge che obbliga i SN a eliminare i contenuti falsi entro 24 ore dalla loro individuazione, con multe fino a 5 milioni di euro per le piattaforme che non si siano attivate a sufficienza nell'eliminare notizie false e contenuti inappropriati come quelli d'incitamento all'odio. Se tale misura è corretta in linea teorica, lo è certamente meno nella sua applicazione, che abbiamo visto essere problematica e costosa: rischia di essere solo un enunciato di principi di fatto inapplicabili in modo sistematico ed efficace.
Secondo altri osservatori,[88] considerata la crescente influenza dei SN e dei grandi portali aggregatori sulla diffusione delle notizie, è arrivato il momento di rivedere l'attuale normativa (nel Regno Unito, la section 230 del *Communications and Decency Act* del 1996) che li esenta dalla responsabilità per ogni genere di contenuti illegali inseriti nella rete o azioni illecite commessi dai suoi utilizzatori. Tale radicale misura, ben vista dai media tradizionali impauriti dal calo degli introiti pubblicitari dovuto alla concorrenza dei media digitali, ipotizza di assoggettare i SN e i grandi portali ad una regolamentazione simile a quella vigente per le *media company*. Tale misura, che fa parte della classe degli strumenti normativi coercitivi, implica però una condivisione con gli *Over-The-Top*, che fino ad oggi l'hanno avversata. Una sua versione soft, proposta da Bassan e Rabitti[89] è riformare la disciplina sulla responsabilità delle piattaforme, che pure risale al 2010 (*notice and take down*), da integrare con le tipologie attuali (SN e portali) non sempre riconducibili a quelle originarie, e con profili di responsabilità più incisivi che sanzionino eventuali inadempienze.
Nicita[90] ha osservato che, se nessun paese ha finora introdotto normative vincolanti contro la post-verità o le fake-news, alcuni passi in avanti sono stati fatti – con l'eccezione degli Stati Uniti – nel disciplinare l'*hatespeech*. Non si tratterebbe quindi di disciplinare o sanzionare le notizie false, ma di dichiarare illegale questo linguaggio, utilizzato sempre più spesso sul web. Secondo Nicita, lo strumento giuridico a livello internazionale è la Convenzione di Budapest sul *Cybercrime* del Consiglio d'Europa, entrata in vigore nel 2004 e ratificata dall'Italia nel 2008. L'Italia ha firmato il Protocollo nel 2011 e il 17 marzo 2015 ha approvato un ddl per la sua ratifica. In quella sede è possibile allargare il tema alle *fake news* che hanno la finalità di propagandare discorsi d'odio.
Anche l'Europa ha deciso di agire sulle *fake news*. Nell'agosto 2017 il Parlamento europeo ha adottato una risoluzione[91] in cui invita la Commissione ad analizzare nel dettaglio la situazione e il quadro giuridico attuali per quanto riguarda le notizie false e a verificare la possibilità di un intervento legislativo per limitarne la divulgazione e la

[88] Cfr. L. Barber, *Fake news in the post-factual age*, *Lecture to Oxford Alumni Festival*, *Oxford University*, 16 September 2017.

[89] F. Bassan - M. Rabitti, *I Consumatori nella social economy tra big data e fake news*, in *Astrid Rassegna* n. 274 (17/2017) dicembre

[90] A. Nicita, *op. cit.*

[91] Parlamento Europeo, Proposta di risoluzione presentata a norma dell'articolo 133 del regolamento sulla nuova task force europea contro le *fake news*, B8 0501/2017, 31 Agosto 2017.

diffusione. A tal fine la Commissione ha prodotto un rapporto sulle notizie false e la disinformazione online, redatto da un gruppo indipendente di esperti di alto livello.[92]
La sintetica rassegna qui riportata dei possibili interventi fino ad oggi proposti, fra loro piuttosto eterogenei, evidenzia la difficoltà strutturale dei decisori pubblici nel valutare sia il quadro concettuale di riferimento – manca ad oggi una tassonomia ragionata dei principi ispiratori delle misure di politica di contrasto alle *fake news* - sia gli effetti, spesso non chiaramente identificati né sufficientemente valutati, che la loro adozione può comportare. Tuttavia, fra le diverse misure proposte, quelle più interessanti e, soprattutto, praticabili, riguardano specificamente i meccanismi interni dei SN, che indubbiamente rappresentano la vera rilevante novità nel mondo dei media rispetto al passato. Proprio perché soggetti a forti effetti di rete, sia diretti che indiretti,[93] di cui godono tutti i media digitali con intensità ben superiore a quelle dei media tradizionali, i SN costituiscono il campo d'applicazione prioritario su cui è opportuno focalizzare gli interventi per limitare i danni sociali generati dalle *fake news*. La procedura adottata da Facebook ne è un chiaro esempio: affida la loro individuazione ad organismi tecnici che godono di elevata indipendenza e reputazione professionale, e contemporaneamente toglie acqua ai loro fornitori che agiscono a fini di profitto.

9. Conclusioni

I metodi dei politici che adottano la filosofia della post-verità e utilizzano *fake news* implicano una deliberata strategia d'inganno nei confronti dei cittadini, "pescati" a loro insaputa e diretti a supportare politiche che non sono rappresentano quasi mai i loro interessi reali. I pescati, però, tendono ad apprezzare le *fake news*, con cui si divertono a vedere ridicolizzati i loro avversari politici, mostrando di crederci se queste sono dirette contro questi ultimi, e anzi ne rafforzano il senso di appartenenza a gruppi polarizzati, se ne sono attratti dalla semplicità dei messaggi diffusi.
È necessario agire sia sull'offerta che sulla domanda delle *fake news*, considerato che una quota crescente di cittadini usa ormai abitualmente Facebook come principale fonte d'informazione (nel 2016, rispettivamente il 30% e il 40% nel Regno Unito e negli Stati Uniti; fonti: *Reuters Digital News Report e Pew Research Report*).
Se le misure oggi adottate o previste, prese isolatamente non sembrano essere sufficienti ad ostacolare le false credenze generate dalle *fake news*, si avverte un crescente bisogno di nuove idee e strategie supportate da robuste evidenze empiriche. Mai come in questo caso informazioni, dati e studi a supporto di qualsiasi proposta d'intervento sono essenziali, proprio per evitare i rischi, piuttosto elevati, di accrescere anziché ridurre la disinformazione fra i cittadini.

[92] European Commission, *A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation*, *Directorate-General for Communication Networks*, *Content and Technology*, 2018.

[93] Nel caso dei SN, l'effetto diretto è l'aumento del beneficio privato goduto da ciascun appartenente alla rete al crescere del numero dei suoi membri, quello indiretto sono le maggiori opportunità (positive e/o negative) ottenute da soggetti terzi all'aumentare degli iscritti alla rete. E' proprio grazie all'esistenza dell'effetto indiretto che i produttori di *fake news* riescono a realizzare profitti.

Saggi

La riforma Orlando: intercettazioni, riservatezza, diritto di cronaca

Le nuove intercettazioni tra selettività arbitraria e ridimensionamento delle garanzie difensive*

Silvia Buzzelli

Abstract

Lo scritto esamina brevemente la nuova disciplina delle intercettazioni telefoniche così come risulta dopo la c.d. riforma Orlando del 2017. In particolare, vengono messe in luce le possibili lesioni delle garanzie difensive e i relativi rischi per l'equità processuale derivanti dalla trascrizione di ciò che l'ufficiale di polizia giudiziaria (delegato all'ascolto) considera rilevante.

The essay aims at exploring the new legislative framework applicable to wiretapping, as result of the so called "Orlando Reform" approved in 2017. It focuses in particular on how the rights of defendants are negatively affected and argues that the fair balance between the prosecution and the defense is called into question in so far as a law enforcement official is put in charge with the selection of the relevant content.

Sommario

1. Tante polemiche, vari cambiamenti: e ora una riforma pericolosamente contorta. - 2. La scarsa affezione per i principi della procedura penale europea: a) il "posto" assegnato alle intercettazioni nello stadio investigativo. - 3. Segue: b) il richiamo parziale alla giurisprudenza di Strasburgo, il silenzio sulle ricadute transnazionali. - 4. Possibili punti di sofferenza: trascrizione e selettività arbitraria; diritto di difesa e svantaggi sostanziali.

Keywords: Processo penale, Riforma Orlando, Intercettazioni telefoniche, Trascrizione, Nozione di irrilevanza

1. Tante polemiche, vari cambiamenti: e ora una riforma pericolosamente contorta

Non si ha la pretesa, e nemmeno la possibilità, di ripercorrere la storia delle intercettazioni: di certo, le vicende si presentano abbastanza tormentate, al pari - se non di più - rispetto a quelle inerenti altri istituti processuali che, nel tempo, hanno subito sostanziose metamorfosi. Nel corso dei decenni sono state avanzate proposte quasi sempre arenatesi, tra mille polemiche, prima dello stadio conclusivo. La soglia di attenzione in ambito

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

dottrinario è rimasta alta[1], elevato il dibattito interno alla magistratura (concretizzatosi in circolari e linee guida)[2], persistente l'interesse mantenuto dalla classe politica.

Adesso, negli ultimi giorni dell'anno appena concluso, è arrivata - se così si può chiamare - la svolta[3] con il decreto legislativo n. 216 del 2017: dopo l'approvazione - nella seduta pomeridiana del 18 dicembre 2017 - il Consiglio dei Ministri, riunitosi il 29[4], ha dato il via libera definitivo al provvedimento preannunciato dalla legge n. 108 di giugno[5] che, al c. 82, delega il Governo ad adottare, tra l'altro, un decreto legislativo «per la riforma della disciplina in materia di intercettazioni di conversazioni o comunicazioni... secondo i principi e i criteri direttivi previsti» dal successivo c. 84.

Fa un discreto effetto dover concentrare il discorso dentro il perimetro di pochi commi, riconducibili a un unico grande articolo-onnicomprensivo, cosa del resto già rilevata da vari commentatori[6]; lo smarrimento preoccupante lo si prova non appena si incominciano a leggere le opinioni, meglio ancora, gli aggettivi scelti per qualificare le novità.

A parte gli aggiornamenti che informano sui continui sviluppi dell'*iter* legislativo - dai toni comunque anch'essi inequivocabili[7] - gli autori parlano di «meccanismo farraginoso e inutilmente complicato per tutti i protagonisti»[8], di «regole contorte» tipiche di una «riforma ambigua»[9]; stando alla nota di sei Procuratori della Repubblica si tratterebbe di «procedura macchinosa e irrealistica»[10].

---

[1] V., tra tanti, A. Camon, *Le intercettazioni nel processo penale*, Milano, 1996; L. Filippi, voce *Intercettazioni telefoniche (diritto processuale penale)*, in *Enc. dir.*, VI aggiornamento, Milano, 2002, 565 ss. In precedenza, cfr. V. Grevi, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1973, 341 ss.; G. Illuminati, *La disciplina processuale delle intercettazioni telefoniche*, Milano, 1983; G. Ubertis - V. Paltrinieri, *Intercettazioni telefoniche e diritto umano alla privatezza nel processo penale*, in *Riv. it. dir. proc. pen.*, 1979, 594 ss.

[2] Cfr. *Intercettazioni, le linee guida del CSM. La delibera approvata dal Consiglio superiore della magistratura nella seduta plenaria del 29 luglio 2016* e G. Cascini, *Intercettazioni e* privacy*: dalle circolari della Procure di Roma, Torino, Napoli soluzioni utili per il legislatore*, ambedue in *Quest. giust.*, rispettivamente 29 luglio e 19 aprile 2016; v. *Dibattito. Quale riforma per la disciplina delle intercettazioni?,* Forum con L. Filippi, G. Illuminati, G. Leo e P. Profiti, in A. Caputo (a cura di), in *Quest. giust.*, 2006, 1207 ss.

[3] D. Stasio, *Intercettazioni/2: riforma equilibrata ma senza risorse rischio boomerang*, in *Quest. giust.*, 8 gennaio 2018, 2, è dell'idea che il "decreto Orlando" abbia «valenza epocale».

[4] Cfr. i Comunicati-stampa n. 62 e 63 del Consiglio dei Ministri, in www.governo.it.

[5] Per una prima lettura della legge 23 giugno 2017, n. 103, v., M. Gialuz - A. Cabiale - J. Della Torre, *Riforma Orlando: le modifiche attinenti al processo penale, tra codificazione della giurisprudenza, riforme attese da tempo e confuse innovazioni*, in www.penalecontemporaneo.it, 20 giugno 2017; G. Spangher, *La riforma Orlando della giustizia penale: prime riflessioni*, in *Dir. pen. cont., Riv. trim.*, 1, 2016, 98 ss.; E. Lorenzetto, *Processo penale e legge n. 103 del 2017: la riforma che non c'è*, in *Proc. pen. e giust.*, 6, 2017, 1067 ss.

[6] M. Gialuz - A. Cabiale - J. Della Torre, *Riforma Orlando: le modifiche attinenti al processo penale, tra codificazione della giurisprudenza, riforme attese da tempo e confuse innovazioni*, cit., 1.

[7] V., ad es., S. Menafra, *Intercettazioni, a natale il decreto "depotenziato"*, in *il Manifesto*, 13 dicembre 2017; G. Negri, *Riforma intercettazioni "blindata", non passano le richieste delle procure*, in *il Sole24 ore*, 17 dicembre 2017 e pure il successivo articolo in data 19 dicembre, *Il governo rafforza la difesa.*

[8] G. Giostra, *L'impraticabile meccanismo di selezione delle intercettazioni*, in *il Sole24 ore*, 20 dicembre 2017; v., anche, L. Ferrarella, *Meno segreti sulle intercettazioni: i primi passi (e i dubbi)*, in *Il Corriere della Sera*, 29 dicembre 2017.

[9] P. Morosini, *Le intercettazioni e il cerino dei pm*, in *Il Fatto Quotidiano*, 15 novembre 2017.

[10] V. quanto riportato da L. Milella, *"Intercettazioni, indagini danneggiate". L'allarme dei procuratori sulla riforma*, in *La Repubblica*, 22 novembre 2017.

I cambiamenti, insomma, sono sgraditi ai giuristi (avvocati e magistrati)[11], non accettati *in toto* dalla dottrina[12] e nemmeno dai giornalisti: addirittura la FNS (Federazione Nazionale della Stampa) e l'OdG (Ordine dei Giornalisti) hanno manifestato il loro netto dissenso per le "norme liberticide" davanti a Montecitorio[13].

In ambito parlamentare non sono mancati i timori per l'aggiramento (sotto l'aspetto metodologico) della Costituzione[14]; inoltre, la seconda Commissione permanente ha pronunciato sì parere non ostativo, inserendo però una serie di «condizioni», di «osservazioni», ravvisando l'esigenza di interventi correttivi per i numerosi «profili di incompatibilità»[15].

Una volta sottratti i giudizi che nel complesso si possono definire negativi[16], e gli orientamenti intermedi[17], resta ben poco. Infatti, alla fine, sembra residuare unicamente la soddisfazione che emerge dai comunicati ministeriali e dalle note dell'Ufficio legislativo (relazione tecnica, analisi di impatto della regolamentazione, analisi tecnico-normativa): esce qui confermato il ruolo delle intercettazioni «strumento indispensabile di indagine», e si ritiene raggiunto l'equilibrio tra «interessi meritevoli di tutela a livello costituzionale», tra «la necessità di segretezza delle forme di comunicazione e il diritto

---

[11] M. Adinolfi, *Intercettazioni. Se la riforma riduce il diritto di difesa*, in *Quotidiano di Puglia*, 30 dicembre 2017; G. Di Fiore, *Migliucci (UCPI): le norme violano la parità tra accusa e difesa*, in *Il Mattino,* 30 dicembre 2017; G. Negri, *Intercettazioni, più tutela della privacy*, in *il Sole24 ore*, 30 dicembre 2017; A. Esposito, *Il decreto sulle intercettazioni colpisce i pm e l'informazione*, in *Il Fatto Quotidiano*, 2 gennaio 2018.

[12] V., con sfumature differenti, C. Conti, *La riservatezza delle intercettazioni nella "delega Orlando". Una tutela paternalistica della privacy che può andare a discapito del diritto alla prova*, in *Dir. pen. cont.*, 3, 2017, 79 ss.; P. Dell'Anno, *Le tre deleghe sulla riforma processuale introdotte dalla legge n. 103 del 2017*, in *Proc. pen. e giust.*, 6, 2017, 1084 ss.; G. Insolera, *Intercettazioni: le vite degli altri nel tritacarne*, in *Il Mattino*, 2 gennaio 2018; S. Lorusso, *Solo una frenata al gossip giudiziario*, in *Gazzetta del Mezzogiorno*, 30 dicembre 2017; G.P. Voena, *Processo penale e mezzi di comunicazione di massa: un instabile stato dell'arte*, in *Proc. pen. e giust.*, 6, 2017, 1113 ss. Cfr. note 8, 17 e 19.

[13] S. Musco, *Più intercettazioni, meno bavagli. La libertà secondo i giornalisti*, in *Il Dubbio*, 23 novembre 2017; cfr., I.M. Prado, *Intercettazioni con rilevanza penale? È ancora più importante non pubblicarle*, in *Il Dubbio*, 6 dicembre 2017.

[14] A. Mascali, *Intercettazioni, l'attacco di Casson: «il Governo ha aggirato la Costituzione»*, in *Il Fatto Quotidiano,* 6 dicembre 2017; «quando l'anno scorso fu votato il maxi-emendamento con la delega al ministro in materia di intercettazioni» - spiega il senatore Casson - «il governo ha posto la fiducia due volte», così l'esecutivo che «dovrebbe essere il legislatore delegato, in sostanza si è fatto la delega, aggirando... la Costituzione, per di più in materia di diritti inviolabili». V. sul punto, la stroncatura di D. Barontini, *Decreto intercettazioni, un semi-golpe in stile felpato*, in contropiano.org, 4 gennaio 2018.

[15] Cfr. Legislatura 17° - 2° Commissione permanente - Resoconto sommario n. 443 del 12 dicembre 2017, Parere approvato dalla Commissione sull'atto del Governo n. 472.

[16] Cfr. C. Nordio, *Intercettazioni, un'inutile mini-riforma*, in *il Gazzettino*, 28 dicembre 2017. V., pure, D. Cacopardo, *Intercettazioni: peggio di prima. La seconda selezione è dei Pm. perché non del giudice?*, in *Italia Oggi*, 4 gennaio 2018; E. Martini, *Intercettazioni, tutti contro la riforma*, in *il Manifesto*, 30 dicembre 2017; C. Morelli, *Intercettazioni, si va per gradi. Il cuore della riforma entrerà in vigore dopo sei mesi*, in *Italia Oggi*, 8 gennaio 2018.

[17] Per D. Stasio, *Intercettazioni/2: riforma equilibrata ma senza risorse rischio boomerang*, cit., 3, la «riforma» sarebbe «tutto sommato accettabile ed equilibrata sia politicamente che tecnicamente» e forse l'unica (si domanda) voce fuori dal coro risulta essere quella del Procuratore della Repubblica di Torino, Armando Spataro. Cfr. T. Bene, *La effettività della funzione del pubblico ministero di direzione delle indagini e la legalità processuale,* in *Proc. pen. e giust.*, 1, 2018, 8; G. Spangher, *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, in www.giurisprudenzapenale.com, 8 gennaio 2018.

dell'informazione», senza «dar luogo a maggiori oneri a carico del bilancio»[18].

2. La scarsa affezione per i principi della procedura penale europea: a) il "posto" assegnato alle intercettazioni nello stadio investigativo

La rassegna riportata nel precedente paragrafo è, di sicuro, minima (ridotta a quanto pubblicato nel periodo più recente) e non ha davvero lo scopo di rimarcare - in maniera quasi compiaciuta - l'ennesimo scontento pressoché generale (qualcosa di simile sta capitando pure sul versante della partecipazione a distanza *ex* art. 146 bis disp. att. c.p.p.).

Attraverso la lettura, minuziosa e puntuale dei quotidiani e degli articoli comparsi sulle riviste specializzate[19], affiorano alcune questioni peculiari che investono direttamente il processo penale.

Non sono questioni marginali, anzi paiono ben visibili al centro del rito penale, concorrendo a caratterizzarlo - quel rito - in modo equo o, al contrario, iniquo; ciò dipenderà dalla soluzione di volta in volta prescelta, dal rispetto e dalla coerenza con i principi di procedura penale europea[20].

L'esame dei materiali legislativi e del testo varato smascherano una sorta di disaffezione per le regole del giusto processo europeo: il loro richiamo - quand'anche presente - non sfocia nell'attuazione consapevole, quindi concreta e non illusoria.

Ci sono parecchi indizi a sostegno di questa disincantata considerazione e si riconoscono - tanto per cominciare - nel "posto" attribuito al mezzo di ricerca della prova di cui si sta discutendo. Un posto «imprescindibile» nel panorama investigativo, secondo i citati materiali di provenienza ministeriale, che sembrerebbe stonare con l'approccio conservato dall'Unione europea e dalla "grande Europa"; lungo l'arco oramai di decenni, la Corte di Strasburgo ha ribadito in molte sentenze la non auspicabilità del ricorso alle intercettazioni[21], «importante» (non ineludibile) «strumento per la tutela degli interessi nazionali, in particolare la sicurezza nazionale e per le indagini relative a gravi reati»[22].

---

[18] In proposito, v. Ufficio legislativo, *Analisi tecnico-normativa* e *Relazione tecnica*.

[19] V. gli undici contributi dedicati al tema "Giustizia penale e informazione giudiziaria", in *Diritto penale contemporaneo-Rivista trimestrale*, 3, 2017 (anticipati sul sito www.penalecontemporaneo.it a partire dal 15 novembre 2017); cfr. *supra* note 8, 12, 17.

[20] Per una visione d'insieme, v. *Manuale di procedura penale europea*, R.E. Kostoris (a cura di), Milano, 2017; G. Ubertis, *Principi di procedura penale europea. Le regole del giusto processo*, Milano, 2009; G. Ubertis-F. Viganò (a cura di), *Corte di Strasburgo e giustizia penale*, Torino, 2016.

[21] ...di solito, indesiderabili (*non souhaitable*) e illegittime in una società democratica (CEDU, *Malone c. Regno Unito*, ric. 8691/79 (1984), § 84).
Cfr. A. Balsamo, *Il contenuto dei diritti fondamentali*, in R.E. Kostoris (a cura di), *Manuale di procedura penale europea*, cit., 171 ss.; M. Bonetti, sub *art. 8 Cedu*, in G. Ubertis- F. Viganò (a cura di), *Corte di Strasburgo e giustizia penale*,cit., 274; A. Gaito - S. Furfaro, *Intercettazioni: esigenze di accertamento e garanzie di riservatezza*, in A. Gaito (a cura di), *I principi europei del processo penale*, Roma, 2016, 367 ss.

[22] Risoluzione del Consiglio del 17 gennaio 1995 sull'intercettazione legale delle telecomunicazioni, in S. Buzzelli - O. Mazza (a cura di), *Codice di procedura penale europea*, Milano, 2005, 807 ss.

Di ciò bisognerà ricordarsi per proseguire nel ragionamento, perché «c'è sempre una *posta* al posto delle cose»: «dimmi come classifichi e ti dirò chi sei», ammoniva Roland Barthes nel 1970[23]. Non siamo di fronte a un dettaglio, nemmeno a un punto fin troppo generico, ma a una ripartizione influente sull'assetto delle indagini preliminari destinate a confluire, nella prospettiva originaria, in una fase che (seguendo la lezione di Massimo Nobili) non avrebbe dovuto né contare, né pesare[24].

3. Segue: b) il richiamo parziale alla giurisprudenza di Strasburgo, il silenzio sulle ricadute transnazionali

Un differente indizio, a conferma della scarsa sensibilità nei confronti della cultura processuale europea, si rinviene scorrendo il c. 84 (art. 1 l. 23 giugno 2017, n. 103) suddiviso in alcune lettere e vari numeri.

Non passa inosservato il criterio *sub* lett. c) da salvaguardare nell'esercizio della delega che impone di «tener conto delle decisioni e dei principi adottati con le sentenze della Corte europea dei diritti dell'uomo a tutela della libertà di stampa e del diritto dei cittadini all'informazione».

La congruenza linguistica con il vocabolario europeo avrebbe suggerito l'uso delle formule chiare, meno arzigogolate, che si trovano spesso nei testi normativi dell'Unione europea e suonano più o meno così: «secondo l'interpretazione della Corte di giustizia dell'Unione europea ("Corte di giustizia") e della Corte europea dei diritti dell'uomo»[25]; un inciso frequente indica l'articolo della Cedu che interessa e aggiunge «come interpretato nella giurisprudenza della Corte europea dei diritti dell'uomo»[26].

Non è una mera pignoleria di natura formalistica[27], o un rimando ovvio all'immancabile effetto prodotto dalla Cedu sul sistema interno[28], che spingono a puntualizzazioni del genere.

Oltre al lessico inappropriato il riferimento indiretto all'art. 10 Cedu e, pertanto, alla sola libertà di espressione sembra piuttosto scarno. La protezione pattizia è diffusa, ha una portata notevolmente più ampia e coinvolge almeno gli artt. 6 (diritto a un processo equo) e 8 (diritto al rispetto della vita privata e familiare) Cedu: è soprattutto in

---

[23] R. Barthes, *La retorica antica. Alle origini del linguaggio e delle tecniche di comunicazione*, 1970, trad. it., Milano, 1993, 53.

[24] Cfr., da ultimo, A. Camon, *La fase che "non conta e non pesa": indagini governate dalla legge?*, in *Legge e potere nel processo penale. Atti del Convegno, 4 e 5 novembre 2016*, Milano, 2017, 93 ss. (spec. 108 ss. dedicate alle intercettazioni).

[25] V., ad es., considerando 10 e 17 Direttiva (UE) 2016/1919 sull'ammissione al patrocinio a spese dello Stato per indagati e imputati nell'ambito di procedimenti penali e per le persone ricercate nell'ambito di procedimenti di esecuzione del mandato d'arresto europeo, in *GUUE*, 4 novembre 2016, L 297, 2-3.

[26] V., ad es., considerando 14 Direttiva 2010/64/UE sul diritto all'interpretazione e alla traduzione nei procedimenti penali, in *GUUE*, 26 ottobre 2010, L 280, 2.

[27] V. le opinioni di G.P. Voena, *Processo penale e mezzi di comunicazione di massa: un instabile stato dell'arte*, cit., 1123 e T. Bene, *La effettività della funzione del pubblico ministero di direzione delle indagini e la legalità processuale,* cit., 8.

[28] F. Viganò, *L'impatto della Cedu e dei suoi protocolli nel sistema penale italiano*, in G. Ubertis - F. Viganò (a cura di), *Corte di Strasburgo e giustizia penale*, cit., 13 ss.

quest'ultimo che si nascondono, assente una menzione espressa, i criteri per risolvere la casistica in tema di intercettazioni[29].

La triangolazione degli articoli - contenenti una fitta rete di garanzie - fornisce bene l'idea del delicato bilanciamento fra processo equo, diritto all'informazione (meglio alla cronaca giudiziaria e alla critica giudiziaria)[30], tutela della privatezza (distinta dalla segretezza come dalla riservatezza)[31]. Solo ricostruendo la scacchiera dei diritti convenzionalmente sanciti, misurando le loro accettabili compressioni incrociate e la regolamentazione offerta dalla giurisprudenza di Strasburgo, risaltano le prerogative in gioco. Così facendo si afferra la complessità del quadro, forse sfuggita al legislatore delegato - meno alla Commissione parlamentare[32] - pronto a reputare compatibile il sistema nazionale con l'art. 8 Cedu sulla scorta di una "decisione" (promossa nel frattempo a "sentenza")[33] specificamente dedicata all'istradamento, tecnica diventata oramai «per le autorità italiane, uno dei più significativi profili di novità» dell'ordine europeo di indagine[34]. Nel caso *Capriotti c. Italia* (decisione 23 febbraio 2016), il ricorrente, coinvolto in un traffico internazionale di stupefacenti, aveva dedotto una doppia violazione (artt. 8 e 6 Cedu), lamentando l'illegalità delle intercettazioni (disposte anche nei confronti di utenze estere senza rogatoria internazionale) e l'iniquità del processo. I giudici di Strasburgo non hanno avuto esitazioni: l'ingerenza è necessaria, in armonia con l'art. 8, c. 2 ,Cedu, e l'applicazione del cosiddetto istradamento (che non dovrebbe richiedere la rogatoria internazionale quando le chiamate provenienti da utenze estere siano canalizzate su centrali site in Italia) sarebbe legittimata da un «granitico quadro giurisprudenziale interno» (adesso rimesso in discussione dall'ordine europeo di indagine)[35]. La Corte europea, infine, ritiene di non avere sufficienti elementi per revocare le conclusioni dei giudici italiani ad avviso dei quali le intercettazioni interamente svolte all'estero non avrebbero avuto un ruolo determinante per condannare il ricorrente.

Resta ancora un'osservazione inerente al fenomeno, per certi versi opposto all'impatto

---

[29] G. Ubertis, *Principi di procedura penale europea. Le regole del giusto processo*, cit., 132.

[30] V. i casi CEDU, *July e Sarl Liberation c. Francia,* ric. 20893/03 (2008) e *Kobenter e Standard Verlags GMBH c. Austria,* ric. 60899/00 (2006).
Cfr., in argomento, G.E. Vigevani, *La libertà di espressione e di informazione*, e C. Melzi d'Eril, *Diritto di cronaca e diritto di critica*, ambedue in C. Malavenda - C. Melzi d'Eril - G.E. Vigevani, *Le regole dei giornalisti. Istruzioni per un mestiere pericoloso*, Bologna, 2012, rispettivamente 25 ss. e 59 ss.

[31] G. Ubertis, *Principi di procedura penale europea. Le regole del giusto processo*, cit., 126.

[32] Legislatura 17° - 2° Commissione permanente - Resoconto sommario n. 443 del 12 dicembre 2017, Parere approvato dalla Commissione sull'atto del Governo n. 472, cit., 1: «non risulta che al predetto principio e criterio direttivo sia stata data alcuna specifica attuazione».

[33] Ufficio legislativo, *Analisi tecnico-normativa*, parte II, p. 5.

[34] *Circolare in tema di attuazione della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale - Manuale operativo*, 26 ottobre 2017, prot. n. DAG. 0203162.U del 30/10/17, 25; v. *infra* nota 38.

[35] In effetti, il consolidato insegnamento della Corte di cassazione «deve fare ora i conti, almeno nel perimetro operativo della direttiva 2014/41/UE... con l'espressa previsione dell'art. 31 che conferisce rilievo - anziché al luogo di esecuzione delle operazioni - al territorio nel quale è utilizzato l'indirizzo di comunicazione della persona soggetta a intercettazione, per imporre allo Stato di intercettazione l'effettuazione di una notifica allo Stato membro "nel quale si trova la persona soggetta a intercettazione", affinché quest'ultimo possa determinarsi in ordine all'ammissibilità o meno dell'avvio (o della prosecuzione) delle autorità captative sul proprio territorio» (*Circolare in tema di attuazione della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale - Manuale operativo*, cit., 25).

delle fonti europee sull'intelaiatura processuale italiana, che si rintraccia nella inevitabile incidenza delle opzioni legislative nazionali sulla cooperazione in materia penale. Le regole, insomma, introdotte dalla novella legislativa di fine 2017 non possono non influenzare la collaborazione giudiziaria tra gli Stati europei. E' sintomatica - per capire questo influsso - la formula (collegata alle informazioni necessarie per decidere) «se la misura richiesta sarebbe presa in un caso analogo a livello nazionale» che figura in numerose disposizioni sulle intercettazioni ed è preferita al concetto di «conformità al diritto nazionale»[36]: qualcosa di simile ritorna anche nel testo della citata Direttiva 2014/41/UE (ordine europeo di indagine penale) [37] che dal maggio 2017 ha sostituito la Convenzione di Bruxelles tardivamente attuata dal nostro Paese[38].

4. Possibili punti di sofferenza: trascrizione e selettività arbitraria; diritto di difesa e svantaggi sostanziali

Il modello allegato alla direttiva sull'ordine europeo di indagine (A - sez. H7 Intercettazione di telecomunicazioni) offre uno spunto ulteriore per continuare il discorso sui problematici risvolti interni: la «preg[hier]a di indicare una preferenza in merito al metodo di esecuzione» (trasmissione immediata, registrazione e successiva trasmissione), e la domanda aggiuntiva se siano richieste, o meno, «trascrizione, decodificazione e decrittazione del materiale intercettato», mettono in luce il primato dei metodi esecutivi e la decisività della tecnica di documentazione in grado di condizionare le altre tappe (deposito, conservazione). Diventa un gravoso impegno comprendere i passaggi successivi[39], senza perdersi nel labirinto normativo, se prima non si chiarisce lo snodo - per l'appunto - della trascrizione, dunque l'alternativa trascrivibile/non trascrivibile.
Il nuovo c. 2-*bis*, inserito nell'art. 268 c.p.p. dal decreto legislativo n. 216 del 2017, vieta[40] «la trascrizione, anche sommaria, delle comunicazioni o conversazioni irrilevanti ai fini delle indagini, sia per l'oggetto che per i soggetti coinvolti, nonché di quelle, parimenti non rilevanti, che riguardano dati personali definiti sensibili dalla legge»; mentre il susseguente c. 3-*bis* autorizza l'organo dell'accusa a disporre, con decreto motivato, la trascrizione «nel verbale quando ne ritiene la rilevanza per i fatti oggetto di prova».

---

[36] *Relazione esplicativa sulla convenzione del 29 maggio 2000 relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea*, in *GUUE*, 29 dicembre 2000, C 379, 22.

[37] Cfr. art. 30, Direttiva 2014/41/UE relativa all'ordine europeo di indagine penale, in *GUUE*, 1° maggio 2014, L 130, 20.

[38] La cosiddetta Convenzione di Bruxelles (relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea) del 29 maggio 2000 è stata attuata grazie al decreto legislativo 5 aprile 2017, n. 52 (cfr. spec. l'intero titolo III); invece, l'ordine europeo di indagine (Direttiva 2014/41/UE) ha trovato più veloce attuazione tramite il decreto legislativo 21 giugno 2017, n. 108 (cfr. art. 23 ss.). Cfr. *Circolare in tema di attuazione della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale - Manuale operativo*, cit., punto 17.4.

[39] Esposti da G. Pestelli, *Brevi note sul nuovo decreto legislativo in materia di intercettazioni: (poche) luci e (molte) ombre di una riforma frettolosa*, in www.penalecontemporaneo.it, 29 gennaio, 2018.

[40] ... «pur senza alcuna specifica sanzione processuale in caso di relativa elusione» (D. Pretti, *Prime riflessioni a margine della nuova disciplina delle intercettazioni*, in www.penalecontemporaneo.it, 29 gennaio, 2018, 3).

La strada percorsa (che non era obbligata) nell'affidare la "scrematura" all'ufficiale di polizia delegato all'ascolto, sulla base della rilevanza per le indagini, genera dubbi e perplessità[41], non motivati da una preconcetta sfiducia nei confronti della polizia giudiziaria o dalla paura di un rinnovato "strapotere di polizia"[42]. C'è, invece, il serio timore di uno svuotamento effettivo della direzione investigativa spettante al pubblico ministero[43] che abbandona senza controllo una fase in cui, al contrario, i controlli sono necessari[44]. La rilevanza poi, come la pertinenza[45], è parametro sfuggente e precario, pronto ad acquistare un senso in situazioni comparative, in rapporto a un determinato contesto e a un *iter* probatorio[46].

Fa da sottofondo uno schema culturale d'impronta inquisitoria - proiettato verso la sede dibattimentale - che trascura la fluttuante natura delle indagini e l'eventualità di procedere a rapide riclassificazioni[47]: lo «scopo» - scrive l'Ufficio legislativo nell'Analisi di impatto - «è quindi, da un lato, quello di stabilire da subito quale sia il materiale sul quale dovranno confrontarsi le parti nel futuro dibattimento, dal momento che solo il materiale utile è destinato a essere trascritto, dall'altro di preservare la riservatezza dei terzi e degli stessi indagati, rispetto a informazioni sensibili inessenziali agli scopi del processo»[48].

Per preservare la riservatezza[49] il legislatore introduce una selettività - avente a oggetto parole, gergo, espressioni dialettali fonti di facili travisamenti[50] - che rischia di contaminare nel suo insieme il metodo dialettico[51], il quale rinuncia ai flussi informativi disor-

---

41 V., tra i molti, G. Pestelli, *Brevi note sul nuovo decreto legislativo in materia di intercettazioni: (poche) luci e (molte) ombre di una riforma frettolosa*, cit. (cfr. il § 5).

42 P. Morosini, *Le intercettazioni e il cerino dei pm*, cit.

43 G. Negri, *Giovanni Legnini (CSM): "interverremo sulle intercettazioni"*, in *il Sole 24 ore*, 4 febbraio 2018: è l'annuncio del vicepresidente del CSM, finalizzato «a rendere più fluidi i rapporti tra pubblici ministeri e polizia giudiziaria, chiamata quest'ultima a un primo filtro di rilevanza degli ascolti».

44 Cfr. i casi CEDU, *Kostantin Moskalev c. Russia*, ric. 59589/10 (2017); CEDU, *Roman Zakharov c. Russia*, ric. 47143/06 (2015).

45 Cfr. L. Ferrarella, *Il "vorrei ma non posso" di un legislatore che "potrebbe ma non vuole"*, in questa *Rivista*, 1, 2018, 201 ss.

46 G. Ubertis, *Principi di procedura penale europea. Le regole del giusto processo*, cit., 74-75.

47 A. Balsamo - A. Tamietti, *Le intercettazioni, tra garanzie formali e sostanziali*, A. Balsamo - R.E. Kostoris (a cura di), in *Giurisprudenza europea e processo penale italiano,* Torino, 2008, 457.
Ampiamente, cfr. F. Cassibba, *L'imputazione e le sue vicende*, in G. Ubertis - G.P. Voena (diretto da), *Trattato di procedura penale*, Milano, 2016, 77 ss.

48 Ufficio legislativo, *Analisi di impatto della regolamentazione (A.I.R.)*, 3

49 Cfr. *supra* nota 31.

50 Cfr. CEDU, *Mazzarella c. Italia*, ric. 24059/13 (2017): condannato in sede di abbreviato per associazione finalizzata al traffico di stupefacenti, il ricorrente contesta la mancata valutazione da parte del g.u.p. di una consulenza tecnica (depositata dalla difesa prima della richiesta del rito speciale) secondo la quale il contenuto delle intercettazioni sarebbe stato travisato al momento della trascrizione. La Corte europea non reputa lesa l'equità processuale (art. 6 CEDU), ribadisce la conformità del rito ai parametri convenzionali, osserva che gli elementi di prova a carico sono stati molteplici; in particolare, l'interpretazione del linguaggio e del contenuto delle conversazioni intercettate costituisce una questione di fatto, rimessa alla valutazione del giudice di merito.

51 Ecco allora l'importanza delle opzioni attuali: «quando un nuovo strumento investigativo ha fatto capolino, abbiamo assistito, pressoché sempre, al tentativo di incasellarlo nella disciplina delle intercettazioni» (A. Camon, *La fase che "non conta e non pesa": indagini governate dalla legge?*, cit., 113).

dinati, non rispettosi dei criteri di cernita dell'ordine selettivo; quest'ultimo respinge le informazioni insignificanti, e si cautela contro il pericolo antitetico, proprio quello cioè di omettere informazioni in maniera arbitraria e intempestiva.

Saranno impressioni da sedimentare nel corso della *vacatio legis*[52]; c'è tempo per riflettere, dopo la consueta "prima" lettura, ne verrà una "seconda". Però, oltre a quanto velocemente elencato fino adesso, non rassicura il ridimensionamento delle garanzie difensive[53] (contrapposto all'estensione «per certi aspetti ... dell'area operativa» delle intercettazioni)[54]: se «il pm ha poco tempo per valutare in corso d'opera la rilevanza delle conversazioni intercettate» - nota il Procuratore della Repubblica di Velletri nelle Linee guida emanate a gennaio di quest'anno - «la difesa ha un tempo ancor più ridotto per la individuazione di quelle eventualmente utili e ciò pone un problema di effettività del diritto di difesa»[55].

Incomincia a traballare la parità accusa-difesa, autentico pilastro dell'art. 6 Cedu: ciò è giustificabile in una precaria «società della comunicazione di massa»[56], appare viceversa indegno di una «società dell'informazione sicura»[57], dove «occorre cogliere attraverso il diritto» le «situazioni nuove», create dalle «tecnologie moderne»[58], senza danneggiare le regole del processo giusto.

---

[52] ... «funzionale a consentire alle procure della Repubblica di dettare le opportune indicazioni per dare attuazione al nuovo articolo 89 bis disp. att. c.p.p. che affida la direzione dell'archivio riservato al procuratore della Repubblica che così dovrà garantire la tutela del segreto su quanto ivi custodito»: Procura della Repubblica di Velletri, *Linee guida sulla nuova disciplina in tema di intercettazioni*, prot. n. 378/2018, Velletri, 15 gennaio 2018, consultabile in www.penalecontemporaneo.it, 3.

[53] Cfr. G. De Minico, *Sulle intercettazioni penalizzati difesa e informazione*, in *il Sole 24 ore*, 23 gennaio 2018.

[54] Procura della Repubblica di Velletri, *Linee guida sulla nuova disciplina in tema di intercettazioni*, cit., 1.

[55] *Ibidem,* 6.

[56] Ufficio legislativo, *Analisi tecnico-normativa*, cit., 2.

[57] V. già Consiglio dell'Unione europea, *Risoluzione del Consiglio su una strategia per una società dell'informazione sicura in Europa*, in *GUUE*, 24 marzo 2007, C 68, 1.

[58] *Relazione esplicativa sulla convenzione del 29 maggio 2000 relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea*, cit., 20.

I captatori informatici: una riforma troppo contenuta per uno strumento investigativo così pervasivo*

Barbara Indovina

Abstract

Lo scritto analizza il funzionamento dei c.d. captatori informatici recentemente introdotti nell'ordinamento italiano con il d.lgs 216/2017 analizzando, in particolare, la pervasività di tale strumento investigativo.
Il testo prende in considerazione sia l'aspetto prettamente tecnico sia quello giuridico ripercorrendo le diverse pronunce giurisprudenziali che hanno portato il legislatore a inserire i captatori informatici come mezzo di ricerca della prova nel codice di procedura penale.

The article concerns the functioning of the so-called Trojan horse malware, recently regulated in Italy by Law 216/2017 examining, in particular, the pervasiveness of the use of this investigative tool.
The essay analyzes both technical and legal aspects of such use retracing the judgments that led the Italian parliament to regulate Trojan horses in the Italian Criminal Procedure Code under the chapter relating to the gathering of evidence.

Sommario

1. Qualche premessa tecnologica. – 2. I captatori informartici: cosa sono e come funzionano. – 3. L'acquisizione delle informazioni contenute sul dispositivo elettronico. – 4. La nuova disciplina su intercettazioni (e captatori).

Keywords: Prova, Captatori, Trojan horse, Intercettazioni, Riforma Orlando

1. Qualche premessa tecnologica

Una storica sentenza della Corte Suprema Usa del 2014 (*Riley v. California*)[1] ha stabilito che per ottenere una perquisizione su un telefonino, anche in caso di arresto, è necessario un mandato giudiziario *ad hoc* questo perché, si legge: «Ormai il 90% degli americani ne possiede, contengono una trascrizione digitale di ogni aspetto delle loro vite, dai più banali ai più intimi, sono una parte pervasiva e onnipresente della vita quotidiana; un marziano sbarcato sulla terra potrebbe pensare che il telefonino è un pezzo importante

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".
[1] www.documentcloud.org/documents/1208245-riley-v-california.html.

dell'anatomia umana»[2]. E ancora il Giudice relatore John G. Roberts Jr. così argomenta la propria decisione: «perfino la parola telefonino ormai è inadeguata, fuorviante. Li potremmo chiamare videocamere, videoregistratori, agendine personali, calendari, librerie, diari, album, televisioni, mappe, giornali».

Niente di più vero e appropriato.

La tecnologia ormai pervade la nostra quotidianità: strumenti quali computer, smartphone, navigatori GPS, macchine fotografiche digitali trattano e raccolgono innumerevoli dati personali e tracce digitali che consapevolmente o inconsapevolmente rilasciamo quotidianamente.

I moderni smartphone, in particolare, contengono numerosissimi dati e diversi tipi di informazioni tutti allocati su un unico dispositivo: informazioni che prese singolarmente o anche combinate tra loro possono fornire una serie innumerevole di risultati. Basti pensare che su un unico dispositivo conteniamo l'elenco dei nostri contatti, messaggi, registro chiamate, video, dati di navigazione, dati relativi alla geo localizzazione, mail, più tutta una serie di dati raccolti dalle più svariate applicazioni (le c.d. "app").

Dati che spesso, soprattutto se combinati con ulteriori *device* quali, ad esempio, gli Smart watch, possono rilevare anche importanti dati connessi al nostro stato di salute e alle nostre abitudini quotidiane.

È indubbio ritenere che negli ultimi anni gli smartphone e, più in generale, gli strumenti informatici (pc, tablet etc.) siano stati un preziosissimo strumento a fini investigativi: la *digital forensics*[3] è largamente utilizzata a fini investigativi praticamente sempre, in qualsiasi indagine, proprio attesa la quantità di dati contenuti in un singolo device utili a ottenere (a volte fondamentali) indizi e prove.

La Convenzione del Consiglio di Europa sul *cyber crime*, poi ratificata dal legislatore italiano con l. 48/2008, ha introdotto nuove regole processuali applicabili alla ricerca e susseguente acquisizione delle prove elettroniche nel procedimento penale.

Negli ultimi anni, proprio alla luce della pervasività degli strumenti informatici, il dibattito tra privacy e sicurezza è più che mai acceso: le nuove tecnologie consentono una trasmissione e conservazione sempre maggiore di dati personali e questi dati sempre più spesso vengono visti come informazioni necessarie a fini investigativi o, ancor maggiormente, a fini di sicurezza e contrasto e prevenzione alla criminalità.

È sempre più difficile bilanciare questi aspetti così compenetrati: il caso Apple/FBI[4] ha portato all'attenzione internazionale proprio il difficile equilibrio tra sicurezza, investigazioni e tutela della privacy degli utenti; e soprattutto si è iniziato a parlare di

[2] *Such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.*

[3] La *digital forensics* è una branca delle scienze forensi che attiene al reperimento, recupero e analisi investigativa del materiale digitale utile a fini investigativi allocato in dispositivi digitali.

[4] Nel febbraio del 2016 l'FBI ha chiesto ad Apple di poter accedere al contenuto del cellulare di uno degli attentatori della strage di San Bernardino del dicembre 2015 mediante una *backdoor* ovvero una "porta di accesso" che fosse in grado di aggirare le tecniche di cifratura poste a tutela di ogni *device* Apple.

crittografia[5] e tecniche di cifratura, argomento fino a quel punto ignorato anche da gran parte degli addetti ai lavori.
Solo pochi anni prima lo scandalo Datagate/Prism aveva fatto emergere il problema della sorveglianza globale delle comunicazioni e dei dati tramite internet e fornitori di servizi elettronici.
I sistemi operativi degli smartphone di ultima generazione hanno previsto (da una data versione in poi) dei sistemi di cifratura così che il loro contenuto diventi ineleggibile da chi non è in possesso della password di sblocco.
Non solo smartphone ma anche alcune app quali, ad esempio, il più diffuso sistema di messaggistica istantanea "Whatsapp[6]", hanno introdotto sistemi di cifratura (*end to end*) volti a garantire la segretezza delle comunicazioni: comunicazioni non solo effettuate via messaggistica testuale ma anche relative alla telefonia e video chiamate.
La cifratura *end to end* è stata via via implementata da pressoché tutte le piattaforme di messaggistica e comunicazione: dapprima Whatsapp, poi Facebook messenger, poi Allo di Google ed è notizia di questi ultimi giorni che anche Skype ha implementato tale tecnologia: mentre in alcune piattaforme prevedono di default il sistema di cifratura (Whatsapp e Signal, ad esempio), in altre piattaforme è l'utente che decide di iniziare una conversazione cifrata (ad esempio in Telegram o Messenger "chat o conversazione segreta").
Le moderne comunicazioni elettroniche, quindi, a differenza di ciò che succedeva un tempo con le comunicazioni telefoniche e di messaggistica istantanea, mediante l'utilizzo di tecniche di cifratura sono, allo stato, inintelligibili qualora intercettate nel loro flusso: da questa doverosa premessa tecnologica è necessario partire per comprendere l'importanza dei nuovi strumenti di captazione che vengono inseriti direttamente nei dispositivi a valle, quindi, del processo di criptazione dei dati in entrata e uscita.

2. I captatori informartici: cosa sono e come funzionano

I captatori informatici sono dei software definiti quali virus (termine usato volgarmente per indicare dei *malicious software-malware*) atteso il loro scopo intrusivo e volto a carpire informazioni nel dispositivo ove vengono rilasciati (iniettati): da tale accezione i più autorevoli esperti hanno coniato il nome di "trojan di stato".
La tipologia di malware è infatti quella definita come "*trojan horse*": come il celeberrimo "cavallo di troia" tali malware si nascondono all'interno di altri programmi apparentemente innocui e vanno a infettare la macchina bersaglio.
Il captatore informatico non viene individuato dai sistemi antivirus dei *device* ove viene allocato in quanto utilizza delle tecniche di inoculazione e/o mascheramento, ossia un pacchetto offensivo in grado di infettare vari tipi di *device* e sistemi di escalation dei

[5] La crittografia (dall'unione di due parole greche: κρυπτός [kryptós] che significa "nascosto", e γραφία [graphía] che significa "scrittura") è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo (da Wikipedia).

[6] www.whatsapp.com/security/?l=it

privilegi, tipici di un *rootkit*, in grado altresì di eludere i sistemi di rilevamento e dare all'intrusore accesso da remoto al contenuto del dispositivo.

Tali software quindi si comportano come programmi di *backdoor* (come abbiamo accennato sopra in relazione al caso Apple/FBI), ossia rendono possibile connettersi in modalità remota al dispositivo "infetto".

I captatori vengono iniettati sfruttando una vulnerabilità all'interno del sistema operativo bersaglio non conosciuta nemmeno agli sviluppatori del programma definita comunemente "0-day"[7], talvolta, unitamente a tecniche di *social engineering*[8] che utilizzano metodi di comunicazione e di persuasione al fine di ottenere o compromettere informazioni personali riguardanti individui o società, tramite un vero e proprio studio di ogni soggetto da intercettare.

Il captatore viene generalmente inoculato con diverse modalità:

- mediante posta elettronica: il malware appare come un allegato apparentemente innocuo di posta elettronica;
- mediante web: il virus è trasmesso tramite un download effettuato dall'utente da una pagina web;
- mediante trasferimento fisico tramite CD-ROM o un'unità USB da collegare all'apparecchio da infettare;
- mediante infezione dall'esterno attraverso connessione dal provider di telecomunicazioni, falsi update o siti civetta, oppure tramite *IMSI Catcher*, anche portatili, che permettono alle forze dell'ordine di portare attacchi di tipo "*man-in-the-middle*" (MTM)

Una volta inoculato all'interno del sistema il captatore può assumere diverse forme e svolgere diverse attività e funzioni, tra le quali:

- raccogliere email, SMS, cronologia telefonica e lista dei contatti;
- intercettare ciò che viene digitato sulla tastiera (*keylogger*);
- visualizzare la cronologia delle ricerche web e "catturare" le schermate visualizzate sul dispositivo;
- registrare le telefonate effettuate anche mediante applicazioni o programmi (Skype etc.);
- usare i telefoni per intercettazioni di tipo ambientale con attivazione del microfono;
- mettere in funzione la foto-videocamera di telefoni o computer;
- sfruttare i sistemi GPS per geolocalizzare i soggetti sorvegliati.

Le operazioni svolte dal captatore rientrano, quindi, per loro natura in quelle attività di "intercettazioni di comunicazioni" ricollegabili alla disciplina di cui agli artt. 266 ss. c.p.p., alla luce dell'interpretazione offerta dalle Sezioni Unite della Corte di cassazione[9] relativamente alle operazioni con carattere occulto e clandestino, avvenute anche

[7] Il termine "*zero-day*" viene utilizzato perché il programmatore del codice vittima dell'attacco ha zero giorni per poter correggere il prodotto dopo che questo viene attaccato sfruttando una sua vulnerabilità intrinseca.

[8] Nel campo della sicurezza informatica le tecniche di ingegneria sociale permettono lo studio del comportamento individuale di una persona al fine di carpire informazioni utili.

[9] Cass. pen., sez. un., 28 maggio 2003, n. 36747, in *Guida al diritto*, 2003, 42 ss.

tramite tecnologia informatica o telematica.

3. L'acquisizione delle informazioni contenute sul dispositivo elettronico

La cifratura delle moderne comunicazioni elettroniche richiede che l'acquisizione delle informazioni contenute sul *device* avvenga mediante l'acquisizione diretta del supporto informatico non cifrato (*rectius* mediante sequestro), o tramite intercettazione a monte dei flussi di comunicazione attraverso software in grado di captarli.
Come sopra evidenziato gli smartphone di ultima generazione sono cifrati mediante codice di accesso e/o codice biometrico (impronta digitale o altro dato biometrico come ad esempio l'ultimo modello della Apple iPhone X, il riconoscimento facciale dell'utente).
Un aspetto interessante fino ad ora mai preso in considerazione dal nostro legislatore, a differenza di altri legislatori come ad esempio quello statunitense, è che non vi è alcun obbligo da parte dell'indagato di rivelare il proprio codice di accesso o le proprie password di de-criptazione; l'indagato ha sempre la facoltà di non rispondere e/o di non dire il vero.
Non solo: le password di accesso dello smartphone se digitate erroneamente per diversi tentativi possono portare alla disabilitazione del telefono con perdita dei dati in esso allocati.
Un sequestro può, quindi, risultare vano attesa la complessità e, talvolta, l'impossibilità di recuperare informazioni custodite all'interno del computer o nello smartphone dell'indagato.
L'utilizzo dei captatori informatici è una tecnica investigativa che potenzialmente può ovviare a tale problema di acquisizione materiale mediante sequestro di un supporto che poi risulta essere non intellegibile e sta diventando l'unico strumento utile per acquisire gran parte del traffico dati che transita mediante IP.
Ancor più quando si consideri l'utilizzo ormai massivo di sistemi di *cloud computing* che garantiscono la fruizione on-line di tecnologie e risorse informatiche con servizi come quelli di archiviazione con conseguente pressoché totale assenza di dati allocati su di un singolo dispositivo.
Sia che il dispositivo venga sequestrato che si agisca mediante captatori è indubbio che gli investigatori vengano a conoscenza di una serie di informazioni (soprattutto se si considerano gli smartphone) che spaziano dalla corrispondenza (e-mail), agli SMS, ai dati di spostamento e geolocalizzazione, al registro chiamate, ai dati bancari, ai documenti.
Dati che vengono acquisiti, quindi, o con sequestro del dispositivo o mediante intercettazione con inoculazione e attivazione del captatore informatico.
Se è vero che mediante captatore informatico vi è una attività di intercettazione di una molteplicità di dati (da qui le grandi preoccupazioni relative ad una corretta regolamentazione legislativa di tali programmi) è pur vero che la stessa cosa può dirsi relativamente al sequestro di un *device*: mediante sequestro dello smartphone (conoscendone la password di sblocco) è possibile accedere a una infinità di dati ivi stanziati.
Tuttavia è innegabile che anche mediante captatore è possibile prendere cognizione di

tutta una serie di dati che sono allocati sul dispositivo ai quali si ha accesso e di cui si può disporre l'acquisizione (dati GPS, vecchie conversazioni e chat, mail).
I nuovi strumenti tecnologici hanno messo a dura prova legislazione e giurisprudenza nell'adattare vecchi strumenti a nuovi problemi e tecnologie: il captatore può svolgere le più disparate attività e a ciascuna di esse possono ricondursi diverse attività investigative riconducibili a pressoché tutti i mezzi di ricerca probatoria disciplinati dal codice di procedura penale.
Numerosi sono stati gli interventi giurisprudenziali volti a fare luce su diverse problematiche afferenti proprio la qualificazione delle diverse attività del captatore in relazione, innanzitutto, alla definizione di cosa sia una attività di intercettazione, alla tipologia di dati presenti su un singolo supporto (equiparabili o meno ad analoghi strumenti analogici) e al loro utilizzo probatorio come ad esempio in tema di pedinamento elettronico (mediante attivazione di GPS) o sequestro di corrispondenza telematica (e-mail) o SMS e chat.
Un captatore può effettuare intercettazioni telematiche (carpire il traffico in entrata e uscita), intercettazioni ambientali (mediante l'attivazione del microfono), effettuare videoriprese, tracciare il movimento mediante GPS; e lo fa mediante una intrusione in un domicilio informatico (tutelato dalla Costituzione come tutelata è la riservatezza dei dati ai sensi dell'art. 8 CEDU).
Una attività tipica del captatore informatico è, infatti, quella di consentire la geolocalizzazione con conseguente possibilità di monitoraggio via GPS dei movimenti del dispositivo intercettato: la giurisprudenza di legittimità sul punto ha caratterizzato tale attività come un mero pedinamento (digitale), e quindi atto atipico di indagine che non rientra nel novero delle intercettazioni.
Il dibattito su tali aspetti tecnologici e giuridici non è ancora sopito anche perché dalle diverse soluzioni interpretative dipendono gravi conseguenze relative anche all'utilizzabilità dei dati acquisiti nella fase investigativa: e nuove problematiche si presentano di continuo.
Pochi giorni dopo la Sentenza Scurato la pronuncia della Corte di cassazione sul caso Occhionero-Eyepyramid, andando oltre i limiti delineati dalla sentenza delle Sezioni unite, ha analizzato un caso di captatore installato su un pc fisso che svolgeva attività di intercettazione telematica (*ex* art. 266-*bis* c.p.p.) e che acquisiva, altresì, screenshot dello schermo del PC controllato qualificando tale ultima attività come atto di perquisizione/ispezione.
Perquisizione occulta, peraltro, e sfornita di tutte le garanzie difensive previste.
E ancora, una delle prime pronunce di legittimità relativa all'utilizzo dei captatori informatici è stata la sentenza "Virruso[10]" relativamente a un captatore in grado, semplicemente, di prelevare e copiare alcuni documenti memorizzati sull'hard disk dell'apparecchio in uso all'indagato: il P.M. titolare delle indagini aveva disposto tale attività ai sensi dell'art. 234 c.p.p. come acquisizione documentale e la Suprema Corte aveva ricondotto le risultanze investigative nell'alveo delle prove atipiche perché l'attività del Pubblico Ministero aveva avuto ad oggetto non un flusso di comunicazioni, ma «una relazione operativa tra microprocessore e video del sistema elettronico», ossia un'attività confi-

[10] Cass. pen, sez. V, 14 ottobre 2009, n. 16556, *CED* 246954.

nata esclusivamente all'interno del dispositivo acquisita poi come mero documento.
Alla luce della più recente giurisprudenza come quella appena citata, tutto ciò che è contenuto in uno smartphone e non sottoposto a captazione di flusso (intercettazione) è teoricamente visualizzabile e, quindi, acquisibile come mero documento (informatico): nel codice di procedura penale non esiste la definizione di cosa sia un documento informatico ma è obbligatorio il rimando a l'unica giuridicamente fondata ovvero quella prevista dal Codice dell'Amministrazione Digitale (d.lgs. 82/2005 e successive modificazioni) secondo cui è documento informatico «la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti».
Così anche sms e chat ritenute non meritevoli della tutela costituzionale e processuale relativa alla corrispondenza (art. 15 Cost e artt. 254 ss. c.p.p.) atteso che la più recente giurisprudenza sul punto[11] ha stabilito che «Non è applicabile la disciplina dettata dall'art. 254 cod. proc. pen. in tema di sequestro di corrispondenza, bensì quella prevista dall'art. 234 stesso codice, concernente i documenti, con riferimento a messaggi WhatsApp e SMS rinvenuti in un telefono cellulare sottoposto a sequestro, in quanto questi testi, non costituendo il diretto obiettivo del vincolo, non rientrano neppure nel concetto di "corrispondenza", la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito».
Tale orientamento è stato confermato da altra, recentissima, sentenza[12] secondo cui «I dati informatici acquisiti dalla memoria del telefono in uso all'indagata (sms, messaggi whatsApp, messaggi di posta elettronica "scaricati" e/o conservati nella memoria dell'apparecchio cellulare) hanno natura di documenti ai sensi dell'art. 234 c.p.p. La relativa attività acquisitiva non soggiace né alle regole stabilite per la corrispondenza, né tantomeno alla disciplina delle intercettazioni telefoniche. Secondo l'insegnamento della Corte di legittimità non è applicabile la disciplina dettata dall'art. 254 c.p.p., con riferimento a messaggi WhatsApp e SMS rinvenuti in un telefono cellulare sottoposto a sequestro, in quanto questi testi non rientrano nel concetto di "corrispondenza", la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito (Sez. 3, n. 928 del 25/11/2015, dep. 2016, *Giorgi*, Rv. 265991). Non è configurabile neppure un'attività di intercettazione, che postula, per sua natura, la captazione di un flusso di comunicazioni in corso, mentre nel caso di specie ci si è limitati ad acquisire ex post il dato, conservato in memoria, che quei flussi documenta».

4. La nuova disciplina su intercettazioni (e captatori)

Negli ultimi anni sono stati diverse le proposte volte a normare una così difficile materia come quella dei captatori informatici: innanzi tutto il d.l. 18 febbraio 2015, n. 7 "Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione

[11] Cass. pen., sez. III, 25 novembre 2015, n. 928, *CED* 265991.

[12] Cass. pen., sez. V, 16 gennaio 2018, n. 1822, in *Processo Penale e Giustizia.*

alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione", convertito successivamente con la l. 43/2015. che inizialmente prevedeva la modifica dell'art. 266-*bis* c.p.p. prevedendo di poter eseguire intercettazioni informatiche anche «attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico».

Una proposta scarna, insufficiente che aveva destato numerose perplessità negli addetti ai lavori e che fu stralciata in sede di conversione della legge.

Tentativi simili furono effettuati rispettivamente dalle proposte di legge C. 3470 del 2 dicembre 2015 e C. 3762 del 20 aprile 2016.

Quest'ultima, in particolare, promossa dal deputato Stefano Quintarelli dal titolo «Disciplina dell'uso dei Captatori legali nel rispetto delle garanzie individuali»[13], è stata redatta dopo un lavoro di quasi due anni che ha coinvolto un gruppo di esperti "giuridici e tecnologici" e poi sottoposto a consultazione pubblica.

Tale proposta di legge prevedeva:

- una definizione ben precisa dei reati per i quali sarebbe stato possibile l'uso dei captatori;
- la previsione che la richiesta di poter utilizzare un captatore a fini intercettivi dovesse essere redatta dal Pubblico Ministero e convalidata da un giudice, il quale avrebbe disposto quindi «l'osservazione dei dispositivi installati e l'acquisizione da remoto dei dati contenuti», aggiungendo inoltre che il decreto autorizzativo dovesse essere notificato all'indagato entro 40 giorni dall'inizio dell'attività captativa del trojan;
- l'introduzione dell'art. 254-*ter* c.p.p., come nuovo mezzo di ricerca della prova denominato «osservazione e acquisizione da remoto»;
- la necessità dell'esecuzione materiale delle operazioni di intercettazione solo tramite la polizia giudiziaria e non tramite soggetti terzi;
- il necessario possesso, da parte dei captatori informatici, di determinati requisiti, «requisiti stabiliti con regolamento del Ministro della Giustizia, di concerto con il Ministro dell'Interno e su parere conforme del Garante per la Protezione dei dati personali», prevedendo in particolare un sistema di omologazione dei captatori affidato all'Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) e, allo stesso tempo, la creazione di un Registro Nazionale dei Captatori informatici prevedendo altresì il diritto per la difesa dell'imputato di ottenere la documentazione relativa a tutte le operazioni effettuate con il captatore informatico, dalla sua installazione fino alla sua rimozione, garantendo anche la verifica del codice sorgente per escludere manipolazioni.

La riforma attuata dalla l. 23 giugno 2017, n. 103 (Riforma Orlando) "Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario" ha previsto un apposito punto della delega all'art. 1, c. 84, lett. *e)* relativo ai criteri direttivi da seguire nel «disciplinare le intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in dispositivi elettronici portatili».

L'attuazione del predetto punto è stata inserita nell'art. 4 del d.lgs. 216 del 29 dicembre

[13] www.civicieinnovatori.it/wp-content/uploads/2017/02/2017.01.31-09_20-Conf.-stampa.pdf

2017; nella relazione illustrativa dello schema del decreto legislativo viene posto l'accento sulla novità di tale strumento investigativo e si evidenzia la pervasività di detto strumento: «l'utilizzo del cosiddetto "trojan" – o, appunto, captatore informatico –, pur ampiamente praticato nella realtà investigativa, non è stato in precedenza oggetto di alcuna regolamentazione a livello normativo. Come noto, si tratta di un malware occultamente installato dall'inquirente su un apparecchio elettronico dotato di connessione internet attiva, il quale consente in ogni momento all'attaccante di captare tutto il traffico dati (sia in entrata che in uscita), di attivare da remoto il microfono e la telecamera registrandone le attività, di "perquisire" gli hard disk e di fare copia integrale del loro contenuto, di intercettare tutto quanto digitato sulla tastiera, di fotografare le immagini ed i documenti visualizzati».

Il *focus* del legislatore è incentrato, innanzi tutto, sul luogo ove le intercettazioni a mezzo captatore possono essere effettuate, limitandosi a codificare la giurisprudenza della Corte di legittimità[14].

Il nuovo art. 266 c.p.p., rubricato "Limiti di ammissibilità", prevede che l'attivazione del dispositivo è sempre consentita nel caso si proceda per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater* c.p. mentre, fuori da tali casi, nei luoghi di cui all'art. 614 c.p. soltanto qualora vi sia il fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

Difformemente dalla decisione delle Sezioni unite n. 26889 del 2016 che considerava una definizione estensiva di reato associativo andando a comprendere qualsiasi forma di associazione a delinquere, il legislatore del 2017 ha previsto i limiti di cui all'art. 51 commi 3-*bis* e 3-*quater*.

Il nuovo testo dell'art. 266 c.p.p., c. 2, quanto ai requisiti di ammissibilità, prevede che nei medesimi casi di cui al c. 1 «è consentita l'intercettazione di comunicazioni tra presenti, che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa».

Il c. 2-*bis* del medesimo art. 266 c.p.p. disciplina poi che «l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater».

Una prima perplessità è sulla locuzione "dispositivo elettronico portatile" che si presterà sicuramente per la propria ambiguità a interpretazioni difformi e che chiude le porte a qualsiasi tipo di attività captativa su dispositivi che portatili non sono: il legislatore segue il solco tracciato dalle Sezioni unite della Cassazione (Scurato) sul tema delle operazioni di intercettazioni "tra presenti" da svolgersi nei luoghi di privata dimora, effettuate proprio a mezzo di captatore informatico installato su un dispositivo portatile con attivazione del microfono trascurando tutti gli altri possibili utilizzi del trojan a fini investigativi.

Il *focus* del legislatore avrebbe dovuto essere un altro, come nella accennata proposta

[14] E. Jannuzzi- A. Regi, *Riforma Orlando e captatori informatici: il difficile compito del Legislatore nel riuscire a stare al passo con la tecnologia*, in www.medialaws.eu, 23 ottobre 2017.

di riforma Quintarelli, al fine di normare e disciplinare uno strumento così invasivo considerandone tutte le potenziali implicazioni.
Ed è indubbio ritenere che la giurisprudenza di legittimità, se pur attraverso poche pronunce, ha negli ultimi anni approfondito la tematica dei captatori informatici comprendendo molto meglio l'ampiezza del problema rispetto al più recente legislatore, passando da una loro qualificazione come fonti prove atipiche a un tentativo di fornir loro una definizione e una copertura normativa quali mezzi di ricerca della prova.
Il legislatore, invece, nonostante il fermento giurisprudenziale dello scorso anno con le sentenze Scurato e Occhionero, non ha fornito una adeguata copertura normativa alle diverse tipologie di attività svolte dai captatori come avrebbe potuto e dovuto fare.
I software captatori sono utilizzati da più di un decennio a fini investigativi e da ancor più tempo a fini di *surveillance* e spionaggio: a parere di chi scrive i tempi erano maturi per definire e normare per lo meno le più utilizzate attività del software-spia fornendo diversi livelli di pervasività dello strumento in relazione alla tipologia di reato e alla sua gravità alla luce del principio di proporzionalità.
La più attenta dottrina[15] e le associazioni forensi ben avevano illustrato la criticità del ricondurre uno strumento così invasivo e tecnico (non si dimentichi che ci si muove all'interno dell'alveo della prova scientifica) nell'area delle prove atipiche ma così, allo stato, sarà, con conseguente lesione dei diritti difensivi in capo all'indagato.
Al P.M. è concesso, peraltro, di procedere con decreto motivato nei casi di urgenze demandando tale attività di captazione (avvio e cessazione) anche a persone idonee di cui all'art. 348, c. 4, c.p.p.: molto diverso da quella riforma Quintarelli che prevedeva l'esclusione di tale ultima possibilità proprio attesa la grande pervasività dello strumento e l'opportunità che i dati carpiti dallo stesso fossero in possesso unicamente delle autorità inquirenti.
Non sono stati pochi, negli ultimi anni, i casi di attività di intercettazioni illecite o *data breach* di società fornitrici per le Procure di software spia: sarebbe stato, quindi, opportuno, impedire l'accesso a tali dati a persone estranee all'apparato investigativo.
La riforma in esame appare, allo stato, una opportunità persa di regolare compiutamente tutte le diverse possibilità offerte dalle nuove tecnologie dettando regole chiare e univoche.
Sarà compito esclusivo del Ministero della Giustizia emanare il relativo disciplinare tecnico relativo alla tipologia dei captatori da utilizzare: i disciplinari tecnici nella normazione di materie relative all'informatica giuridica sono una parte fondamentale.
Vedremo se saranno ascoltati tutti i tecnici, consulenti ed esperti che da anni studiano questi programmi e ne conoscono tutte le enormi potenzialità e relativi pericoli e che richiedono, oltre all'emanazione di un disciplinare tecnico, un sistema esterno di verifica, certificazione e trust delle operazioni effettuate[16]: ad una prima lettura della norma il riferimento esclusivo al Ministero della Giustizia sembra escludere tale possibilità.
Per ora nel testo del decreto appaiono solo scarni riferimenti (con la modifica dell'art.

---

[15] G. Lasagni, *L'uso dei captatori informatici (trojans) nelle intercettazioni "tra presenti"*, in *Diritto Penale Contemporaneo*, 7 ottobre 2016.

[16] G. Ziccardi, *Parlamento Europeo, captatore informatico e attività di hacking delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche*, in *Archivio Penale*, 1, 2017, 234 ss.

89 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale) al tipo di software utilizzato e al luogo ove lo stesso verrà attivato senza nessun riferimento alla progettazione e alla conformità dello stesso («Quando si procede ad intercettazione delle comunicazioni e conversazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile, il verbale indica il tipo di programma impiegato e i luoghi in cui si svolgono le comunicazioni o conversazioni»).
Nessun accenno appare poi riconducibile direttamente alla conservazione dei relativi file di log: le nuove norme prevedono che « le comunicazioni intercettate sono trasferite, dopo l'acquisizione delle necessarie informazioni in merito alle condizioni tecniche di sicurezza e di affidabilità della rete di trasmissione, esclusivamente verso gli impianti della procura della Repubblica. Durante il trasferimento dei dati sono operati controlli costanti di integrità, in modo da assicurare l'integrale corrispondenza tra quanto intercettato e quanto trasmesso e registrato».
Vedremo nel disciplinare tecnico come questi aspetti verranno normati certo è che si parla di requisiti tecnici e non di certificazioni od omologazioni.
Ad ogni modo, allo stato, non vi è alcun accenno a un possibile diritto della difesa di ottenere la documentazione relativa a tutte le operazioni effettuate con il captatore informatico, dalla sua installazione fino alla sua rimozione, garantendo anche la verifica del codice sorgente per escludere manipolazioni.
Staremo a vedere.

Altri saggi

Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-*ter*, c. 2, n. 1, c.p.)*

Sergio Seminara

Abstract

Il saggio esamina i diversi indirizzi interpretativi formatisi in relazione al delitto di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente, soffermandosi in particolare su due sentenze delle sezioni unite della Cassazione, che giungono a esiti opposti in ordine alla configurabilità dell'art. 615-*ter,* c. 2, n. 1, c.p. Attraverso l'esegesi della norma e la disamina della sua interpretazione giurisprudenziale, l'Autore espone le ragioni che ostano a una ricostruzione del reato in parola come forma di eccesso o sviamento di potere del pubblico agente.

The essay explores the different views taken by Italian courts on the construction of the crime of unauthorized access to computer or telecommunications systems committed by a public servant. In particular, the Author focuses on two recent stances of the Italian Supreme Court whereby different approaches emerged with respect to the possible framing of the crime provided for by Article 615-*ter,* c. 2, no. 1, of the Italian Criminal Code. In light of the interpretation of this provision and the relevant case law, the Author argues that this crime cannot be framed as result of a misuse of power by public servants.

Sommario

1. Introduzione: il quadro normativo. – 2. L'evoluzione giurisprudenziale. – 3. La scomposizione del problema nei suoi distinti aspetti. – 4. Il bene giuridico tutelato dall'art. 615-*ter* c.p. – 4.1. La tutela penale della riservatezza e della segretezza. – 5. La struttura oggettiva o soggettiva della fattispecie. – 6. Il rapporto tra i commi 1 e 2 e la nozione di abuso. – 7. Conclusioni.

Keywords: Accesso abusivo a sistema informatico o telematico, Reati informatici, Cybercrime, Riservatezza, Sistemi informativi

1. Introduzione: il quadro normativo.

L'art. 615-*ter,* c. 1, c.p. sanziona con la reclusione fino a tre anni chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ov-

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

vero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. La norma è inserita nel codice penale tra i «delitti contro la inviolabilità del domicilio» e risulta costruita in aderenza al paradigma del reato di violazione di domicilio: l'art. 614 infatti punisce, con la reclusione da sei mesi a tre anni, chiunque si introduce nell'altrui privata dimora contro la volontà espressa o tacita di chi ha il diritto di escluderlo o vi si trattiene in violazione dell'altrui volontà espressa ovvero agisce clandestinamente o con inganno.

Stabilito dunque il parallelismo tra le due fattispecie, entro i limiti in cui lo consente l'accostamento tra realtà fisiche e virtuali[1], la questione insorge quando soggetto attivo sia un pubblico agente che si introduce o si mantiene all'interno del sistema abusando dei suoi poteri o violando i propri doveri, per lecite o illecite ragioni personali. Qui la specularità fra gli artt. 614 e 615-*ter* trova conferma nella procedibilità di ufficio del fatto ora considerato rispetto alla perseguibilità a querela della fattispecie base, ma al tempo stesso risulta negata in quanto, per l'ipotesi di abuso del pubblico agente, l'art. 614 cede il posto all'art. 615, che prevede un reato autonomo per la violazione di domicilio commessa da un pubblico ufficiale con abuso dei poteri, mentre l'art. 615-*ter* rinvia a una circostanza aggravante soggettiva prevista nel c. 2, n. 1.

A sua volta – e così dicendo viene messo definitivamente a fuoco l'oggetto di queste riflessioni –, l'art. 615-*ter*, c. 2, n. 1 appare formulato in termini assai problematici, non essendo chiaro il rapporto che intercorre tra l'abuso *ex* c. 1, caratterizzante l'introduzione o il mantenimento nel sistema, e l'abuso dei poteri tipizzato nel c. 2, n. 1 insieme alla violazione dei doveri funzionali.

La giurisprudenza, soprattutto nell'ultimo decennio (l'art. 615-*ter* è stato introdotto dall'art. 4 l. 23 dicembre 1993, n. 547), ha operato interpretazioni di segno contrastante, culminate in due divergenti pronunce delle Sezioni unite, intervenute nel 2011 e nel 2017.

2. L'evoluzione giurisprudenziale

Al fine di chiarire l'essenza del problema, conviene preliminarmente notare che il pubblico ufficiale o l'incaricato di un pubblico servizio, il quale si introduce o si mantiene all'interno di un sistema informatico o telematico per ragioni private e personali, può disporre di un'abilitazione per lo svolgimento di attività connesse alla funzione ovvero può essere sfornito di qualsiasi titolo di accesso. In questa seconda ipotesi, se il fatto viene commesso fuori da qualsiasi contesto funzionale è ovviamente priva di rilievo la qualifica dell'agente e si configura solo l'art. 615-*ter,* c. 1; ove invece il soggetto si sia avvalso della propria posizione, ad esempio per ottenere la *password*, è ravvisabile l'abuso dei poteri tipizzato dall'art. 615-*ter*, c. 2, n. 1. I dubbi e le difficoltà interpretative emergono al momento di stabilire la sussistenza della fattispecie aggravata nei confronti del pubblico ufficiale o dell'incaricato di un pubblico servizio che, per ragioni private,

[1] Per la critica a una nozione di domicilio informatico intesa come perfettamente speculare a quella di domicilio fisico, tra gli altri, C. Pecorella, *Diritto penale dell'informatica*, Padova, 2006, 315 s.; L. Picotti, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in Id. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 59 ss.

si introduce o si mantiene all'interno del sistema utilizzando un proprio valido titolo di abilitazione.

In giurisprudenza, fino a pochi anni fa, trovavano alterno riscontro due opposte soluzioni, l'una volta a escludere la ricorrenza dell'art. 615-*ter* ogni volta che l'imputato detenesse legittimamente i profili di autenticazione, giacché il requisito dell'abusività rinvia a un difetto di autorizzazione e la contraria volontà del titolare del sistema va riferita esclusivamente alla condotta di accesso o mantenimento, senza riguardo per le finalità perseguite dall'agente[2]; l'altra invece tesa ad affermare l'integrazione del reato, in base all'assunto che ogni accesso per fini e ragioni estranee a quelle consentite dall'abilitazione risulta abusivo o comunque si risolve in una permanenza all'interno del sistema che evoca necessariamente il tacito dissenso del titolare di esso[3].

Per la comprensione anche degli svolgimenti successivi, è opportuno rimarcare che entrambi gli orientamenti si riferivano all'art. 615-*ter,* c. 1, rispettivamente negando o ammettendo la natura abusiva dell'introduzione o del mantenimento nel sistema alla luce dell'abilitazione dell'agente ovvero della presunta volontà contraria del titolare del sistema. La situazione di contrasto imponeva comunque un intervento delle Sezioni unite, che – all'interno della prospettiva ora delineata – nel 2011 vengono chiamate ad esprimersi sulla seguente questione di diritto: «se integri la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto abilitato ma per scopi o finalità estranei a quelli per i quali la facoltà di accesso gli è stata attribuita»[4].

La soluzione adottata dalle Sezioni unite è netta quanto al ripudio dell'interpretazione che lega il reato alla direzione finalistica della condotta, affermandosi che lo *ius excludendi* del titolare del sistema «si connette soltanto al dato oggettivo della permanenza (per così dire "fisica") dell'agente in esso. Ciò significa che la volontà contraria dell'avente diritto deve essere verificata solo con riferimento al risultato immediato della condotta posta in essere, non già ai fatti successivi»[5]. Ai fini della valutazione sulla legittimità dell'accesso – prosegue la Corte –, occorre tenere conto della «oggettiva violazione delle disposizioni del titolare in ordine all'uso del sistema. Irrilevanti devono considerarsi gli eventuali fatti successivi: questi, se seguiranno, saranno frutto di nuovi atti volitivi e, pertanto, se illeciti, saranno sanzionati con riguardo ad altro titolo di reato»;

---

[2] Cass. pen., sez. V, 17 gennaio 2008, n. 2534; Cass. pen., sez. V, 3 luglio 2008, n. 26797; Cass. pen., sez. VI, 21 ottobre 2008, n. 39290 (ove si critica l'espressione «abusivamente si introduce» a causa della «sua forte ambiguità e la conseguente possibilità d'imprevedibili e pericolose dilatazioni della fattispecie penale se non intesa in senso di "accesso non autorizzato"»); Cass. pen., sez. V, 14 ottobre 2009, n. 40078.

[3] Cass. pen., sez. V, 6 dicembre 2000, n. 12732; Cass. pen., sez. V, 1° ottobre 2008, n. 37322; Cass. pen., sez. V, 16 gennaio 2009, n. 1727; Cass. pen., sez. V, 30 aprile 2009, n. 18006; Cass. pen., sez. V, 22 gennaio 2010, n. 2987; Cass. pen., sez. V, 21 maggio 2010, n. 19463; Cass. pen., sez. V, 10 novembre 2010, n. 39620 (quest'ultima però relativa a un caso di accesso fraudolento). Per una ricostruzione della giurisprudenza sul punto C. Pecorella, *Art. 615*-ter, in *Codice penale commentato*, diretto da E. Dolcini-G. Gatta, Milano, 2015, III, 605 s.

[4] L'ordinanza di rimessione è in Cass. pen., sez. V, 23 marzo 2011, n. 11714.

[5] Questa soluzione trova una conferma nella tipizzazione delle condotte di introduzione e di mantenimento nel sistema, nel senso che la seconda condotta sarebbe pleonastica «se la prima fosse integrata anche da chi usa la legittimazione all'accesso per fini diversi da quelli cui è stato legittimato dal titolare del sistema»: così Cass. pen., sez. VI, 21 ottobre 2008, n. 39290; Cass. pen., sez. V, 14 ottobre 2009, n. 40078.

più specificamente, il dissenso del *dominus loci* va stabilito esclusivamente sulla base di «quelle disposizioni che regolano l'accesso al sistema e che stabiliscono per quali attività e per quanto tempo la permanenza si può protrarre, (…) mentre devono ritenersi irrilevanti, ai fini della configurazione della fattispecie, eventuali disposizioni sull'impiego successivo dei dati». Da notare come, in un passaggio intermedio, la sentenza equipari alla violazione delle prescrizioni impartite dal titolare del sistema la realizzazione di «operazioni di natura ontologicamente diversa da quelle di cui egli (= il soggetto attivo) è incaricato ed in relazione alle quali l'accesso era a lui consentito. In questi casi è proprio il titolo legittimante l'accesso e la permanenza nel sistema che risulta violato: il soggetto agente opera illegittimamente, in quanto il titolare del sistema medesimo lo ha ammesso solo a ben determinate condizioni, in assenza o attraverso la violazione delle quali le operazioni compiute non possono ritenersi assentite dall'autorizzazione ricevuta»[6].

Il ricorso all'ontologia non costituiva una novità rispetto al tema in esame, poiché già rinvenibile in precedenti sentenze. L'autorevole riconoscimento fornitogli dalle Sezioni unite funziona però da volano per una serie di pronunce successive, che sulla difformità ontologica tra le ragioni funzionali a base dell'abilitazione conferita e le finalità private dell'agente costruisce il concetto di dissenso tacito come presupposto del reato *ex* art. 615-*ter*[7]. In un siffatto contesto si inserisce in particolare una sentenza che lega «la ontologica incompatibilità dell'accesso al sistema informatico (…) a un utilizzo dello stesso fuoriuscente dalla *ratio* del conferimento del relativo potere», sulla base dell'art. 1 della l. 7 agosto 1990, n. 241[8]: dopo questo primo richiamo ai generali principi dell'attività amministrativa, altre decisioni evocheranno il vincolo di fedeltà posto a carico di tutti i pubblici dipendenti, l'interesse al buon andamento e all'imparzialità della pubblica amministrazione, l'obbligo di riservatezza sancito dagli artt. 335 c.p.p. e 110-*bis* disp. att. c.p.p., fino a convertire l'art. 615-*ter* in una norma sanzionatoria di un abuso di potere. Inevitabile, dunque, un nuovo intervento delle Sezioni unite.

A questo punto della ricostruzione è opportuno però un chiarimento. Nella già riferita decisione delle Sezioni unite, l'"ontologica" diversità tra le condotte autorizzate e quelle rilevanti penalmente assumeva una valenza meramente negativa, riferita all'assenza di legittimazione, senza alcun riguardo per il finalismo dell'agente o per la lesione

[6] Cass. pen., sez. un., 7 febbraio 2012, n. 4694, commentata da R. Bartoli, *L'accesso abusivo a un sistema informatico (art. 615* ter *c.p.) a un bivio teleologicamente orientato*, in *Dir. pen. cont.*, 2012, 1, 123 ss.; R. Flor, *Verso una rivalutazione dell'art. 615* ter *c.p.?*, *ivi*, 2, 2012, 126 ss.; C. Pecorella, *L'attesa pronuncia delle Sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Cass. pen.*, 2012, 3692 ss. Conf. Cass. pen., sez. V, 18 aprile 2012, n. 15054; Cass. pen., sez. II, 22 marzo 2013, n. 13475; Cass. pen., sez. V, 24 ottobre 2014, n. 44390; Cass. pen., sez. V, 10 marzo 2015, n. 10083; Cass. pen., sez. V, 16 aprile 2015, n. 15950.

[7] Tra le altre Cass. pen., sez. V, 13 marzo 2017, n. 11994; Cass. pen., sez. V, 25 gennaio 2017, n. 3818; Cass. pen., sez. V, 19 agosto 2016, n. 35127; Cass. pen., sez. V, 29 luglio 2016, n. 33311; Cass. pen., sez. V, 6 luglio 2016, n. 27883; Cass. pen., sez. V, 15 febbraio 2016, n. 6176; Cass. pen., sez. V, 3 novembre 2015, n. 44403.

[8] Cass. pen., sez. V, 22 maggio 2013, n. 22024. *Contra* Cass. pen., sez. V, 24 ottobre 2014, n. 44390, che lega l'abusività della condotta esclusivamente alle disposizioni impartite dal *dominus loci*, negando rilevanza alle disposizioni – come l'art. 1, l. 241 del 1990 – che regolano l'attività amministrativa.

del bene della riservatezza[9]. Al contrario, la successiva giurisprudenza aveva utilizzato l'ontologia in un'accezione positiva come abuso di potere, in grado di esprimere il nucleo di illiceità della condotta.

Si comprende così che il nuovo quesito sottoposto alle Sezioni unite questa volta concerne non più l'art. 615-*ter* ma il suo c. 2, n. 1, del quale si chiede se «sia integrato anche nella ipotesi in cui il pubblico ufficiale o l'incaricato di pubblico servizio, formalmente autorizzato all'accesso ad un sistema informatico o telematico, ponga in essere una condotta che concreti uno sviamento di potere, in quanto mirante al raggiungimento di un fine non istituzionale, pur in assenza di violazione di specifiche disposizioni regolamentari ed organizzative»[10].

Come si vede, alle Sezioni unite viene ora prospettato il netto superamento della posizione precedentemente assunta mediante un ribaltamento della questione di diritto: come nel 2011 era stato chiesto di stabilire se la configurabilità dell'art. 615-*ter* fosse subordinata all'assenza di abilitazione o alla violazione delle prescrizioni impartite dal titolare del sistema, ora si propone una lettura che rende irrilevante la disciplina apposta dal gestore mediante uno sganciamento dal c. 1 del c. 2, n. 1, al fine di riferire quest'ultimo all'eccesso di potere legato al fine privato perseguito. Va da sé che in questa nuova prospettiva si realizza anche un ribaltamento della descrizione del fatto, poiché l'abusività ora risiede non già nel mantenimento all'interno del sistema contro la volontà tacita del titolare, bensì in un accesso che, se anche formalmente autorizzato, è abusivo in quanto viziato da uno sviamento del potere, contrastante con la volontà presunta del gestore. E le Sezioni unite si esprimono proprio in questo senso.

La decisione delle Sezioni unite non risulta ispirata da una rigorosa coerenza. Dopo avere affermato in esordio il carattere abusivo dell'accesso *ex* art. 615-*ter* «qualora avvenga mediante superamento e violazione delle chiavi fisiche ed informatiche di accesso o delle altre esplicite disposizioni su accesso e mantenimento date dal titolare del sistema», l'esegesi risulta incentrata esclusivamente sul c. 2, n. 1. Rispetto a questo, i giudici escludono che si tratti di un reato autonomo, alla luce del rilievo che per il pubblico agente, l'investigatore privato e l'operatore del sistema «il reato è sempre aggravato, proprio perché la circostanza è inscindibilmente collegata a quella qualità soggettiva ed in tutti i casi la configurata aggravante comporta un abuso, che ben può connotarsi delle caratteristiche dell'esecuzione di "operazioni ontologicamente estranee" rispetto a quelle consentite». Si tratta di un evidente paralogismo, poiché la qualifica aggrava il reato solo in quanto nel fatto ricorra un abuso dei poteri o della qualità ovvero un esercizio professionale, non potendosi dubitare che altrimenti quei soggetti rispondono come privati cittadini; ma esso è funzionale a raggiungere il medesimo risultato interpretativo derivante dalla costruzione del c. 2, n. 1 come reato autonomo.

Allo scopo di evitare la concezione oggettiva dell'abuso precedentemente sancita dalle Sezioni unite, infatti, la sentenza dapprima identifica l'abuso *ex* c. 2, n. 1 in un eccesso o sviamento di potere e quindi, facendo coincidere questo abuso con quello di cui al c. 1, perviene al risultato che «non esce dall'area di applicazione della norma la situazione nella quale l'accesso o il mantenimento nel sistema informatico dell'ufficio a cui è ad-

[9] Per questo rilievo C. Pecorella, *L'attesa pronuncia*, cit., 3704 s.

[10] L'ordinanza di rimessione è in Cass. pen., sez. V, 14 marzo 2017, n. 12264.

detto il pubblico ufficiale o l'incaricato di pubblico servizio, seppur avvenuto a seguito di utilizzo di credenziali proprie dell'agente ed in assenza di ulteriori espressi divieti in ordine all'accesso ai dati, si connoti, tuttavia, dall'abuso delle proprie funzioni da parte dell'agente, rappresenti cioè uno sviamento di potere, un uso del potere in violazione dei doveri di fedeltà che ne devono indirizzare l'azione nell'assolvimento degli specifici compiti di natura pubblicistica a lui demandati»[11].

Attraverso il richiamo dell'art. 1 l. 7 agosto 1990, n. 241, del d.p.r. 16 aprile 2013, n. 62, e degli artt. 54, 97 e 98 Cost. – cioè di buona parte dell'armamentario utilizzato dalla giurisprudenza per fondare la violazione delle norme di legge sulla quale gravita il reato di abuso di ufficio previsto dall'art. 323 c.p. –, la configurabilità dell'art. 615-*ter*, c. 2, n. 1 viene così affermata in ogni caso di «"ontologica incompatibilità" dell'accesso al sistema informatico, connaturata ad un utilizzo dello stesso estraneo alla *ratio* del conferimento del relativo potere»[12].

3. La scomposizione del problema nei suoi distinti aspetti

Al fine di valutare l'interpretazione ora accolta dalle Sezioni unite conviene procedere con ordine, distinguendo i diversi piani dell'indagine.

Più specificamente, trattandosi di un problema interpretativo è opportuno anzitutto muovere alla ricerca del bene protetto dall'art. 615-*ter*.

La seconda fase della riflessione verrà invece dedicata alla ricostruzione, in senso oggettivo o soggettivo, dell'art. 615-*ter*, in modo da verificare la consistenza delle divergenti ricostruzioni nella giurisprudenza di legittimità. In tale prospettiva, utili spunti verranno offerti anche dalla considerazione del momento consumativo del reato e della trama codicistica in riferimento alla tutela della riservatezza e della segretezza.

L'ultimo stadio della ricerca avrà ad oggetto la nozione di abuso sia nel c. 1 che nel c. 2,

[11] La decisione delle Sezioni unite si muove così nel solco tracciato dall'ordinanza di rimessione, le cui cadenze argomentative possono essere così sintetizzate: la difformità tra le ragioni funzionali dell'abilitazione e le finalità private dell'introduzione o del mantenimento nel sistema si risolve in una «violazione di normative non regolamentari ma, ancor prima, di livello legislativo, ossia quelle concernenti il vincolo di fedeltà cui sono tenuti indistintamente tutti i pubblici dipendenti, oltre che in violazione dell'interesse al corretto funzionamento ed all'imparzialità della pubblica amministrazione»; l'art. 615-*ter* cpv. «induce a ritenere censurabile, comunque, la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che si estrinsechi in un abuso dei poteri conferitigli, tra cui – evidentemente – quello di accessi non istituzionali, e quindi ponendo in essere una condotta formalmente corretta ma ontologicamente difforme dalle finalità operative di cui egli è incaricato»; infine, «almeno con riferimento ai soggetti di cui sopra (e dunque alla ipotesi di cui al c. 2, n. 1, dell'art. 615 *ter* c.p.), le finalità per le quali essi accedono ad (o si trattengono in) un sistema informatico, posto funzionalmente (*scilicet*: per esigenze di servizio) a loro disposizione, non possono essere considerate ininfluenti ai fini della configurazione del delitto in questione» (Cass. pen., sez. V, 14 marzo 2017, n. 12264; la medesima impostazione in esame si rinviene già in Cass. pen., sez. V, 21 maggio 2010, n. 19463).

[12] Cass. pen., sez. un., 8 settembre 2017, n. 41210, criticamente annotata da F. Fasani, *Accesso abusivo a un sistema informatico: le Sezioni Unite cambiano di nuovo rotta*, in *Soc.*, 2017, 1393 ss.; R. Flor, *La condotta del pubblico ufficiale fra violazione della* voluntas domini, *"abuso" dei profili autorizzativi e "sviamento di potere"*, in *Dir. pen. proc.*, 2018, 506 ss. In senso conforme alle Sezioni unite, da ult., Cass. pen., sez. VI, 4 maggio 2018, n. 19497; Cass. pen., sez. V, 12 gennaio 2018, n. 1021.

n. 1 dell'art. 615-*ter*, al fine di accertare il fondamento dell'interpretazione fornita dalle Sezioni unite nel 2017.

4. Il bene giuridico tutelato dall'art. 615-*ter* c.p.

L'art. 615-*ter* c.p. è inserito nel titolo XII (Dei delitti contro la persona), capo III (Dei delitti contro la libertà individuale), sezione IV (Dei delitti contro la inviolabilità del domicilio).

Questa collocazione trova una giustificazione nel suo immediato antecedente storico, costituito dalla Raccomandazione sulla criminalità informatica 13 settembre 1989, n. R(89)9, del Comitato dei Ministri del Consiglio d'Europa, che invitava i legislatori nazionali a prevedere, tra l'altro, una norma che incriminasse l'«accesso non autorizzato» a un sistema informatico, al fine di apprestare «una protezione, in via anticipata e indiretta, contro i rischi di manipolazioni informatiche, di danneggiamento dei dati e di spionaggio informatico»[13]; la medesima prescrizione sul divieto di accesso non autorizzato a sistemi di informazione veniva poi reiterata nell'art. 2 della Convenzione del Consiglio d'Europa sulla criminalità informatica, adottata a Budapest il 23 novembre 2001 e nell'art. 2 della Decisione quadro 2005/222/GAI del 24 febbraio 2005.

Sulla scorta di tale precedente deve convenirsi che l'art. 615-*ter* c.p. è stato introdotto nell'ordinamento «per assicurare una protezione all'ambiente informatico o telematico che contiene dati personali che devono rimanere riservati e conservati, al riparo da ingerenze ed intrusioni altrui, e rappresenta un luogo inviolabile, delimitato da confini virtuali, paragonabile allo spazio privato dove si svolgono le attività domestiche»[14].

Al di là di ogni pretesa di identificazione tra il domicilio reale e il domicilio informatico, la norma in esame tutela dunque uno spazio di riservatezza, cioè una sfera di manifestazione della personalità individuale o di autodeterminazione della propria vita privata[15]. La stessa sistemazione del codice penale, ove i reati contro l'inviolabilità del

[13] Conseil de l'Europe, *La criminalité informatique*, 1990, 56 s.

[14] Testualmente Cass. pen., sez. un., 24 aprile 2015, n. 17325. Vd. pure Cass. pen., sez. V, 3 luglio 2008, n. 26797.

[15] Con varietà di accenti, tra gli altri, M. Bellacosa, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni unite*, in *Dir. pen. cont.*, 2 febbraio 2015, 6; F. Fasani, *Accesso abusivo*, cit., 1404; G. Fiandaca – E. Musco, *Diritto penale*, *pt. sp.*, Bologna-Roma, 2013, II t. I, 293; F. Mantovani, *Diritto penale*, *pt. sp.*, Padova, 2016, I, 577; C. Pecorella, *Diritto penale dell'informatica*, cit., 322 ss.; Ead., *L'attesa pronuncia*, cit., 3694 s.; C. Piergallini, *I delitti contro la riservatezza informatica*, in C. Piergallini – F. Viganò – M. Vizzardi – A. Verri, *I delitti contro la persona*, in *Trattato di diritto penale*, *pt. sp.*, diretto da G. Marinucci-E. Dolcini, Milano, 2015, X, 772 s. Vd. anche L. Picotti, *La tutela penale della persona*, cit., 59 ss., il quale, senza evocare dimensioni plurioffensive, sottolinea l'esigenza di tutela dello spazio cibernetico e la stretta connessione funzionale tra riservatezza e sicurezza informatiche (conf. Id., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. Picotti (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 80 ss.); analogamente R. Flor, *La condotta del pubblico ufficiale*, cit., 512; I. Salvadori, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in *Tutela penale della persona e nuove tecnologie*, cit., 147 ss.; per una critica alla commistione tra riservatezza e sicurezza Cass. pen., sez. V, 29 luglio 2016, n. 33311. Nel senso invece di intendere l'accesso abusivo come accesso alla conoscenza dei dati contenuti nel sistema G. Aronica, *L'accesso abusivo ad un sistema informatico o telematico (art. 615* ter *c.p.) nella giurisprudenza*, in *Ind. pen.*, 2010, 220.

domicilio precedono quelli contro l'inviolabilità dei segreti, conferma che la nozione di riservatezza va intesa come pacifico godimento della propria sfera privata, indipendentemente dal successivo utilizzo dei dati o dei fatti la cui conoscenza viene preclusa a quanti siano privi di una facoltà di accesso. Solo nella prospettiva delineata si comprende il motivo per cui i reati di cui agli artt. 614 e 615-*ter* sono integrati con l'abusiva introduzione o mantenimento nel domicilio, evitando di tipizzare qualsiasi ulteriore evento di danno o di pericolo.

Fermiamoci un momento. Alla conclusione ora raggiunta potrebbe obiettarsi che, a differenza del domicilio reale, per quello virtuale l'art. 615-*ter* subordina la tutela alla presenza di misure di sicurezza, che starebbero a dimostrare uno spostamento dall'asse della riservatezza a quello della segretezza e degli ulteriori interessi che il vincolo del segreto è inteso a proteggere[16]. Ma non è così, poiché alle misure di sicurezza viene attribuita la funzione di manifestare all'esterno quello *ius excludendi* che è implicito nel domicilio fisico e che, soprattutto nel mondo della rete, non caratterizza necessariamente ogni sistema: è pertanto indifferente che tali misure siano adeguate od obsolete, facilmente o difficilmente aggirabili, poiché la loro rilevanza si esaurisce in una valenza sintomatica[17], mirata appunto ad assicurare l'equivalenza tra domicilio reale e informatico. A ulteriore conferma dell'assunto, va notato che la norma non richiede una necessaria violazione delle misure di sicurezza, giacché del mantenimento non autorizzato all'interno del sistema risponde anche chi abbia un titolo legittimante l'accesso o questo si sia realizzato in modo casuale[18].

Una volta individuato il bene protetto nella riservatezza, si comprende anche che, legandosi i reati tipizzati dagli artt. 614 e 615-*ter* alla violazione della volontà espressa o tacita del titolare del diritto di esclusione, risulta privo di ogni rilevanza il fine perseguito dal soggetto attivo: che egli sia stato ispirato da mera curiosità, dallo scopo di dimostrare la propria abilità, da un obiettivo di profitto patrimoniale o anche morale ovvero dall'intenzione di recare danno, il reato di cui all'art. 614 o 615-*ter* è allo stesso modo integrato.

Ecco perché appare errata l'affermazione che il reato tipizzato dall'art. 615-*ter* ha natu-

---

[16] Da notare, sul punto, che l'art. 2 della Convenzione del Consiglio d'Europa del 23 novembre 2001 e l'art. 2 della Decisione quadro 2005/222/GAI lasciavano libertà agli Stati in ordine alla previsione del requisito della protezione dei sistemi informatici e telematici mediante misure di sicurezza.

[17] Conf. Cass. pen., sez. un., 24 aprile 2015, n. 17325: «La tutela giuridica è riservata ai sistemi muniti di misure di sicurezza perché, dovendosi proteggere il diritto di uno specifico soggetto, è necessario che questi abbia dimostrato di volere riservare l'accesso alle persone autorizzate e di inibire la condivisione del suo spazio informatico con i terzi». Analogamente Cass. pen., sez. I, 27 settembre 2013, n. 40303, ove espressamente si ammette che le misure di sicurezza possono essere «anche di minima efficacia e facilmente aggirabili», purché assolvano «alla specifica funzione di manifestare la volontà di non diffusione a persone non autorizzate»; conf. Cass. pen., sez. V, 1° ottobre 2008, n. 37322; Cass. pen., sez. II, 14 settembre 2006, n. 30663; Cass. pen., sez. V, 6 dicembre 2000, n. 12732. Nello stesso senso, tra gli altri, R. Flor, *Verso una rivalutazione*, cit., 131, il quale, affermando l'irrilevanza che le misure siano obiettivamente inefficaci o anche temporaneamente disattivate, giustamente sottolinea come la consumazione del reato si leghi alla violazione dello *ius excludendi* e non alla neutralizzazione delle misure di sicurezza; conf. C. Pecorella, *Diritto penale dell'informatica*, cit., 324 ss.; I. Salvadori, *L'accesso abusivo*, cit., 143 ss. Vd. pure R. Bartoli, *L'accesso abusivo*, cit., 126, secondo cui il requisito delle misure di sicurezza sposta il fulcro del disvalore sullo strumento inteso a fini di conservazione ed elaborazione dei dati personali.

[18] Conf. C. Pecorella, *L'attesa pronuncia*, cit., 3695.

ra plurioffensiva[19]: per quanto sia ovvio e incontestabile che l'accesso abusivo al sistema obbedisce alle finalità più svariate, la norma incrimina l'accesso e non le condotte successive, che eventualmente configurano diversi paradigmi criminosi[20]. Ma, così dicendo, ci siamo avvicinati alla seconda tappa della nostra riflessione.

4.1. La tutela penale della riservatezza e della segretezza

Prima di entrare nel merito della ricostruzione del reato in senso oggettivo o soggettivo, è opportuna una breve digressione.

Alla stregua di quanto finora osservato, gli artt. 614 e 615-*ter* c.p. non sono preposti a proteggere la segretezza di alcunché, come dimostra il rilievo che entrambi i reati risultano integrati indipendentemente dall'accesso a dati o a fatti segreti: l'illecito consiste solo nella violazione della riservatezza assicurata dalla legge al domicilio fisico e al sistema informatico o telematico.

Che fra la tutela della riservatezza e della segretezza sussista una netta separazione è dimostrato dalla trama codicistica, che in tema di inviolabilità dei segreti distingue fra condotte di procacciamento da un lato e condotte di rivelazione e utilizzazione dall'altro: le prime costituiscono oggetto di incriminazione solo relativamente ai segreti di Stato (art. 256 e, per quanto riguarda lo spionaggio, artt. 257 e 258 c.p.), le seconde riguardano invece, oltre i segreti di Stato, i segreti di ufficio e i segreti professionali (rispettivamente, artt. 261 ss., 325 s. e 621 s. c.p.). In sostanza, a seconda della natura del segreto e della sua rilevanza il codice penale stabilisce una tutela graduata: massima nel caso di segreti di Stato, al punto che ne viene già punita l'indebita acquisizione, limitata invece nel caso di segreti di ufficio o professionali, dei quali è sanzionata solo la cessione o lo sfruttamento. All'interno di quest'ultima tipologia di segreti è poi introdotta un'ulteriore differenziazione attinente al regime di procedibilità, poiché la natura pri-

[19] Così Cass. pen., sez. V, 14 marzo 2017, n. 12264, secondo cui l'art. 615-*ter* tutela «interessi molteplici e variegati, rilevanti non solo a livello patrimoniale – come il diritto all'uso indisturbato dell'elaboratore per perseguire fini di carattere economico e produttivo – ma anche a livello pubblicistico – quali il diritto alla riservatezza, i diritti afferenti alla sfera militare, sanitaria, quelli inerenti all'ordine pubblico ed alla sicurezza e, tra essi, anche quello al corretto funzionamento dell'amministrazione giudiziaria»; conf. Cass. pen., sez. V, 1° ottobre 2008, n. 37322. Questa prospettazione nel senso della plurioffensività può tuttavia anche attribuirsi a un'infelice formulazione, giacché essa equivale all'assunto che la norma in esame, nel proteggere la «riservatezza della sfera individuale, quale bene anche costituzionalmente protetto, (…) non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello *jus excludendi alios*, quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia che titolare dello *jus excludendi* sia una persona fisica, persona giuridica, privata o pubblica, o altro ente» (Cass. pen., sez. V, 26 ottobre 2012, n. 42021).

[20] Conf., per tutte, Cass. pen., sez. un., 24 aprile 2015, n. 17325: «Dal momento che oggetto di tutela è il domicilio virtuale, e che i dati contenuti all'interno del sistema non sono in via diretta ed immediata protetti, consegue che l'eventuale uso illecito delle informazioni può integrare un diverso titolo di reato»; analogamente Cass. pen., sez. I, 27 settembre 2013, n. 40303, secondo cui l'art. 615-*ter* esclude la necessità «che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa». Conf., tra gli altri, E. Mengoni, *Accesso autorizzato al sistema informatico o telematico e finalità illecite: nuovo* round *alla configurabilità del reato*, in *Cass. pen.*, 2011, 2205.

vata del segreto giustifica una perseguibilità a querela del reato che, per ovvie ragioni, non ha luogo rispetto ai segreti di ufficio.
Come si vede, la tutela della segretezza si articola su differenti modelli, legati alla natura del segreto, mentre la protezione della riservatezza si svolge su un piano anticipato rispetto alla violazione del segreto e anzi prescinde totalmente da essa. In altre parole, l'incriminazione dell'abusiva introduzione nel domicilio fisico o virtuale rimane distinta dall'apprendimento di dati o fatti segreti, che a sua volta può essere autonomamente sanzionato come procacciamento o può invece costituire un atto preparatorio rispetto al reato consistente nella loro successiva rivelazione o utilizzazione. In ogni caso una tesi che, nell'accesso abusivo a un domicilio o a un sistema informatico o telematico, volesse punire il fine di acquisire abusivamente un segreto determina un'indebita sovrapposizione di piani diversi e si rivela ulteriormente errata per le ragioni che andiamo ora a esaminare.

5. La struttura oggettiva o soggettiva della fattispecie

Il contrasto fra le due sentenze delle Sezioni unite risiede nella natura oggettiva o soggettiva dell'abusività dell'accesso: senza soffermarci sulla notazione che la decisione del 2011 verte sul c. 1 dell'art. 615-*ter* e la decisione del 2017 si concentra invece sul c. 2, n. 1, in ogni caso la prima coglie la natura abusiva dell'introduzione o del mantenimento nell'assenza di abilitazione o nella violazione delle prescrizioni impartite dal titolare del sistema, mentre la seconda fonda l'abusività sull'eccesso o sullo sviamento di potere che finalisticamente connota la condotta dell'agente.
Evitando di indugiare sul rilievo che in entrambe le prospettazioni l'alternativa refluisce nell'art. 615-*ter,* c. 1, in quanto il c. 2 prevede un reato circostanziato (vd. § 6), al fine di sciogliere il dilemma fra le prospettive oggettiva e soggettiva è utile richiamare, a causa della sua specularità, l'art. 614, ipotizzando il caso di chi si rechi in un'abitazione su invito del proprietario ma con l'intenzione di compiervi un furto, così ontologicamente violando le regole dell'ospitalità[21].
In una situazione del genere, però, a nessuno verrebbe in mente di contestare all'ospite il reato di violazione di domicilio, giacché il suo ingresso nell'appartamento era stato autorizzato dal proprietario e non può essere qualificato come clandestino o fraudo-

[21] L'analogia tra gli artt. 614 e 615-*ter* è invocata da Cass. pen., sez. V, 6 dicembre 2000, n. 12732, al fine di affermare la configurabilità del secondo reato nei confronti di «chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Infatti, se l'accesso richiede un'autorizzazione e questa è destinata a un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva». Nel senso del testo invece E. Mengoni, *Accesso autorizzato*, cit., 2205 nota 16.

lento[22]: ciò significa che la configurabilità dell'art. 614 dipende dalla volontà del titolare dello *ius excludendi*, anche se essa risulti frutto di un errore diverso dall'altrui inganno, e le finalità di colui che poi abuserà dell'ospitalità sono assolutamente irrilevanti. Di più: il reato di violazione di domicilio si consuma con l'introduzione nell'abitazione e non può certo la sua configurabilità farsi dipendere dal successivo comportamento dell'agente, a seconda che – si ripete: dopo avere avuto accesso nella privata dimora – egli rispetti o no le leggi dell'ospitalità. Invero, il delitto *ex* art. 614 gravita non sull'*animus* del soggetto attivo, bensì sull'esercizio del diritto di esclusione da parte del titolare di esso ovvero, per il caso di mantenimento, sulla violazione delle prescrizioni da lui impartite. Nella prospettiva delineata si comprende altresì l'equiparazione tra la volontà espressa o tacita, che ovviamente ha un senso solo in quanto all'una e all'altra possa essere attribuito un contenuto oggettivo.

Alla luce delle considerazioni che precedono, interpretando l'art. 615-*ter* in aderenza al paradigma dell'art. 614, si impone l'accoglimento dell'interpretazione oggettiva e il fermo ripudio di quella soggettiva che, come si è visto, è costretta a riempire la nozione di abuso attraverso elementi estranei – e cronologicamente successivi – al fatto tipico.

La conclusione appena raggiunta riceve conferma quando, spostando la riflessione sul piano tecnico, ci si chieda quale sia il momento consumativo del reato di cui all'art. 615-*ter*. Al di là delle peculiarità che caratterizzano il domicilio informatico e si riflettono sul *locus commissi delicti*[23], il delitto in esame si consuma con l'accesso o il mantenimento abusivo, cioè nel momento in cui l'agente ha digitato sulla tastiera del terminale periferico i comandi necessari che gli hanno consentito di entrare nel sistema, superandone le barriere di protezione, ovvero in quello in cui, trovandosi egli già all'interno del sistema, vi permane in violazione delle prescrizioni del titolare: è ovvio che una siffatta condotta precede l'acquisizione del segreto come pure ogni altra condotta in grado di rivelare l'eccesso o lo sviamento di potere[24]. Due conclusivi rilievi valgono a illustrare i paradossi in cui cade la teoria soggettiva qui criticata.

---

[22] Così già V. Manzini, *Trattato di diritto penale*, Torino, 1937, VIII, 706: «Neppure è consentito presumere codesta volontà (il dissenso dell'avente diritto, *n.d.s.*), quando l'ingresso non sia clandestino o fraudolento, sul solo dato del fine illecito dell'agente, argomentando che se l'avente diritto avesse conosciuto codesto fine, avrebbe vietato l'ingresso (es.: fine di adulterio o d'altra copula illegittima, di furto, o d'altro reato). Chi "avrebbe", non ha». Sull'irrilevanza del dissenso c.d. presunto vd. pure F. Antolisei, *Manuale di diritto penale*, *pt. sp.*, Milano, 2016, I, 283; G. Fiandaca - E. Musco, *Diritto penale*, *pt. sp.*, cit., 277 s.; F. Mantovani, *Diritto penale*, *pt. sp.*, cit., 560 s.; C. Piergallini, *I delitti contro la riservatezza domiciliare*, in C. Piergallini – F. Viganò – M. Vizzardi – A. Verri, *I delitti contro la persona*, cit., 737. Allo stesso modo nel caso esemplificato va esclusa la configurabilità dell'art. 624-*bis* c.p., che richiede l'illegittimità dell'introduzione nella privata dimora (anche per i riferimenti giurisprudenziali R. Bartoli, *Art. 624* bis, in G. Forti-S. Seminara-G. Zuccalà (a cura di), *Commentario breve al codice penale*, Padova, 2017, 2176).

[23] Per la più recente giurisprudenza la consumazione del reato *ex* art. 615-*ter* si realizza nel luogo in cui si trova colui che effettua l'introduzione abusiva o si mantiene all'interno del sistema (così Cass. pen., sez. un., 24 aprile 2015, n. 17325; conf. M. Bellacosa, *Il luogo di consumazione*, cit., 1 ss.); diff., ravvisando la consumazione nel luogo in cui si trova il sistema informatico, Cass. pen., sez. I, 27 settembre 2013, n. 40303, favorevolmente annotata da C. Pecorella, *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo a un sistema informatico o telematico*, in *Dir. pen. cont.*, 11 ottobre 2013.

[24] Conf. R. Flor, *Verso una rivalutazione*, cit., 133; Id., *La condotta del pubblico ufficiale*, cit., 515; vd. pure A. Sciré, *Abuso del titolo di legittimazione all'accesso ad un sistema informatico: alle SS.UU. la questione della configurabilità del delitto di cui all'art. 615* ter *c.p.*, in *Dir. pen. cont.*, 21 settembre 2011, 3. Sul momento consumativo del reato in esame Cass. pen., sez. I, 27 settembre 2013, n. 40303.

Il primo concerne l'ipotesi di un'irruzione delle forze dell'ordine nella postazione in cui sta operando il pubblico agente che, in possesso di tutti i profili di autenticazione, si è appena collegato al sistema: data l'imperscrutabilità dei fini, non è possibile muovere nessuna accusa a colui che riesca a dimostrare la parvenza di una ragione funzionale nella propria condotta, giacché le finalità private dell'azione sono destinate a emergere solo quando, successivamente, il funzionario infedele proverà a rivelare o utilizzare i segreti di ufficio acquisiti. In sostanza, l'interpretazione qui contrastata perviene alla singolare costruzione di un reato incentrato sull'intenzione e in grado di manifestarsi all'esterno solo attraverso la commissione di altro e successivo delitto[25].

Il secondo rilievo è altrettanto agevole: «se (…) dovesse ritenersi che, ai fini della consumazione del reato, basti l'intenzione, da parte del soggetto autorizzato all'accesso al sistema informatico ed alla conoscenza dei dati ivi contenuti, di fare poi un uso illecito di tali dati, ne deriverebbe l'aberrante conseguenza che il reato non sarebbe escluso neppure se poi quell'uso, di fatto, magari per un ripensamento da parte del medesimo soggetto agente, non vi fosse più stato»[26].

In conclusione, va respinta la pretesa di convertire una fattispecie fondata sull'accesso non autorizzato in un reato legato a un'infedeltà tutta interiore ed estranea al fatto tipico.

6. Il rapporto tra i commi 1 e 2 e la nozione di abuso

Si è già più volte rilevato che la decisione delle Sezioni unite del 2017 verte esclusivamente sul c. 2, n. 1, dell'art. 615-*ter*: questa impostazione può avere due differenti spiegazioni.

La prima consiste nell'affermare la relazione di specialità fra i reati tipizzati nel c. 1 e nel c. 2, n. 1: quello destinato a un anonimo «chiunque» e configurato come norma generale, questo rivolto solo ad agenti qualificati e dunque costruito – ciò che verrebbe confermato anche dall'autonoma cornice di pena – come norma speciale.

La spiegazione alternativa si identifica nella sovrapposizione delle due nozioni di abuso: l'abusiva introduzione prevista dal c. 1 coincide con l'abuso di cui al c. 2, la cui menzione obbedisce solo allo scopo di rimarcare la necessità che, ai fini dell'aggravamento di pena, il fatto sia stato commesso con abuso dei poteri o con violazione dei doveri.

[25] Analogamente F. Fasani, *Accesso abusivo*, cit., 1405, il quale perviene alle medesime conclusioni attraverso il caso del pubblico funzionario che, consultando una banca dati per ragioni di ufficio, si avvede della presenza del nome di un conoscente nella pratica lavorata, sicché modifica il proprio *animus* e decide di permanere nella pagina per un tempo maggiore di quanto necessario al fine di memorizzare le informazioni utili al conoscente.

[26] Cass. pen., sez. V, 17 gennaio 2008, n. 2534. Conf. E. Mengoni, *Accesso autorizzato*, cit., 2205.

La prima opzione[27] va abbandonata per la sua inconciliabilità con il testo normativo: il c. 2 utilizza in esordio la consueta formula – «se il fatto è commesso» – che caratterizza le fattispecie circostanziali, richiamando integralmente la condotta tipizzata al c. 1 e fondando il più grave trattamento sanzionatorio sulle qualifiche soggettive[28]. Rispetto a queste qualifiche, è poi appena il caso di rilevare che, se il pubblico agente e l'operatore di sistema sono caratterizzati attraverso l'abuso dei poteri o della qualità che connota la condotta descritta nel c. 1, a maggior ragione la dipendenza del c. 2, n. 1 dal c. 1 vale per l'investigatore privato, il cui fatto è privo di ogni definizione. Concludendo sul punto, i commi 1 e 2 dell'art. 615-*ter* sono costruiti rispettivamente come fattispecie base – il cui disvalore si fonda sull'abusiva introduzione o mantenimento nel sistema – e reato circostanziato; ne deriva che l'abuso caratterizzante l'accesso non si identifica con l'abuso dei poteri o con la violazione dei doveri[29].

La seconda soluzione evita il problema appena esaminato, postulando una nozione unitaria di abuso, valida sia per il c. 1 che per il c. 2, incentrata sull'eccesso di potere: «poiché ogni potere pubblico è conferito per il raggiungimento di finalità e obiettivi istituzionali (si argomenta dall'art. 97 Cost.), sembra a questo Collegio (…) che il pubblico ufficiale o l'incaricato di pubblico servizio che utilizzi strumenti informatici del suo ufficio per finalità non coincidenti con quelle per le quali il predetto uso gli è stato concesso, commetta, per ciò solo, il delitto *ex* art. 615-*ter*, c. 2, n. 1 c.p. perché, in tal caso, il "tradimento" della predetta finalità istituzionale integra inevitabilmente la rescissione del forte vincolo che deve collegare l'obiettivo da raggiungere col potere conferito, appunto, per tale scopo»[30].

Alla base dell'assunto ora riferito sta però un evidente salto logico, poiché una circostanza aggravante fondata sulla natura agevolatoria dell'abuso rispetto alla commissione del reato[31] viene convertita nel nucleo dell'illecito ovvero – il che è comunque lo stesso – viene utilizzata come chiave di lettura dell'abuso di cui al c. 1, del quale ora si predica l'irrilevanza della formale autorizzazione in presenza dello sviamento di potere: trascurando però che il perseguimento degli scopi extraistituzionali costituisce un

[27] La tesi dell'art. 615-*ter*, c. 2, n. 1 come reato autonomo e in rapporto di specialità con l'ipotesi del c. 1 è stata enunciata da Cass. pen., sez. V, 16 gennaio 2009, n. 1727, secondo cui «ogni diversa interpretazione renderebbe illogico e contraddittorio il tenore letterale dell'art. 615-*ter*, comma 2 n. 1, c.p.»; nei medesimi termini Cass. pen., sez. V, 20 giugno 2011, n. 24583. *Contra*, per tutte, Cass. pen., sez. un., 7 febbraio 2012, n. 4694; Cass. pen., sez. V, 3 novembre 2015, n. 44403. In favore dell'autonomia del reato sembra esprimersi R. Bartoli, *L'accesso abusivo*, cit., 124, laddove, rispetto al caso concreto sottoposto al giudizio delle Sezioni unite del 2011, osserva: «se potevano esservi dubbi in ordine alla conformità del fatto in esame alla fattispecie (base) prevista dal primo comma dell'art. 615 *ter*, al contrario era indubbio che tale fatto rientrasse nell'ambito applicativo del comma II, n. 1» (vd. pure *ivi*, 126).

[28] Sulla pluralità di indici univocamente orientati in favore della natura circostanziale della previsione, per tutti, F. Fasani, *Accesso abusivo*, cit., 1402 s.

[29] Così anche F. Fasani, *Accesso abusivo*, cit., 1403; R. Flor, *Verso una rivalutazione*, cit., 136.

[30] Cass. pen., sez. V, 14 marzo 2017, n. 12264.

[31] Cfr. Cass. pen., sez. V, 31 marzo 2016, n. 13057, secondo cui l'aggravante in esame «non presuppone necessariamente che il reato sia commesso in relazione al compimento di atti rientranti nella sfera di competenza del pubblico ufficiale o dell'incaricato di un pubblico servizio, né l'attualità dell'esercizio della funzione o del servizio, ma è configurabile anche quando il pubblico ufficiale abbia agito al di fuori dell'ambito delle sue funzioni, essendo sufficiente che la sua qualità abbia reso possibile o comunque facilitato la commissione del reato».

atto successivo all'abusiva introduzione o mantenimento nel sistema, cui l'art. 615-*ter,* c. 1 àncora la punibilità. Pur evitandosi di costruire il c. 2, n. 1, come reato autonomo, l'abuso funzionale ivi descritto viene così chiamato a surrogare l'abusività dell'accesso di cui al c. 1, con un'interpretazione *contra legem* che muove dalla circostanza aggravante *ex* c. 2, n. 1 per trasformare il fatto tipico descritto dal c. 1[32].

Invero, il testo della norma è chiaramente incentrato su due distinti abusi, l'uno attinente all'introduzione o al mantenimento nel sistema (c. 1) e l'altro all'esercizio dei pubblici poteri (c. 2, n. 1). Quanto al primo abuso, alla luce degli antecedenti storici della fattispecie, della sua collocazione topografica e della sua formulazione in rapporto al reato di violazione di domicilio, esso consiste in un difetto di autorizzazione all'accesso o alla permanenza nel sistema informatico o telematico e tale carenza di abilitazione può svolgere la funzione di selezionare tra condotte lecite e illecite solo se dotata di una valenza oggettiva, riguardante le modalità, i tempi, l'oggetto dell'accesso ecc., mentre per necessità prescinde dalle intenzioni del soggetto abilitato: qualsiasi ontologia – come ebbe ad esprimersi un grande Maestro ad altro proposito – è davvero fuori luogo[33].

Passando al secondo abuso, previsto dal c. 2, n. 1, l'intento legislativo parrebbe chiaro: l'aggravamento della pena per l'investigatore privato, per l'operatore del sistema e per il pubblico agente suppone che essi abbiano agito nei rispettivi ruoli, il primo esercitando la professione, il secondo abusando della qualità – cioè utilizzando la propria abilitazione all'accesso per compiere operazioni diverse dalla manutenzione e dall'aggiornamento del sistema – e il terzo sfruttando i poteri o violando i doveri inerenti alla funzione o al servizio[34]. Ma affinché l'assimilazione sul piano sanzionatorio abbia un senso, è necessario che l'investigatore privato, l'operatore del sistema e il pubblico agente si siano tutti e allo stesso modo «abusivamente» introdotti o mantenuti nel sistema, cioè abbiano commesso il fatto tipizzato nel c. 1: laddove, al contrario, l'interpretazione qui criticata propone una costruzione esclusivamente soggettiva valida solo per il pubblico agente.

A questo punto diviene chiaro che l'inversione operata dalle Sezioni unite nel 2017, con cui l'abuso del c. 2, n. 1 è chiamato a sostituire quello tipizzato nel c. 1, si risolve in una trasformazione del reato di cui all'art. 615-*ter*, concepito come un abuso dell'ufficio o servizio e conseguentemente interpretato alla stessa stregua dell'art. 323 c.p.[35]. Ne deriva un sovvertimento della fattispecie nei confronti dei pubblici agenti "colpevoli"

---

[32] Conf. Cass. pen., sez. V, 24 ottobre 2014, n. 44390, che rispetto all'orientamento qui criticato rileva che «il parametro di riferimento è divenuto (…) non già il complesso delle disposizioni impartite dal *dominus loci*, ma il complesso delle disposizioni che regolano e indirizzano l'attività amministrativa verso i fini determinati dalla legge, finendo con l'identificare l'abusività – com'era inevitabile, data la premessa – nella violazione della regola di imparzialità e trasparenza che regge l'azione amministrativa». Criticamente vd. pure F. Fasani, *Accesso abusivo*, cit., 1403.

[33] Cfr. C. Pedrazzi, *Ontologia fuori luogo (A proposito di una contravvenzione punita con la multa)*, in *Riv. it. dir. pen*., 1957, 68, il quale osservava che «al dato ontologico ha senso richiamarsi nei limiti in cui la normazione positiva si sovrappone a una realtà già strutturata, già pregna di quei significati che danno ragione della rilevanza giuridica».

[34] Da notare che l'art. 326 c.p. incrimina la rivelazione e l'utilizzazione di segreti di ufficio impiegando la formula «violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità».

[35] Analogamente R. Flor, *La condotta del pubblico ufficiale*, cit., 513 s.

di eccesso o sviamento di potere, in quanto abbiano operato per fini privati e comunque non istituzionali.
Questo esito interpretativo appare problematico già sul piano formale, poiché il precetto sancito dall'art. 615-*ter* rimane inalterato per tutti gli altri consociati, cui viene inibito l'accesso non autorizzato al sistema, mentre per il pubblico ufficiale e l'incaricato di un pubblico servizio assume un significato totalmente diverso. Ma questa nuova accezione dell'accesso abusivo, fondato sull'eccesso o sviamento di potere, risulta priva di ogni fondamento anche sistematico, in quanto evoca una fattispecie che non esiste nel diritto penale, solo che si consideri come l'art. 323 c.p. leghi il delitto di abuso d'ufficio alla produzione di un ingiusto vantaggio patrimoniale o di un danno ingiusto.

7. Conclusioni

Vediamo di concludere. Fin quando gli archivi hanno custodito materiale esclusivamente cartaceo, è stato ritenuto sufficiente l'attuale apparato penalistico (*retro*, § 4.1): non che allora mancassero le abusive consultazioni per finalità private, ma per contrastarle si è fatto affidamento sulle fattispecie in tema di procacciamento, rivelazione e utilizzazione dei segreti.
Il processo tecnologico, con l'avvento delle banche dati, ha determinato un enorme incremento degli stimoli e delle opportunità di accessi abusivi per ragioni extraistituzionali. Ancora nel 1993 il problema non era avvertito con particolare sensibilità e la l. 547, in quell'anno emanata, manifestava attenzione – come già la Raccomandazione R(89)9 del Consiglio d'Europa – per i «rischi di manipolazioni informatiche, di danneggiamento dei dati e di spionaggio informatico» (così si esprimeva la relazione alla Raccomandazione). Al contrario, soprattutto nell'ultimo decennio le statistiche giudiziarie riportano un notevole aumento dei procedimenti penali per abusive intrusioni in sistemi informatici e telematici e, tra essi, assai numerosi sono i casi di accesso per finalità private a banche dati da parte di soggetti appartenenti al personale della cancelleria dei tribunali o alle forze dell'ordine ovvero dipendenti dal Ministero dell'Economia e delle Finanze o dei Trasporti.
Tali accessi avvengono il più spesso sulla base di accordi corruttivi e sono dunque destinati ad avere un seguito nella commissione del reato di rivelazione di segreti di ufficio *ex* art. 326 c.p., la cui dimostrazione in sede processuale può però rivelarsi difficoltosa. La via più breve consiste dunque nel configurare a carico del pubblico agente l'art. 615-*ter*, c. 2, n. 1, la cui cornice di pena assicura un'efficace risposta sanzionatoria.
Questa soluzione rappresenta però un'invenzione della giurisprudenza, che non trova nessun appiglio nel testo normativo – rivelandosi quindi incompatibile con il principio di legalità – e non appare dotata di un sufficiente fondamento politico-criminale, dovendosi dubitare della correttezza di un'equiparazione fra tutte le finalità private che abbiano ispirato l'accesso abusivo, addirittura prescindendo dal loro contenuto lecito o illecito. Neppure va trascurato che le condotte in esame potrebbero in parte trovare un'adeguata reazione in sede disciplinare, restando esclusa la loro rilevanza penale.
In ogni caso, la decisione sull'introduzione di una fattispecie autonoma, incentrata

sull'accesso al sistema per finalità extraistituzionali, malgrado l'evidente difficoltà di caratterizzarne la dimensione lesiva esclusivamente alla luce dello scopo dell'agente, rientra nell'esclusiva competenza del legislatore.

La conclusione è obbligata: questa volta le Sezioni unite della Cassazione non hanno esercitato una funzione nomofilattica.

Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations*

Manuel David Masseno
Cristiana Santos

Abstract

Data lies at the core of all smart tourism activities as tourists engage in different and personalized touristic services whilst the pre/during/post travelling or in holidays. From these interactions, a digital data trail is seamlessly captured in a technology embedded environment, and then mined and harnessed in the context of STD - Smart Tourist Destinations to create enriched, high-value experiences, namely those related to eco-responsibility, as well as granting destinations with competitive advantages. The perceived enjoyment of experiences must be considered within the legal framework of Privacy and Data Protection by exposing inherent risks, analysing the available answers given by the GDPR – the General Data Protection Regulation of the European Union. Hence the purpose of this paper is i. to singularize the specificities of Smart Tourism Destinations; ii. to show how the principles of personal data protection, as set forth by the GDPR, are allocated within the STD realm; iii. and, finally, to derive potential legal implications of this ecosystem. Our approach is based on a legal analysis engaged in scholarship research. We have mostly denoted the underestimation of the legal implications of technology-enhanced tourism experiences, and the marginalization of both informed involvement and awareness by the individual in these processes. This study is novel in having undertaken an initial exploration of the legal implications of experiences taking place by STD.

Summary

1. Introduction. - 2. Specificities of STD. - 2.1. Smart Tourism Destinations. - 2.2. Technology-Enhanced and Empowered Experiences. - 3. Compliance of Smart Tourism Destinations with the privacy and data protection principles. - 3.1. Fairness and Transparency. - 3.2. Lawfulness of Processing: Consent, Legitimate Interests, Contract and Public sector. - 3.3. Purpose Limitation. - 3.4. Data Minimization: Collection and Retention. - 3.5. Accuracy and Up-to-date Processing. - 4. Reflections and Conclusions

Keywords: Privacy, Data Protection, Smart Tourism Destinations, GDPR, Touristic Services

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

1.Introduction

Smart Tourism Destinations (hereinafter called STD) are an offspring of the technological foundations of Smart Cities, themselves benefiting from the interplay with other technological environments based on the Internet of Things (IoT) and the Cloud, as enabled by Big Data Analytics.

However, while these subjects have been examined extensively within Privacy literature, their specific context and legal consequences on STD is still to be explored. As a matter of fact, this is perceived and pointed out as a missing issue by the Tourism Science literature regarding STD[1]. Given the insufficiencies in the literature and these recent claims, this study aims to provide a theoretical review of the technology-empowered tourism experiences and its legal implications to privacy and data protection. Theoretically and in practice, STD have been designed to enrich tourism experiences and to enhance the competitiveness of each destination.

ICTs embedded within tourism destinations environments allow the collecting and analysis of large amounts of tourism data for the identification of attitude patterns and to predict behaviors of tourists and travelers. This is achieved by addressing their potential needs and desires even at an unconscious level of travelers.

Regarding this connection between Tourism and ICTs, we're facing a new relationship between clients-tourism providers which is very context-specific: i.) Short-lived engagement, focused on the pre/during/post travel, which makes trust-building and costumer's loyalty much harder[2]; ii.) Imminent need for real-time information *in situ,* for vacation decision-making, so that tourists might be easily persuaded to forego their data; iii.) Heightened benefits or "perceived enjoyment" (evoked by the engaging content, discounts, and interactive system features)[3], suggesting that personal data is traded therewithal for useful purposes and hence privacy concerns might be temporarily suspended; iv. Tourism activities take place in locations outside of the usual realm of the traveler, and are often facilitated by unknown local service providers, which decrease privacy risk perceptions[4], for instance at natural spaces apparently far from urban invasive surveillance; v. Growing number of connected smart objects and wearable devices involved in a network of multiple vendors and interoperating systems, where privacy issues are blanked out; vi. Multiple stakeholders' interaction making it even harder to identify privacy flaws.

The following illustrative examples provide insight towards the personalized and smart added-value services that STD can offer:

[1] Even being tourism the world's largest industry, with receipts of almost 1,200 USD Billion in 2017, and growth expectations of 4% to 5% for 2018, according to the UNWTO Barometer, notwithstanding internal tourism.

[2] B. Neuhofer – D. Buhalis et al., *Smart technologies for personalized experiences: a case study in the hospitality domain*, in *Electronic Markets*, vol 25, issue 3, 2015, 243 ss.

[3] *Ibidem.*

[4] U. Gretzel, Ulrike – M. Sigala et al., *Smart tourism: foundations and developments*, in *Electronic Markets*,vol. 25, issue 3,179 ss.

Full historic immersions through smart optics devices or augmented reality for a "happy guest" are services already offered. Further, location-based services (LBS) could alert users to the closeness of birds to be watched or to endemic plants. Besides, estimated waiting time for the entrance to Natural Parks and other Protected Sites can be accurately quoted, to the minute, so tourists may reorganize their visiting or trail options or get a drink in a bar while waiting. Besides, aware on customers' special dietary circumstances in regard with their medical condition, as well as religion restrictions, tourism service providers may provide for meals that suits their preferences. As for transport, real-time information about the tourist's destinations, which direction to get on, and the ability to respond (i.e., by suggesting alternatives) to unpredictable events in real-time are envisioned, namely sudden weather changes. RFID tags on their outfit would make it easier to locate travelers in case of being lost or in order to identify those liable for damages inflicted to natural spaces or protected species.

All these enhanced services allow tourists to get much more from their travel and helps them fulfilling the experiential travelling potential of the destination[5]. STD experiences are hence achieved through intensive personalization, context-awareness and real-time monitoring[6]-[7] processes of information management which entail legal risks, demanding a careful analysis within the data protection framework.

Given the nature of STD and its uses, the application of some of the principles of data processing (*e.g.* the principles of data minimization, purpose limitation, fairness and transparency, and free, specific and informed consent) may be challenging in this technological scenario.

As a large spectrum of user-generated content is tourism data processed in a smart tourism environment concern personal data and human interaction, there is a direct impact on individuals and their rights with regard to the processing of personal data.

As explicitly mirrored in Article 8 (3) of the Global Code of Ethics for Tourism[8], tourists and visitors should benefit from the same rights as the citizens of the country visited concerning the confidentiality of the personal data and information concerning them, especially when these are stored electronically. Therefore, it should be underlined that Privacy and Data Protection evaluation is needed in any tourism environment, balancing the tradeoff value and affordances added by STD and its legal protection. This work therefore provides a study of the principles of data protection, as set forth by the GDPR, within the STD context.

The paper is organized as follows. Section 1 explains the background of STD, describing briefly its specificities and giving examples of technologically enhanced and

[5] D. Buhalis – A. Amaranganna, *Smart Tourism Destinations*, in Z. Xiang – L. Tussyadiah (eds.), *Information and Communication Technologies in Tourism 2014 - Proceedings of the International Conference in Dublin, Ireland*, Heidelberg, 2014, 553 ss.

[6] *Ibidem.*

[7] D. Buhalis - A. Amaranganna, *STD: Enhancing Tourism Experience Through Personalisation of Services*, in L. Tussyadiah – A. Inversini (eds.), *Information and Communication Technologies in Tourism 2015 - Proceedings of the International Conference in Lugano, Switzerland*, Heidelberg, 2015, 377 ss.

[8] Accessible online at www.ethics.unwto.org/.

empowered experiences. Section 2 explains how smart technologies affect compliance with the principles of the General Data Protection Regulation[9], as the current basis of Privacy and Data Protection Legal system in the European Union. Section 3 concludes the paper and provides some clues for future directions.

2. Specificities of STD

This section describes the constituents of STD, objectives and derived added value.

2.1. Smart Tourism Destinations

In order to characterize more closely the utility functions layered in tourism destinations, it is worthy to point out that successful destinations are composed by five tourism dimensions: transportation, accommodation, gastronomy, attractions and ancillaries services, which can be then structured into six axes or "6As" as the literature describes[10], namely: i. Attractions, which can be natural, like as mountain or a seaside; artificial, as amusement parks or sports facilities; or cultural such as music festival or a museum; ii. Accessibility refers to the transportation within the given destination; iii. Amenities characterize all services, namely accommodation, gastronomy and leisure activities; iv. Available Packages; v. Activities; and vi. Ancillary Services (e.g. daily use services such as bank, postal service and hospital).
By applying *smartness* into tourism destinations, STD are defined as:
«[…] tourism supported by integrated efforts at a destination, to find innovative ways to collect and aggregate/harness data derived from physical infrastructure, social connections, government/organizational sources and human bodies/minds in combination with the use of advanced technologies to transform that data into enhanced experiences and business value-propositions with a clear focus on efficiency, sustainability and enriched experiences during the trip»[11].
This embracing concept comprises three core elements of destinations[12]:
i.) Reliance on smart technology infrastructures, wireless sensor networks (IoT) and integrated communications systems, e.g. sensor technology, ubiquitous wifi, near-field communication (NFC), smart mobile connectivity, radio-frequency-identification (RFID), sophisticated data warehouses; data mining algorithms, also considered vital to creating a smart technology infrastructure[13]. IoT provides support in terms of

[9] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), applicable from the 25th May 2018.

[10] D. Buhalis, *Marketing the Competitive Destination of the Future*, in *Tourism Management*, vol. 21, 2000, 97 ss.

[11] U. Gretzel – S. Reino et al., *Smart Tourism Challenges*, in *Journal of Tourism*, vol. 16, issue 1, 2015, 41 ss.

[12] M. Höjer – J. Wangel, *Smart Sustainable Cities: Definition and Challenges*, in L. Hilty - B. Aebischer (eds.), *ICT Innovations for Sustainability, Advances in Intelligent Systems and Computing*, Heidelberg, 2015, 333 ss.

[13] U. Gretzel – S. Reino et al., *op. cit.*

information gathering and analysis as well as regarding automation and control. For instance, chips embedded to entrance tickets, or a smartphone app, allow tourism service providers to track tourists' locations and their consumption behavior, enabling location-based advertising or rescue in case of them getting lost when departing from an usual trail. In addition, cloud computing services may provide access to solid web platforms and data storage through public electronic communications network. It also encourages information sharing, a fundamental feature for STD. For example, a sophisticated tour guide system could serve massive number of tourists without being actually installed on any personal device, even allowing personalizing experiences;
ii.) Built on an infrastructure of state-of-the-art technology, «[…] accessible to everyone, which facilitates the visitor's interaction with and integration into his or her surroundings, increases the quality of the experience at the destination, and improves residents' quality of life»[14];
iii.) Smart business networks, referring to the number of applications at various levels supported by a combination of Cloud Computing and IoT.

2.2 Technology-Enhanced and Empowered Experiences

The shared purpose of all omni-channel actors of a smart tourism ecosystem is to provide enhanced/enriched, high-value, meaningful, memorable tourism experiences through services and products mediated through technology (technology-mediated experiences).
Such experiences are rendered enhanced or empowered, according to the type and role of technology used. In technology-enhanced experiences, technology available in the Web 2.0 plays a supporting role to make consumers actively participate and shape the creation of their experiences. Consumers use social networking sites and mobile apps to interact with organizations, use review sites, comment and use media to share their experiences[15].
On the other hand, "technology-empowered experiences" emerge from advanced technological developments, such as interactive environments, augmented reality, near field communications, gaming, etc. At this latter level, technology is pervasive and allows tourists to interact and engage with the different service-providers throughout all the stages of travel, service encounters and touch-points, either in the physical tourism destination or in the online space. These new experiences are predicted to be richer, more participatory. In fact, consumers play an active part in co-creating[16] their own experiences, recognizing these way active consumers co-creating their experiences in a quest for personal growth and value.
It is pertinent to systematize and explore some types of technologies worn in practical

[14] M. Höjer – J. Wangel, *op. cit.*

[15] L. Tussyadiah - D. Fesenmaier, *Mediating the tourist experiences access to places via shared videos*, in *Annals of Tourism Research*, vol. 36, issue 1, 2009, 24 ss.

[16] C.K. Prahaland – V. Ramaswamy, *Co-creation experiences: the next practice in value creation*, in *Journal of Interactive Marketing,* vol. 18, issue 3, 2004, 5 ss.

settings within destinations to enhance and empower experiences. Technologies range from:

- Social networking sites (SNSs);
- Mobile applications (destination apps);
- Interactive websites;
- Interactive ordering systems (eTable technology);
- Interactive mobile platforms (iPads);
- Wearable devices;
- Big data analytics;

Social networking sites (SNSs), as referred in i., have already expanded their capabilities as build-in apps to meet social media user´s needs; they are mostly Facebook, YouTube, Twitter, TripAdvisor, Yelp and have made user-generated content (UGC) such as preferences, needs, interests, profiles, etc. freely accessible online. Such user-input content is reified in social profiles, reviews, ratings, comments, impressions on past experiences, recommendations for future purchases, etc.). The travel review website TripAdvisor generates a significant source of tourism-related (open) data given the figures and reviews on attractions/destinations; as a means of illustration, «in 2015, TripAdvisor reached 320 million reviews and had 6.2million opinions on places to stay, to eat and on things to do - including 995,000 hotels and forms of accommodation, 770,000 vacation rentals, 3.8 million restaurants and 625,000 attractions in 125,000 destinations throughout the world»[17].

Destination mobile applications mentioned in ii. are characterized by their "*mobiquity*" (mobility and ubiquity), and free wifi access to information anywhere and anytime have led to a behavioral transformation of tourists from *"sit and search" to "roam and receive"*[18].

As an example of iii., the interactive online website *PixMeAway*[19] is a picture-based search engine that allows consumers to interact with the interface, select appealing travel motifs, photos, the traveler type, and define their travel personality. The website will provide destination suggestions matching their criteria.

As an example of iv. the Inamo Restaurant[20] provides an instance in which the technology empowers the tourism experience. This restaurant «[…] introduces a fully digitalized dining experience and interactive ordering system. This system, developed by E-Table, uses a combination of table touchpads and overhead projection to allow customers to see the food and drinks menu projected onto the table surface. The system further allows customers to change table clothes to the current mood and preferences, watch their food being prepared in the kitchen through a webcam in real time, manage the waiter and bills, explore the local neighborhood for activities afterwards or order a cab home. By doing so, the restaurant provides the physical technology (interactive

[17] E. Pantano – C.V. Priporas et al., *You will like it!' Using open data to predict tourists' responses to a tourist attraction*, in *Tourism Management*, vol. 60, 2017, 430 ss.; and also the *TripAdvisor annual report for 2015*, accessible online.

[18] M. Pihlström, *Perceived Value of Mobile Service Use and its Consequences*, Helsinki, Swedish School of Economics and Business Administration, 2008, accessible online.

[19] Accessible online.

[20] Accessible online.

tables) without which the unique dining experience could not occur, rendering the technology the central element of the experience creation».

As an example of v., the Hotel Lugano Dante[21] provides a case of hotel enrichment context where mobile platforms can come into play to facilitate and enhance the level of interaction between company and guests throughout the entire hotel experience. In such hotel, «Guests provide personal information and preferences, such as room temperature, favorite beverages, and preferred newspapers and so on, whereas members of staff retrieve this specific information. By accessing the platform on a mobile device, the hotel and guests co-create through exchanging information in real time, which are used to facilitate encounters on multiple touch points. This leads to more personalized interactions, more valuable service encounters and on overall enhanced experience for the guest».

Wearable devices, listed as vi. are body-attached computers and are part of the IoT, therefore contributing to ubiquitous computing. Nowadays, there are different types of wearables applied to tourism destinations[22]:

- Smart watches provide notifications such as status updates, comments, photo tags, check-in, etc. Tourists can also receive real-time flight alerts, gate changes, and other information on their wrists;
- Bracelets/watches can track guests' sleeping patterns, as clients wear a watch while sleeping and wake them through gentle vibrations;
- Wrist band able to swipe hotel room keys;
- Smart glasses used by tourists in museums, art galleries to see cultural artifacts and activate digital contents, such as video, games, photos, etc. on the glass display screen by simply looking at the collection item; visitors can easily switch between real objects and augmented reality.

All wearables have in common the fact they collect and process user-specific data. Alongside body-data, many wearables record location-data and geo-data, often unnoticed by the users, for they can be used to calculate the distance travelled, to determine the user's location, etc., which poses a challenge for present data protection and privacy. Moreover, the use of wearable devices does not only involve its user (the owner of the device), but also the manufacturer, third-party providers and other intermediaries (insurance companies, scientists or advertising companies). Furthering, data is often not stored locally or processed by the device itself, but forwarded to a Cloud service (even possibly located outside Europe)[23].

Concerning big data analytics, pointed in vii., tourism data is an asset being exploited using a multi-modal pipeline of advanced data analysis methods called big data analytics[24] comprising content analytics crawlers (mining unstructured content), machine

[21] B. Neuhofer - D. Buhalis et al., *op. cit.*

[22] R. Atembe, *The Use of Smart Technology in Tourism: Evidence From Wearable Devices*, in *Journal of Tourism and Hospitality Management*, vol. 3, n. 11-12, 2015, 224 ss.

[23] T. Jülicher – M. Delisle, *Step into 'the circle'—a close look at wearables and quantified self*, in T. Hoeren – B. Kolany-Raiser (eds.), *Big data in context - legal, social and technological insights*, Heidelberg, 2018, 81 ss.

[24] K. Waterman – P. Bruening, *Big data analytics: risks and responsibilities,* in *International data privacy law*, vol. 4, issue 2, 2014, 89 ss.

learning (ML) algorithms, natural language processing tools (NLP) and data mining techniques (DM). Distinctive aspects of big data analytics are briefly mentioned herewith to foresee its implications on data protection[25]: i. Use of large numbers of ML algorithms against data to find correlations, inferences between data. Once relevant correlations are identified (originally unforeseen), a new ML algorithm can be created and deployed to specific cases in the future; ii. Tendency to collect and analyze *all* the data that is available; iii. Repurposing of data for which it was originally collected, as analytics can mine data for new insights and find correlations between apparently disparate datasets; and iv. Use of new types of data automatically generated and coming from the IOT devices, as sensors. Even though these methods endow stakeholders with a fine-grained data to extract value, trends and patterns, thereby enabling them to customize technology-empowered experiences through smart products and services, they also increase known risks hampering privacy and data protection[26].

The implementation of the above mentioned smart ICT enhances tourism experience through the offer of products/services that are customized, personalized (personalized infotainment services), to meet each of the visitor's unique needs and even implied desires, since understanding travelers' needs, wishes and desires becomes increasingly critical for the attractiveness of destinations. Such customization, personalization and profiling is attained by *collecting* UGC from all these technological artifacts, and *reusing* it to provide meaningful offers fitting perfectly the clients' needs[27] with the ultimate desideratum of achieving more satisfaction[28] at the experience environment.

Therefore, tourism-related data has multiplied geometrically[29] through its varied provenance (SNSs, apps, sensors, etc.). These sources provide a massive size of volunteered, observed, inferred or collected digital traces, resulting in multidimensional sets of data, known as big data[30]. This massification of real-time tourism-related data, analyzed by IoT industries, has created big pools of data to mine. Hence, SDT can be considered both as consumers and producers of big data.

This tourism-related data, inherently cross-border, holds strategic commercial value. It comprises, for example, i. transactional data between tourists and transportation/hospitality undertakings (airlines, hotel, restaurants and rental car businesses)[31] derived

[25] A. Mantelero – G. Vaciago, *The 'dark side' of big data: private and public interaction in social surveillance. How data collections by private entities affect governmental social control and how the EU reform on data protection responds in social surveillance,* in *Computer law review international*, vol. 14, 2013, 161 ss.

[26] H. Couturier, *At the big data crossroads: turning towards a smarter travel experience*, Amadeus IT group report, 2013, accessible online.

[27] L. Edwards, *Privacy, security and data protection in smart cities: a critical EU law perspective*, in *European data protection law review*, vol. 2, 2016, 28 ss.

[28] R. Law – R. Leung et al., *Information technology applications in hospitality and tourism: a review of publications from 2005 to 2007*, in *Journal of travel & tourism marketing*, vol. 26, issue 5-6, 2009, 599 ss.

[29] J. Manyika – M. Chui et al., *Big data: the next frontier for innovation, competition, and productivity*, Report McKinsey Global Institute, 2011, accessible online.

[30] B. Habegger – O. Hasan et al., *Personalization vs. Privacy in Big Data Analysis*, in *International Journal of Big Data*, issue 1, 2014, 25 ss.

[31] These activities reveal aspects on destination/origins, way-finding preferences (beach, sports, culture, restaurants, etc.), spending capacities, and on behaviors (family tourism, leisure, night clubs, events, etc.), etc.

from queries/searches, purchases, and other exchanges; ii. geographical data; and iii. UGC from client's profiles, established preferences, needs, etc. These data can reveal commercial preferences of its users, allows the detection and prediction of future behaviors and trends, rendering enormous interest for economic operators, and allow destinations to better plan for future tourists in terms of mobility, popular attractions, and other potential issues. By managing such big data, tourism organizations can extract valuable insight from information that could elevate them to a new dimension of customer experience and improve the way they interact with customers, hence gaining competitive advantage[32]. Such information is the fabric for companies to convert big and open data[33] into future preferences and value propositions[34].
However, such processing of personal information (data trails or digital footprints) contains the risk of building of a detailed profile of tourists, actually, a holistic personal mosaic of the individual users, with imminent implications for privacy and data protection[35].

3. Compliance of Smart Tourism Destinations with the privacy and data protection principles

3.1. Fairness and Transparency

Article 5(1) (a) states that personal data must be «processed fairly, lawfully and in a transparent manner in relation to the data subject». Accordingly, destinations must assess if their processing of personal data is fair and transparent. Transparency of automated decision-making is taking an increasingly important role with the advent of big data analytics. Whether the data are volunteered, observed, or inferred, or collected from accessible sources, individuals are fully entitled to know which are they, from where and from whom the controllers obtained it, and how automated decisions were taken. Denote that big data algorithms (also used in STD scenarios) learn and change in a (semi) autonomous way, making them hard to document; further, organisations often claim secrecy over "how" data is processed on grounds of commercial confidentiality and copyright protecting the software and the trade-secret shield[36]. Profiling and cor-

[32] D. Buhalis – A. Maranggana, *op. cit.*

[33] We denominate this data as "open data", as it accomplishes the criteria of i. availability and access; ii. reuse and redistribution; iii. Universal participation, i.e., this data can be reused by anyone, https://okfn.org/opendata/. It is notable to state that growing amount of tourism-related open data is available in machine-readable ways (XML, CSV, or JSON format), E. Pantano – C.V. Priporas et al., *op. cit.*

[34] M.D. Masseno, *On the relevance of Big Data for the formation of contracts regarding package tours or linked travel arrangements, according to the New Package Travel Directive*, in *Comparazione e diritto civile*, 4, 2016, 2 ss.

[35] I. Rubinstein, *Big Data: The End of Privacy or a New Beginning*, in *International Data Privacy Law*, vol 3, issue 2, 2013, 74 ss.; also, R. Kemp, *Legal aspects of managing big data*, in *Computer Law and Security Review*, vol. 30, 2014, 482 ss.

[36] P. Schwartz – D. Solove, *The pii problem: privacy and a new concept of personally identifiable information*,in *New York University Law Review*, vol. 86, 2011, 1814 ss.

relation results are hence invisible and opaque, and its results often impenetrable to laymen. Secret-tracking and decision-making on the basis of profiles are then hidden from any consumer-tourist, which is left without meaningful information about the employed "algorithmic logic". Still, we are attentive to a right to know the "logic of the processing" applied to data (Recital 63, and Arts. 13(2) (f), and 15(1) (h)), respectively.
The GDPR defines profiling in Article 4 as: «[…] any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements».
Profiling is an important feature in tourism destinations. Tourism service providers are adapting their serviceable approach to meet the personalization expectation[37]. In fact, data-processing scenarios collect user's input and feedback which are used to build fine-grained premium services and recommender systems in the form of trail packages. The richer the user profile, the higher the temptation for the operators to target a user with unsolicited advertising or to engineer a pricing structure capable to extract as much surplus from the user as possible[38].
The GDPR prohibits automated individual decision-making that significantly affect individuals, Art. 22 (1). Notably, «[…] analytics based on information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behavior patterns».[39]
Indeed, developments on consumer-tourist automated profiles, facilitated by big data analytics, can *significantly affect* data subjects[40]. Covert profiling can, in certain cases, lead to unintended consequences:
i. when based on incomplete data, profiling can lead to false negatives, depriving individuals from benefits that they would be entitled to;
ii. "*filter bubbles*" effect[41], according to which data subjects will only be exposed to content which confirms their own preferences and patterns, without any door open to serendipity and casual discovery;
iii. isolation and/or discrimination, e.g., including price differentiation, without providing the individuals the possibility to contest these decisions. In a STD, ML decisions and profiling can lead to promote direct or indirect discrimination decisions through the exclusion/denial of services/goods, e.g. denial of insurances, exclusion from the sale of touristic services or high-end products, shops or entertainment complexes to certain profiled tourists and even other decisions that reflect upon health, creditworthiness, recruitment, insurance risk, etc; it even can lead to discriminate essential utilities for those unwilling to share personal data[42]. In this synopsis, tourists might be

[37] L. Edwards, *op. cit.*

[38] ENISA 2015 report, *Privacy and data protection by design – from policy to engineering.*

[39] Art. 29 WP, Opinion 8/2014, *Recent developments on the Internet of Things.*

[40] EDPS, Opinion 3/2015, *Europe's big opportunity*, *EDPS recommendations on the EU's options for data protection reform.*

[41] E. Pariser, *The filter bubble: what the Internet is hiding from you*, New York, 2011.

[42] P Schwartz – D. Solove, *op. cit.*

discriminated against because they belong to a particular social group, but also, such ascertainment might be based on factors, identified by the analytics, that they share with members of that group.
Therefore, in order to ensure a fair and transparent processing, automated decisions should account all the circumstances concerning the data and not be based on merely de-contextualized information or on data processing results.
In furtherance of this aim, the controller should find ways to build discrimination detection into their ML systems, to prevent inaccuracies and errors assigned to labeled profiles; as referred in Recital 71, the controller should «[…] use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect».

3.2. Lawfulness of Processing: Consent, Legitimate Interests, Contract and Public sector

In this sort of intelligent environment, it is dubious to give or withhold our prior consent to data collection[43], as it seems to be absent by design. The awareness that the ubiquitous sensors are so embedded in the destination that they literally "disappear" from the users' sight, so that they will not even be conscious of their presence and hence consent to the collection, can be envisaged within STD. We can, at some extent, concede that the obtaining of such consent, in STD contexts, would be defined in a mechanical or perfunctory manner, or as a "routinization".
We note also that as for CCTV, ANPR and MAC whilst tracking and sensing, the notice in the form of information signs in the area being surveilled, or on related websites, does not conform to the consent requirements. The issue of the IoT embedded in STD is that its sensorization devices are explicitly designed to be unobtrusive and seamless, invisible in use and unperceived to users[44] and thereupon, users do not hold the opportunity give their unambiguous, informed, specific, explicit, and granular consent[45]-[46]. Therefore, the data controller might have difficulty in demonstrating that the

[43] R. Kitchin, *Getting smarter about smart cities: Improving data privacy and data security*, Data Protection Unit, Department of the Taoiseach, Dublin, 2016.

[44] P. Schwartz - D. Solove, *op. cit.*

[45] Art. 29 WP, Opinion 15/2011, *Definition of Consent*; Art. 29 WP (259 rev. 01), *Guidelines on Consent under Regulation 2016/679*.

[46] A. Mantelero, *The future of consumer data protection in the E.U. Re-thinking the 'notice and consent' paradigm in the new era of predictive analytics*, in *Computer Law and Security Review*, vol 30, 2014, 643 ss.

consent was given, and the data subject is not able to withdraw that consent[47].
Still, consent is not yet part of a function specification of IoT devices, and thus, they do not have means to display «provide fine-tuned consent in line with the preferences expressed by individuals» because smart roads, trams, tourist office devices are usually small, screenless and lack an input mechanism (a keyboard or a touch screen)[48].
Regarding the amount and assortment of these interactions, it is just too onerous for each data subject to assess their privacy settings across dozens of entities, if any, in order to ponder about the non-negotiable tradeoffs of agreeing to privacy policies without knowing how the data might be used now and in the future, and to assess the cumulative effects of their data being merged with other datasets[49].
Reverting also to other legal grounds, processing personal data relies on "public interest", which can sidestep the need for consent (health, national governmental agencies gather data for e. g. e-Government systems, e-Health). Nevertheless, this possibility should not conceal any eventual "third-party interest".
Most commercial systems rely on the "legitimate interests" ground, even if they consist in «the vaguest ground for processing»[50], and offers a lot of scope for industry to process data by claiming any deemed necessary "legitimate interest". In fact, the processing must be "necessary" for the legitimate interests and not just *potentially* interesting[51]. It follows that the processing is not necessary if there is any other way of meeting the legitimate interest that interferes less with the people's privacy[52]. Implicitly, the task of balancing commercial interests and user fundamental rights [53] is delegated to the controllers themselves[54].
As for the contractual condition, it may be difficult to show that big data analytics in STD are strictly necessary for the performance of a contract, since the processing goes beyond what is required to sell a product or deliver a service.

3.3. Purpose Limitation

This principle utters that the purpose for which the data is collected must be specified and lawful, Art. 5(1) (b). This principle also prevents arbitrary reuse[55], calling for a «compatibility assessment of the new purpose»[56]. As for a repurpose, personal data should not be further processed in a way that the data subject might consider

47 E. Carolan, *The continuing problems with online consent under the EU's emerging data protection principles*, in *Computer Law and Security Review*, vol. 32, issue 3, 2016, 462 ss.

48 Art. 29 WP, Opinion 8/2014, *Recent developments on the Internet of Things*.

49 B. Habegger – O. Hasan et al., *op. cit.*

50 EP Study, Big *Data and Smart Devices and their Impact on Privacy* (2015).

51 ICO, *Big Data*, *Artificial Intelligence, Machine Learning and Data Protection*, UK, 2017.

52 Art. 29 WP, Opinion 06/2014, *Notion of legitimate interests of the data controller.*

53 EDPS, Opinion 7/2015, *Meeting the challenges of big data.*

54 P. Schwartz - D. Solove, *op. cit.*

55 Art. 29 WP, Opinion 03/2013, *Purpose Limitation*, 21.

56 ICO, *Big Data, Artificial Intelligence,* cit.

unexpected, inappropriate or otherwise objectionable[57] and therefore unconnected to the delivery of the service; concretizing, by exposing data subjects to different/greater risks than those contemplated by the initial purposes could be considered as a case of further processing of data in an unexpected manner.
In what refers the compatibility assessment, Article 29 WP states that «By providing that any further processing is authorized as long as it is not incompatible […], it would appear that the legislators intended to give some flexibility with regard to further use. Such further use may fit closely with the initial purpose or be different. The fact that the further processing is for a different purpose does not necessarily mean that it is automatically incompatible: this needs to be assessed on a case-by-case basis». This Opinion sets out an approach to assessing whether any further processing is for an incompatible purpose. Moreover, Recital 50 of the GDPR states that in assessing compatibility it is necessary to take account of any link between the original and the new processing, the reasonable expectations of the data subjects, the nature of the data, the consequences of the further processing, and the existence of safeguards.
Yet, automatic capture of tourism data through sensors might be collected for potentially secondary unauthorized purposes that had not been initially scheduled or still to be discovered, or for profiling, for abusive marketing activity, undermining this way the purpose limitation principle.
Anyway, in practical settings, companies «[…] repackage data by de-identifying them (using pseudonyms or aggregation) or creating derived data, with only the original dataset being subjected to data minimization. The repackaged data can then be sold on and repurposed in a plethora of ways that have little to do with the original reason for data generation and without the need to give notice or consent to those that the data concerns»[58].

3.4. Data Minimization: Collection and Retention

The GDPR says personal data shall be «[…] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed», Art. 5 (1) (c), and so organizations should minimize the amount of data they collect and process, and the length of time they keep the data.
Yet, in substance, smart technology purports the massive collection, aggregation and algorithmic analysis of all the available for various reasons, such as understanding customer buying behaviors and patterns or remarketing based on intelligent analytics. Big data analytics may discover unexpected correlations that do not retrospectively justify obtaining the data in the first place, for example, between data about people's lifestyles and their credit worthiness. Therefore, organizations need to be clear about which data is deemed to be *necessary, excessive* and *relevant* for the purposes of the pro-

[57] Council of Europe Guidelines, *Protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD, 2017.

[58] D. Solove, *I've Got Nothing to Hide and Other Misunderstandings of Privacy*, in *San Diego Law Review*, vol. 44, 2017, 745 ss.

cessing.
In addition, personal data shall not be kept longer than necessary for the purpose for which it is being processed, as prescribed by the storage limitation principle, Art. 5 (1) (e). This principle is becoming part of the lifecycle governance strategy retention policies of companies that defensibly dispose irrelevant data instead of keeping data archived forever. Retention schedules allow unnecessary data to be disposed of as it is no longer of business value or needed to meet legal obligations.

3.5. Accuracy and Up-to-date Processing

Results drawn from big data analysis may not always be representative or accurate as sought (Art. 5 (1) (d)), if sources aren´t accurate as well (*i.*e. analysis based on social media resources are not necessarily representative of the whole population at stake) [59].
Organizations employing ML algorithms to discover associations need to consider the distinction between correlations and causations[60], *i.e.*, when there is no *direct cause and effect* between two phenomena that show a close correlation. In these cases there is a risk of drawing inaccurate, but also – and when applied at the individual strata – potentially unfair and discriminatory conclusions[61]. The potential accuracy (or inaccuracy) of any resulting decisions might cause discriminatory, erroneous and unjustified decisions, regarding data subject´s behavior on health, creditworthiness, recruitment, insurance risk, etc..
Even exercising the "right to be forgotten" (Art. 17), where data subjects will have the right for their data to be erased in several situations, for e.g., when the data is no longer necessary for the purpose for which it was collected, or based on inaccurate data, it may be difficult for a business to find and erase someone's data if it is stored across several different systems and jurisdictions[62].
Further, inaccuracy of data endangers the data quality principle and triggers abstract strict liability for damage[63].
The quality of the profiles and the quality of personal data on which they are built, again, seem to matter for the prosperity of the industry, yet another relevant privacy principle.

4. Reflections and Conclusions

This study is novel in having undertaken an initial exploration of the legal implications

[59] ICO, *Big Data, Artificial Intelligence,* cit..

[60] *Ibidem*

[61] EDPS, Opinion 7/2015, *Meeting the challenges of big data.*

[62] C. Bartolini – L. Siry, *The right to be forgotten in the light of the consent of the data subject*, in *Computer Law and Security Review*, vol. 32, 2016, 218 ss.

[63] T. Hoeren, *Big Data and Data Quality*, in T. Hoeren – B. Kolany-Raiser (eds.), *Big Data in Context - Legal, Social and Technological Insights*, Heilderberg, 2018, 1 ss.

that technology-enhanced (and empowered) tourism experiences imply to data protection and privacy. The preceding analysis brings out that smart tourism is becoming a big contributor and benefactor of ubiquitous, always-on data-capture about consumer-tourists towards empowered tourism experiences and competitive markets. This data allows the detection and prediction of future behaviors and trends; allows the analysis of development and optimization processes of products/services, retention of customers, and ultimately is useful for future decision-making.

Patently, with new forms of ICTs emerging over the coming years, more types of technology-empowered experiences are expected to flourish further and trigger new challenges to the body of tourism knowledge and wariness therewith.

As for now, the current assumption is that all captured information is extremely valuable and necessary to organizations and will be freely provided by the smart tourists who seek enriched tourism experiences[64].

This extensive collection and processing of personal data in the context of smart tourism destinations using algorithm-driven techniques has given rise to serious privacy concerns, especially relating to the wide ranging electronic surveillance, profiling, and disclosure of private data.

Moreover, the lack of privacy and data protection mindset of engineers and coders working in IoT/cloud business poses a very large problem for the future[65].

In this line, smart technologies used in STD often produce situations of imbalance, where data subjects are not aware of the fundamental elements of data processing and related consequences, being unable to negotiate their information, which leads to a side effect of enhanced information asymmetry[66].

Information asymmetry and inadequate provision of information and data sharing to the public about data use can be seen as hampering tourist trust in STD.

This scenario is particularly acute with "digital natives" or "*millennials*" tourists who have grown up with ubiquitous internet access and share willingness personal information via social media with fewer concerns for how it may be used.

Smart tourism raises big issues with respect to information governance[67] and about correctly deriving the *added* value from information in an open and ubiquitous info-structure. The apprehension here is to understand if the affordances of the technology, the personalized services, and empowered experiences can cope with data protection obligations without a micro-targeting and profiling for unintended uses, safeguarding the right to equal treatment, to non-discrimination and the protection of personal autonomy based on a person's right to control his/ her personal data, that may never be the price paid for an enhanced awareness.

---

64 P. Tallon, *Corporate governance of big data: perspectives on value, risk, and cost,* in *Computer*, vol. 46, issue 6, 2013, 32 ss.

65 P. Schwartz - D. Solove, *op. cit.*

66 M.D. Masseno, *Personal data circulation from the EU to USA and now what for the American Tourism Industry with business in Europe*?, 23rd International Tourism Safety Conference, Las Vegas, 2016.

67 I. Hadar – T. Hasson et al., *Privacy by designers: software developers' privacy mindset*, in *Empirical Software Engineering*, vol. 23, issue 1, 2018, 259 ss.

In the forthcoming future, controllers should adopt a precautionary approach[68] in regulating data protection in this field of STD, such as adoption of compliance tools enable STD organizations meeting their data protection obligations while protecting people's privacy rights in a STD context, and they are: anonymization and pseudonymization techniques, privacy policies, data protection impact assessment (DPIA), personal data stores, algorithmic transparency, privacy seals/certification, and privacy by design measures to mitigate the appointed legal risks and implications. It is suggested that STD are to proceed with test prototyping and research before the implementation of new technologies and services in large-scale real-life environments, such as the Mobile Living Lab[69].

As future work, besides addressing related information security issues according to the NIS Directive[70], future research regarding mobile devices and tracking will be needed, following the adoption of the new *ePrivacy* Regulation[71], as well as qualifying the roles of data controller and data processer in the context of STD. Besides, as stated in the Tourism Science literature, tourism, by definition, is a service-intense industry with a "business network", since it relies on a number of stakeholders for its ability to deliver products and services[72]. Hence, the term *business network* refers to «[…] a collection of inter firm relationships, including alliances, long-term buyer-supplier relationships, and informal collaborations» where each of the actors involved process personal data and therefore their legal obligations should abide to the GDPR.

[68] ICO, *Big Data, Artificial Intelligence,* cit.

[69] L. Edwards, *op. cit.*

[70] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[71] Proposal of a Regulation of the EP and of the Council concerning the respect for private life and the protection of personal data in electronic communications, COM/2017/010 final - 2017/03 (COD).

[72] P. Robertson, *An Assessment of Collaborative Governance in a Network for Sustainable Tourism: The Case of RedeTuris*, in *International Journal of Public Administration*, vol. 34, issue 5, 2011, 279 ss.

Economia della privacy: una rassegna della letteratura*

Jacopo Arpetti

Abstract

L'analisi dei nessi tra avanzamento tecnologico ed erosione della sfera della riservatezza costituisce un elemento caratterizzante dell'odierno dibattito sulla privacy, in particolare in relazione ai mutamenti verificatisi nel settore delle comunicazioni di massa. In tale ambiente, pochi *gatekeeper* posti in posizione apicale rispetto al mercato risultano in grado di tracciare e correlare le abitudini di miliardi di consumatori attraverso piattaforme, servizi online e siti internet. Si è così dato luogo ad una nuova forma di sorveglianza di cui sono protagoniste alcune imprese private che, tramite la rilevazione delle preferenze, dei desideri e degli interessi di miliardi di persone, hanno reso la raccolta e lo sfruttamento dei dati il core-business delle loro attività. Si è pertanto innescato un processo per il quale i dati personali vengono percepiti come "merce di scambio". Merce che viene ceduta dai consumatori al fine di ottenere, senza il pagamento di un corrispettivo in denaro, i servizi offerti dalle imprese, e che viene acquisita da queste ultime al fine di proporre ai consumatori servizi ad-hoc, vendere spazi pubblicitari mirati, ovvero destinarla al commercio con terzi. A fronte della rivelazione di proprie informazioni personali, l'individuo può infatti trarre benefici tangibili ed immediati in termini di compensazioni monetarie sotto forma di sconti o premi, accesso a trattamenti preferenziali, o a servizi personalizzati. Al contempo, l'individuo dovrà però sostenere dei costi che si concretizzano - da un lato - in termini di "costi di invasione" in relazione a spam, telemarketing, pubblicità postale e - dall'altro - in relazione ai costi legati alla "profilazione": sarà infatti possibile che all'utente vengano rivolte offerte selettive e disegnate, cioè, sulle sue specifiche capacità di spesa, nonché sulle sue propensioni.

The analysis of the connections between technological enhancement and erosion of the privacy sphere is one of the most relevant issues within the current debate around privacy, particularly in the light of the changes occurred in the mass communications sector. In this context, few data gatekeepers in a dominant position are able to trace and correlate the habits of billions of consumers by exploiting platforms, online services and websites. A new form of surveillance has therefore arisen: through the identification of preferences, wishes and interests of billions of people, some private companies collect and exploit such information, making data the core-business of their activities.In such context, personal data are perceived as a "tradable asset"; they are identified indeed as goods transferable by consumers in order to obtain, without mo-

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

netary exchanges, the services offered by such companies. These latter, in turn, acquire such data in order to offer ad-hoc services to the same consumers, or to sell targeted advertising space, or to sell them to third parties. By disclosing personal information, individuals can obtain tangible and immediate benefits in terms of monetary compensations such as discounts and rewards; or they can access preferential treatments and customized services. However, beside benefits, there are costs that individuals have to face in terms of "invasion" (such as spam) and "profiling": the consumer might be receiving selective offers based on his specific spending power and propensities.

Sommario

1. La privacy nella società dell'informazione - 2. Definizione del concetto di privacy - 3. Il concetto economico di privacy - 4. Profilazione dei consumatori e pratiche di discriminazione di prezzo nell'era dell'economia digitale

Keywords: Privacy, Big Data, Piattaforme, Discriminazione di prezzo, Dati personali

1. La privacy nella società dell'informazione

Le nozioni di privacy rintracciabili in letteratura sono molteplici e differiscono l'una dall'altra a seconda dell'angolo visuale da cui vengono analizzate le problematiche relative al conflitto tra gli interessi racchiusi nella sfera pubblica e quelli afferenti alla sfera privata degli individui, intesi anche quali consumatori. Nell'arco degli ultimi decenni sono state attribuite al concetto di privacy, a seconda dell'ambito di indagine[1], decine di differenti definizioni[2]. In proposito, si rileva, da un lato, l'impossibilità di isolare una definizione univoca del concetto di privacy (i numerosi tentativi di individuare una definizione hanno portato all'emersione di un quadro frammentato e spesso composto da enunciazioni non empiricamente verificate); dall'altro, emerge con forza la consapevolezza di come l'evoluzione del concetto generale di privacy e la ridefinizione dei confini tra sfera privata e pubblica[3], facciano il paio con l'evoluzione della tecnologia dell'informazione[4].L'analisi dei nessi tra avanzamento tecnologico ed erosione della sfera della riservatezza costituisce d'altronde un elemento caratterizzante l'intero dibattito sulla privacy[5], che affonda le radici nell'affermazione della fotografia sulla carta stampata alla fine del XVIII secolo. Furono Warren e Brandeis, nel noto articolo pub-

[1] «*The term "privacy" is an umbrella term, referring to a wide and disparate group of related things*». Si veda: L. Brandimarte - A. Acquisti, *The Economics of Privacy*, in *The Oxford Handbook of the Digital Economy*, Oxford, 2012, 547 ss.

[2] K.-L. Hui - I. Png, *Economics of Privacy*, in *Handbook of Information Systems and Economics, Terry Hendershott,* Amsterdam, 2005, 471 ss.

[3] *Ibid.*

[4] D.J. Solove, *A Taxonomy of Privacy*, in *University of Pennsylvania Law Review* 154, 2005, Philadelphia, 477 ss.

[5] *Ibid.,* 195.

blicato sulla Harvard Law Review nel 1890[6], ad evidenziare la portata rivoluzionaria dei mezzi di comunicazione di massa ai fini della riservatezza[7].

Dalla fine dell'800 ad oggi, alla sopra citata nozione di privacy quale diritto soggettivo fondamentale identificabile con il diritto ad essere lasciati indisturbati ("*to be left alone*"), è subentrata – tra gli anni '60 e '70 del '900 – l'idea secondo la quale il diritto alla privacy si gioca piuttosto sul fronte delle modalità di gestione dei dati riferibili all'individuo; non è un caso che la prima legge europea in tema di privacy, la legge svedese del 1973, porti il nome di *Datalangen*.

In tale evoluzione della concettualizzazione sulla privacy, un ruolo rilevante è stato giocato dal progresso tecnologico e, in particolare, dai mutamenti da ultimo intervenuti nel settore delle comunicazioni di massa. A tale proposito, tra le rivoluzioni che si sono imposte nel secolo scorso, quella che ha maggiormente permeato ogni settore dell'economia ed ogni aspetto della vita quotidiana è stata quella relativa alla rete Internet e all'imporsi del Web, un sistema informativo distribuito e ipermediale, giunto oggi alla sua versione 2.0.

Si è passati infatti dal Web 1.0, «in cui l'utente appariva come un passivo ricettore di dati e informazioni, […] (al, *ndr.*) Web 2.0 (universo in cui, *ndr.*) si è cominciato ad assistere a un'inedita interattività, per la quale i contenuti sono più spesso prodotti dagli utenti della rete»[8]; ciò ha reso gli individui non più meri fruitori di informazioni nel web, ma vere e proprie fucine di dati, spesso a carattere altamente personale. La diffusione del *mobile computing*, unitamente al dilagare delle tecnologie legate ai sensori, ha inoltre offuscato la distinzione tra ciò che è digitale e ciò che è fisico, tra *online* e *offline*. In tale contesto, si sono imposti sul mercato servizi in grado di generare e, contestualmente, registrare informazioni relative ad attività personali ovvero professionali dell'individuo, delle quali precedentemente non si lasciava traccia nel mondo reale[9]. Al contempo, Internet si è evoluta da un'architettura decentrata e basata su interazioni anonime, ad una in cui pacchetti di dati registrano ogni genere di comportamento tenuto dagli utenti[10]. In ragione di tale evoluzione, garantire la sicurezza dei propri dati, proteggere la propria privacy, diventa sempre più difficile in un contesto in cui la disponibilità delle informazioni nel web aumenta esponenzialmente in un'ottica di condivisione sempre più ampia e di portata globale[11].

In tale ambiente, pochi *gatekeeper* posti in posizione apicale rispetto al mercato risultano in grado di tracciare e correlare le abitudini di miliardi di consumatori attraverso piattaforme, servizi online e siti internet[12]. «Si è così dato luogo ad una "nuova sorveglian-

---

6 S.D. Warren - L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review* 4, no. 5, 1890, 193 ss.

7 *Ibid.*

8 U. Pagallo, *La Tutela Della Privacy Negli Stati Uniti d'America e in Europa : Modelli Giuridici a Confronto*, Milano, 2008.

9 A. Acquisti - C.R. Taylor - L. Wagman, *The Economics of Privacy*, in *SSRN Electronic Journal*, 2015, 3.

10 U. Pagallo, *Il Diritto Nell'età Dell'informazione: Il Riposizionamento Tecnologico Degli Ordinamenti Giuridici Tra Complessità Sociale, Lotta per Il Potere e Tutela Dei Diritti*, Torino, 2014, 172 - 173

11 K. Cukier, *Data, Data Everywhere*, in *The Economist*, Special report, 2010.

12 A. Acquisti - C.R. Taylor - L. Wagman, *The Economics of Privacy,* cit., 3.

za"»[13] di cui sono protagoniste alcune imprese private che, tramite la rilevazione delle preferenze, dei desideri e degli interessi di miliardi di persone, hanno reso la raccolta e lo sfruttamento dei dati il *core-business* delle loro attività. Mentre a metà degli anni 2000 si restava ancora stupiti che il miracolo della rete fosse fondato sull'offerta, all'apparenza gratuita, di una molteplicità di servizi[14], oggi i consumatori - anche alla luce dell'ultimo scandalo che ha coinvolto il colosso di Menlo Park[15]-[16] - stanno acquisendo consapevolezza del fatto che i colossi del web traggono parte delle proprie fortune dalla "compravendita" dei dati personali[17].

Si è pertanto innescato un processo per il quale i dati personali vengono percepiti come "merce di scambio". Merce che viene ceduta dai consumatori al fine di ottenere, senza il pagamento di un corrispettivo in denaro, i servizi offerti dalle imprese, e che viene acquisita da queste ultime al fine di proporre ai consumatori servizi ad-hoc, vendere spazi pubblicitari mirati, ovvero destinarla al commercio con terzi.

A fronte della rivelazione di proprie informazioni personali, l'individuo può infatti trarre benefici tangibili ed immediati in termini di compensazioni monetarie sotto forma di sconti o premi, accesso a trattamenti preferenziali, o a servizi personalizzati. Vi sono tuttavia due generi di costi che l'individuo dovrà sostenere. Dovrà fronteggiare, da un lato, maggiori "costi di invasione" in relazione a *spam*, *telemarketing*, pubblicità postale e, dall'altro, costi legati alla "profilazione". Sarà infatti possibile che all'utente vengano rivolte offerte selettive (disegnate cioè sulle sue specifiche capacità ed intenzioni di spesa) e che lo stesso sia destinatario di politiche di discriminazione del prezzo[18].

Nel momento in cui presta il consenso alla cessione dei propri dati personali, l'individuo – in maniera più o meno consapevole – compie pertanto una valutazione in termini di costi-benefici, analoga a quella svolta a fronte di qualsivoglia scelta di acquisto. In questo specifico frangente, tale scelta è però orientata a comprendere se sia conveniente barattare le proprie informazioni personali in cambio di benefici di altra natura (economici e non).

Gli individui non dispongono di tutte le informazioni atte a misurare i costi (incerti e potenziali) in maniera puntuale, proprio perché immersi in un contesto nel quale è difficile compiere valutazioni di questo genere[19]. In relazione a tale contesto - mutuando le parole di Varian[20] - Alessandro Acquisti usa la metafora della sottoscrizione dell'"assegno in bianco" per descrivere il momento in cui l'individuo decide di rivelare le proprie

[13] U. Pagallo, *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti,* cit., 179 ss.

[14] *Ibidem*, 181.

[15] M. Rosenberg - N. Confessore - C. Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, *The New York Times*, 2018.

[16] C. Cadwalladr - E. Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, *The Guardian*, 2018.

[17] A. Acquisti, *Privacy*, in *Rivista di politica economica,* V–VI, 2005, 332.

[18] *Ibid.*

[19] H.R. Varian, *Economic Aspects of Personal Privacy*, in *Internet Policy and Economics,* Boston, 1996, 127 -137.

[20] *Ibid.*

informazioni personali[21]. Infatti, gli individui chiamati a compiere scelte in ordine alla cessione delle proprie informazioni personali, sono immersi in un ambiente incerto e connotato da componenti esogene ed endogene di difficile comprensione[22].

Prima componente che condiziona la scelta è pertanto l'incertezza: gli individui, contestualmente alla cessione di propri dati, dovranno cioè fare i conti con l'incertezza riguardante la natura stessa dei *trade-off* implicati e le proprie preferenze al riguardo. D'altronde, l'incertezza è uno degli elementi costituitivi dell'asimmetria informativa (Akerlof, 1970[23]) dovuta al progresso tecnologico ed al *data collection*. Infatti, la tecnologia ha fatto sì che la raccolta e l'utilizzo dei dati personali siano invisibili agli occhi dell'utente e questi ultimi hanno quindi raramente consapevolezza di quali e quante informazioni ad essi riferite vengano effettivamente acquisite, né di come le stesse vengano utilizzate e con quali conseguenze. Tale scenario fa sì che le persone, nella misura in cui non sono consapevoli della limitatezza della propria conoscenza al riguardo, mostrino un certo grado di incertezza rispetto ai dati da condividere[24].

Seconda componente che influenza le scelte del consumatore in tema di privacy è quella del contesto (c.d. "*context-dependence*" delle preferenze individuali in tema di privacy), che induce atteggiamenti diversi di un medesimo individuo con riferimento ai timori riguardanti la condivisione dei propri dati personali; i soggetti passano cioè da estrema preoccupazione a totale indifferenza rispetto alla cessione degli stessi al variare delle situazioni di contesto. Gli autori più sopra citati sintetizzano efficacemente tale fenomenologia mutuando la terminologia usata da Westin[25]-[26] nel 1968: "siamo tutti pragmatici della privacy, fondamentalisti della privacy o incuranti privacy, a seconda del momento e del luogo"[27].

Terza ed ultima determinante delle scelte dei consumatori in tema di cessione di propri dati personali è la "malleabilità" dei detentori degli stessi. Tale duttilità è dovuta alla generalmente scarsa consapevolezza dei diversi fattori che, in un data circostanza, determinano la predisposizione nei confronti della cessione di propri dati personali. Tale limitatezza informativa fa il paio invece con la complessità informativa nella disponibilità degli attori la cui prosperità, a livello economico, si fonda sul *data collection*[28]. L'emergere dell'era dell'informazione, congiuntamente ai crescenti interessi economici sviluppatisi attorno al *business* della raccolta dei dati personali, ha fatto sì infatti che le aziende interessate a tali mercati mettessero a punto e sfruttassero alcuni processi comportamentali e psicologici per promuovere la *disclosure* dei dati personali da parte

21 A. Acquisti, *The Economics of Personal Data and the Economics of Privacy*, 2010, 26.

22 A. Acquisti - L. Brandimarte - G. Loewenstein, *Privacy and Human Behavior in the Age of Information*, in *Science,* New York*,* 347, no. 6221, 2015, 510-514.

23 G.A. Akerlof, *The Market for "Lemons" Quality Uncertainty and the Market Mechanism*, in *The Quarterly Journal of Economics,* 84, no. 3, 1970, 488 ss.

24 A. Acquisti - L. Brandimarte - G. Loewenstein, *Privacy and Human Behavior in the Age of Information,* cit.*,* 510-514.

25 A.F. Westin, *Privacy And Freedom*, in *Washington and Lee Law Review,* 166, 1968.

26 J.M. Urban - C.J. Hoofnagle, *The Privacy Pragmatic as Privacy Vulnerable.*

27 A. Acquisti - L. Brandimarte - G. Loewenstein, *Privacy and Human Behavior in the Age of Information,* cit.*, 511.*

28 *Ibid,* 512.

degli utenti. Tali meccanismi fanno perno sulla "malleabilità" delle preferenze espresse dagli individui circa il livello di privacy desiderato[29].
Si assiste dunque ad un'evoluzione nell'articolazione del contesto in cui gli individui assumono le proprie decisioni relative al livello di tutela della privacy desiderato, in ragione di un alto livello di asimmetria informativa, incertezza e vulnerabilità, frutto delle complessità proprie dell'era dell'informazione. Data l'evoluzione dei mercati, la privacy non viene pertanto intesa più esclusivamente quale diritto soggettivo, ma si è piuttosto affermato il concetto di "*Information Privacy*", la cui elaborazione - al netto delle diverse sfumature assegnategli dagli autori - dimostra l'avvenuta rimodulazione del diritto soggettivo ed il progressivo assestamento su una nozione di privacy che non può non contemplare il controllo sui potenziali usi dei dati personali all'interno del relativo mercato secondario.

2. Definizione del concetto di privacy

L'avanzamento tecnologico e l'introduzione di banche dati globalmente interconnesse nel perimetro della società dell'informazione hanno fatto sì che ai dati personali venisse assegnato un valore in quanto nuova fonte di ricchezza economica e sociale[30]. Di converso, a tale evoluzione della società e dei mercati ha corrisposto l'attribuzione di un valore alla tutela della privacy, ossia alla scelta di non condividere dati personali. Alla condivisione di proprie informazioni con terzi si associano infatti costi potenziali, quali quelli sostenuti dal consumatore in caso di attuazione di pratiche di discriminazione di prezzo da parte del fornitore del servizio. Allo stesso tempo, sono evidenti i benefici per il consumatore nei casi in cui la cessione di propri dati personali avvenga, ad esempio, allo scopo di poter contattare un proprio amico tramite un social network, ovvero di ottenere sconti personalizzati, o ancora di conseguire un risultato più aderente alle proprie preferenze attraverso il motore di ricerca usato per navigare su internet[31]. Come affermato da Kupfer[32] nel 1987, siamo naturalmente portati a valutare e soppesare, nel momento in cui vengono condivisi, benefici e costi della cessione di dati personali. E questo in ragione della natura stessa della privacy:
«[…] *When we share information about ourselves with someone, therefore, we share something made valuable because made scarce or special by privacy*[33]».
Sul piano definitorio, la privacy può così essere identificata con il proprio diritto di "ritirarsi dal mondo" così come espresso da Warren e Brandeis; con il diritto al controllo e alla salvaguardia delle proprie informazioni personali (Westin, 1968[34]); essa può inoltre essere declinata quale aspetto qualificante della dignità, dell'autonomia e, in

[29] *Ibid.*

[30] O. Tene - J. Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, in *Stan. L. Rev. Online*, 2011, 63-69.

[31] A, Acquisti -C.R. Taylor - L. Wagman, *The Economics of Privacy*, cit., 4.

[32] J. Kupfer, *Privacy, Autonomy, and Self-Concept*, in *American Philosophical Quarterly* 24, no. 1, 1987, 81 -89.

[33] *Ibid,* 85. Kupfer cita, a sua volta: S.D. Warren - L.D. Brandeis, *The Right to Privacy,* cit.

[34] A.F. Westin, *op. cit.*

definitiva, della libertà umana, quale «*selective control of access to the self*»[35] (Altman, "il controllo selettivo dell'accesso al sé"), ovvero, così come espresso da Stone ed altri[36], quale: *«[…] The ability (i.e., capacity) of the individual to control personally (vis-a-vis other individuals, groups, organizations, etc) information about one's self»*[37].

Una definizione, quest'ultima, che gli autori qualificano come "*control-oriented*"[38] e che segnala pertanto come l'individuo eserciti un duplice controllo sulle informazioni ad esso riferite, da un lato applicato all'ammontare dei propri dati personali suscettibili di cessione e, dall'altro, riferito invece alle modalità di condivisione dei medesimi[39].

Le definizioni di privacy messe a fuoco dalla letteratura e più sopra riportate, nonostante differiscano l'una dall'altra in ragione delle diverse prospettive di analisi degli autori, presentano come minimo comune denominatore l'elemento del confine tra sé e gli altri, tra ciò che è privato e ciò che è pubblico.

In qualità di individui e di consumatori varchiamo continuamente tale confine, e le decisioni che assumiamo in relazione ad esso implicano benefici (tangibili e intangibili), ma anche costi, per noi stessi e per la società[40]. *L'economia della Privacy* esplora i *trade-off* associati al bilanciamento tra sfera pubblica e privata nell'ambito delle interazioni tra gli attori che entrano in contatto, vale a dire individui, organizzazioni e governi[41]. In tale contesto, l'interesse degli economisti per la privacy si è focalizzato principalmente sulla dimensione informativa della stessa, vale a dire sui *trade-off* derivanti dalla scelta, indicativamente razionale dell'individuo (informata cioè da relativi rischi e benefici) in ordine alla cessione o meno di propri dati personali[42].

Se si affronta la privacy non come diritto assoluto, ma come "sfera" soggetta ai principi economici alla base dell'analisi costi-benefici[43], è allora possibile categorizzare la *privacy* come *commodity* e considerare la cessione di dati personali alla stregua della cessione di merce. È possibile esplicitare la nozione di *privacy as a commodity* congegnata da Ben-

[35] S.T. Margulis, *On the Status and Contribution of Westin's and Altman's Theories of Privacy*, in *Journal of Social Issues* 59, no. 2, 2003, 418.; e I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*, Irvington, 1975.

[36] E.F. Stone et al., *A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes across Several Types of Organizations*, in *Journal of Applied Psychology* 68, no. 3, 1983, 459-468.

[37] *Ibid,* 460. La letteratura scientifica che affronta tali aspetti, basa i propri studi sull'analisi della teoria del comportamento pianificato, della teoria dell'azione ragionata, della teoria della scelta razionale, della teoria della deterrenza e della teoria della motivazione alla protezione.

[38] *Ibid,* 460.

[39] A. De Santo - C. Gaspoz, *Influence of Users' Privacy Risks Literacy on the Intention to Install a Mobile Application.*, in *New Contributions in Information Systems and Technologies,* Volume 1, 2015, 329.

[40] A. Acquisti - C.R. Taylor - L. Wagman, cit., 42.

[41] *Ibid.*

[42] *Ibid.*

[43] H.J. Smith - T. Dinev - H. Xu, *Information Privacy Research: An Interdisciplinary Review*, in *MIS Quarterly*, vol. 35, in *Society for Management Information Systems,* 2011, 993.

nett[44], e poi ripresa da Davies[45]-[46].

Tale approccio alla privacy ha da subito innescato un aspro dibattito (si veda Cohen[47]) in ragione del fatto che non sempre gli individui dimostrano di saper compiere scelte razionali. La maggior parte degli studi condotti in proposito evidenzia infatti come l'utente abbia una scarsa capacità di assumere decisioni che tengano adeguatamente conto dei rischi connessi alla diffusione dei propri dati personali[48], e ancor più evidenzia come ogni situazione differisca significativamente dall'altra e che, sulla base di ogni singola circostanza, ogni individuo compia una scelta a sé stante in relazione alle specifiche preoccupazioni indotte dal contesto[49]; d'altro canto, Altman definisce quest'ultimo come una vera e propria estensione del sé: «[…] *enviroment is both a determinant and an extension of behavior (self)*»[50]. Lungo un'analoga linea interpretativa, Malhotra ed altri nel 2004[51] evidenziano come le problematiche connesse alla salvaguardia del diritto alla privacy siano percepite dai singoli individui in maniera diversa, poiché condizionate da elementi esogeni come la cultura relativa a tali aspetti, o la normativa di riferimento[52]. Inoltre, la percezione di un individuo rispetto ai rischi connessi alla privacy può derivare da esperienze personali ed è pertanto normale che individui differenti mostrino opinioni e sensibilità diverse rispetto all'opportunità che un'impresa faccia *collection* dei propri dati personali[53].

La letteratura isola pertanto fattori esogeni e, per altro verso, fattori di natura fortemente personale quali elementi alla base del processo decisionale che un individuo mette in atto nel momento in cui è in procinto di cedere i propri dati personali. Tra essi, possono essere ricompresi: il tipo di informazioni raccolte (almeno dichiaratamente) dal venditore, i vantaggi economici che l'utente trae dall'operazione o dal servizio offerto e la percezione che l'utente ha rispetto alla tutela della propria privacy, nel momento in cui interagisce con uno specifico sito Web[54].

---

44 C.J. Bennett, *In Defence of Privacy: The Concept and the Regime*, in *Surveillance & Society* 8, no. 4, 2011, 485-496.

45 S. Davies, *Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, in P. Agre - M. Rotenberg (eds.), *Technology and Privacy: The New Landscape,* Cambridge, 1997, 144.

46 H.J. Smith - T. Dinev - H. Xu, *Information Privacy Research: An Interdisciplinary Review,* cit., 993.

47 J.E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffrey Rosen*, in *Georgetown Law Journal* 89, 2000.

48 H. Li - R. Sarathy - H. Xu, *Understanding Situational Online Information Disclosure as a Privacy Calculus*, in *Journal of Computer Information Systems* 51, no. 1, 2015.

49 D.J. Solove, *op. cit,* 507.

50 S.T. Margulis, *op. cit*, 420.

51 N.K. Malhotra - S.S. Kim - J. Agarwal, *Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model*, in *Information Systems Research* 15, no. 4, 2004, 337 ss.

52 *Ibid.*

53 *Ibid.*

54 H. Li – R. Sarathy – H. Xu, *Understanding Situational Online Information Disclosure as a Privacy Calculus*, in *Journal of Computer Information Systems*, 2010, 3 ss.

3. Il concetto economico di privacy

Il presente articolo si propone di scandagliare i principali *trade-off* associati a decisioni alternativamente di condivisione ovvero di protezione dei dati personali, in relazione alla possibilità, da parte degli individui, di beneficiare di alcuni servizi offerti sul mercato in cambio della cessione dei propri dati personali. Mutuando le parole di Eli Noam nel 1997:

«[…] *Privacy is not a static concept but an interaction, in which the rights of different parties collide.* […] *Privacy is an issue of control over information flows, with a much greater inherent complexity than a conventional "consumers versus business*»[55].

Peraltro, citando L. Brandimarte e A. Acquisti, si può utilmente integrare tale accezione "informazionale" e transattiva della privacy (intesa cioè quale ambito di disponibilità e relativa gestione di un monte dati personali in un contesto di transazioni economiche) tramite il brocardo:

«[…] *Where trade-offs are, there lie opportunities for economic analysis*»[56].

In tale ottica, va tuttavia preliminarmente evidenziato che gli studi oggetto della presente *review* non hanno raggiunto risultati tali da determinare in maniera univoca se la *disclosure* dei propri dati personali, ovvero una maggiore avversione rispetto alla condivisione degli stessi, implichino cambiamenti economici netti in termini positivi o negativi[57].

Come anticipato al capitolo 2 del presente lavoro, è tuttavia possibile condurre un esame della c.d. *informational privacy* che, da un'angolazione economica[58], permetta cioè di quantificare i costi-opportunità soppesati da individui e organizzazioni coinvolti in decisioni relative alla gestione di dati personali, i costi ed i benefici connessi alla protezione o alla condivisione degli stessi e le relative esternalità. D'altronde, le implicazioni economiche del concetto di *privacy* sono note dal 1977, da quando Posner constatò quanto segue[59].

Posner rilevò[60] che, mentre può essere discutibile se il concetto di privacy abbia implicazioni economiche significative laddove inteso come contrapposizione dei concetti di "*freedom*" e "*quiet*", esso ne ha certamente qualora inteso come occultamento di informazioni personali[61]. D'altronde, le informazioni non sono che un segnale (secondo

[55] E.M. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, in *Privacy and Self-Regulation in the Information Age*, 1997, 21-33.

[56] L. Brandimarte - A. Acquisti, *The Economics of Privacy*, in *The Oxford Handbook of the Digital Economy*, Oxford, 2012, 548.

[57] A. Acquisti - C.R. Taylor - L. Wagman, *op. cit.,* 443-444.

[58] L. Brandimarte - A. Acquisti, *op. cit,* 550 ss.

[59] R.A. Posner, *The Right of Privacy*, in *Georgia Law Review* 12, no. 3, 1977, 393 ss.

[60] R.A. Posner, *The Right of Privacy*, *op. cit.*, 394: *«People invariably possess information, including facts about themselves and contents of communications, that they will incur costs to conceal. Sometimes such information is of value to others: that is, others will incur costs to discover it. Thus, we have two economic goods, "privacy" and "prying." We could regard them purely as consumption goods, the way economic analysis normally regards turnips or beer; and we would then speak of a "taste" for privacy or for prying».*

[61] L. Brandimarte - A. Acquisti, *op. cit.,* 549.

quanto esposto dalla teoria di Spence[62]-[63]) riguardante una persona, un segnale che gli individui possono voler razionalmente condividere o celare nel corso delle transazioni con altre parti. Mette conto, a tale proposito, ricordare che costituiscono oggetto di analisi della teoria economica anche le modalità di massimizzazione dell'utilità di un agente economico e, nella misura in cui l'esigenza di *informational privacy* rientra nella funzione di utilità di un agente, la teoria economica non potrà che trattarla quale oggetto di studio[64].

Abbiamo dunque, da un lato, individui, imprese e governi che vogliono carpire quante più informazioni possibile riguardo agli attori con cui interagiscono – facendo però attenzione a non travalicare il limite per il quale tali azioni sarebbero percepite come invasive da parte dei soggetti *target* – e, dall'altro, individui che decidono di rivelare proprie informazioni personali per poter beneficiare di trattamenti privilegiati in cambio di un pezzo della propria privacy. Il bilanciamento dei *trade-off* per ciascun attore, unitamente al fronteggiarsi di interessi confliggenti, fa sì che emergano, in relazione alla privacy, dinamiche di stampo economico.

Prima di procedere all'analisi dei benefici e dei costi relativi alla protezione o alla rivelazione dei propri dati personali, è bene precisare tre elementi. Innanzitutto va ribadito come, anche in presenza di *trade-off* da valutare razionalmente, l'agente economico non sia pienamente consapevole dell'impatto delle proprie decisioni sul proprio livello di privacy; in secondo luogo, non è possibile presumere che ad ogni *trade-off* relativo a questioni di privacy sia associato un corrispettivo monetario[65] (anche se alcuni elementi che contribuiscono al benessere psicologico e fisico degli individui potrebbero essere interpretati in termini economici quali fonti di utilità individuale[66]); infine, vengono in rilievo dimensioni della privacy che, pur limitando il benessere degli individui, potrebbero essere di fatto non misurabili, pur non configurandosi quali totalmente intangibili[67].

È possibile analizzare il valore economico della privacy osservando i costi e i benefici, sociali e personali, associati alla *disclosure* o alla mancata cessione di dati personali. La letteratura analizzata nella presente rassegna prende in considerazione due attori: i

[62] «Nel 1973 il premio Nobel per l'economia M. Spence elaborò un modello, basato sul mercato del lavoro, in cui dimostrava che informazioni convenzionali, come livello di educazione, età, esperienza di un individuo, costituiscono dei s. per il datore di lavoro durante le fasi di contrattazione e di assunzione. Spesso, infatti, un datore di lavoro assume i propri dipendenti in condizioni di incertezza, poiché ha una conoscenza solo parziale dell'effettiva produttività e delle capacità individuali del futuro dipendente. Spence distingue, in particolare, gli attributi riferiti agli individui presenti sul mercato del lavoro in 'fissi', come l'età, il sesso e la razza, e "variabili", ossia modificabili attraverso comportamenti e investimenti effettuati dall'individuo, come l'esperienza, il livello di educazione e le capacità. Questa seconda categoria fornisce, secondo Spence, il s. che aiuta il datore di lavoro a definire la distribuzione di probabilità della produttività del futuro dipendente; e poiché alcune di queste modifiche, come quelle relative al livello di istruzione, sono costose, individui razionali decideranno di agire solo in base a s. che massimizzino la differenza tra i ritorni attesi (i livelli salariali) e i costi di modifica del segnale», dalla voce: "Segnale", Enciclopedia Treccani, disponibile al presente indirizzo.

[63] M. Spence, *Job Market Signaling,* in *The Quarterly Journal of Economics* 87, no. 3, 1973, 355 ss.

[64] L. Brandimarte - A. Acquisti, *op. cit*, 550.

[65] A. Acquisti, *Privacy*, in *Rivista Di Politica Economica,* V–VI, 2005, 326.

[66] A. Acquisti*, The Economics of Personal Data and the Economics of Privacy,* cit., 5.

[67] L. Brandimarte - A. Acquisti, *op. cit.,* 550-551.

consumatori e le imprese[68].
Vanno inoltre fatte le seguenti precisazioni in merito alla privacy intesa come bene economico, ovvero quale *"commodity*". Queste attengono alle caratteristiche, sotto il profilo economico, delle informazioni personali scambiate sul mercato[69]:

non rivalità e non escludibilità: le informazioni personali degli individui mostrano alcune delle caratteristiche proprie dei beni pubblici, come la non rivalità e la non escludibilità, nonostante una delle principali caratteristiche della *Information privacy* sia rappresentata dall'interesse a mantenere riservate le informazioni personali al fine di escludere i terzi dal loro possesso ed utilizzo;

informazione asimmetrica: la società dell'informazione, nella quale le transazioni che riguardano la gestione dei dati personali avvengono in ambiente online, presenta contraddizioni tali per cui a generici richiami all'esigenza di assicurare un maggior grado di privacy ad individui e consumatori, si contrappone la facilità con cui gli stessi condividono in rete propri dati personali in cambio di esigui incentivi. Tale contraddizione è dovuta ad una duplice forma di asimmetria informativa[70]-[71]: inizialmente è l'individuo a rendersi protagonista di un tentativo di controllo delle proprie informazioni, non volendo divulgare ciò che lo riguarda e che gli altri non conoscono (prima di cedere le proprie informazioni, il consumatore sa quale sia la propria disponibilità a pagare, mentre non è a conoscenza chi vuole ottenere tale informazione); dopodiché, una volta ceduti propri dati, il soggetto che ha fornito il proprio benestare in tale senso, ne perde il controllo e non ha più contezza dei futuri contesti in cui essi verranno usati o a chi verranno rivenduti in seguito[72];

*classificazione della privacy come bene economico: s*ul fronte della classificazione dei beni economici, la privacy mostra tratti riconducibili sia ai beni strumentali (o intermedi), sia a quelli di consumo (o finali)[73]: nel momento in cui, adottando la prospettiva soggettiva degli individui, si pensa alla privacy quale bene in sé, la si concepisce come bene finale. Al contrario, se si pensa all'insorgere dei *trade-off* relativi alla decisione del consumatore di proteggere ovvero condividere i propri dati, si pensa alla privacy quale bene

68 A. Acquisti*, The Economics of Personal Data and the Economics of Privacy,* cit., 10 ss.

69 A. Acquisti - C.R. Taylor - L. Wagman, *op. cit.,* 446.

70 Si veda: G.A. Akerlof, *op. cit.*; e : A. Acquisti, *Privacy*, cit.

71 «Per asimmetria informativa si intende la condizione che si verifica nel mercato quando uno o più operatori dispongono di informazioni più precise di altri. In generale, interferisce con il buon funzionamento dei mercati, portando a situazioni di sotto utilizzazione delle risorse disponibili. L'a. i., infatti, può indurre l'operatore meglio informato a comportamenti opportunistici: per es., un'impresa finanziata da terzi potrebbe assumersi rischi eccessivi, un assicurato potrebbe non tutelare le sue proprietà con la dovuta cura, un lavoratore difficilmente licenziabile potrebbe sottrarsi al proprio impegno. Questi comportamenti portano, rispettivamente, al razionamento del credito da parte delle banche, all'impossibilità di ottenere copertura assicurativa completa a prezzi equi e a una minore occupazione […]». Dalla voce "*Asimmetria informativa*" dell'Enciclopedia Treccani.

72 A. Acquisti, *Privacy,* cit., 342.

73 A. Acquisti - C.R. Taylor - L. Wagman, *op. cit.,* 447.

intermedio[74], in quanto il consumatore si focalizza (a seconda di quello che sarà il bilanciamento da esso operato tra costi e benefici) sui benefici, (dovuti, ad esempio, alla possibilità di usufruire di servizi personalizzati, o alla possibilità di accedere ad alcuni servizi gratuiti), oppure sui costi associati alla perdita di privacy, e questo indipendente dal valore che lo stesso individuo assegna alla perdita di privacy in assoluto e non in relazione a quello specifico *trade-off*.

A partire dagli anni '70, la teoria economica ha visto il progressivo consolidamento di alcune posizioni riguardo il valore delle informazioni personali e le relative problematiche di privacy. In estrema sintesi, richiamando la definizione di *privacy as commodity* (di cui al capitolo 2) la Scuola di Chicago, attestandosi su posizioni liberiste ed utilitariste, si è opposta a chi, come Hirshleifer, teorizzava che la privacy fosse qualcosa di più di una merce da scambiare.

In linea con quest'ultimo pensiero, e rifacendosi alla scuola austriaca di von Hayek, alcuni economisti hanno cominciato ad interpretare la teoria economica declinandola in relazione al valore dell'informazione, ossia a partire dal valore informativo che il prezzo assume nell'economia di mercato. Di converso, la Scuola di Chicago (tra i cui maggiori esponenti trattati in questa rassegna figurano Posner e Stigler) ha teorizzato, sullo sfondo di un approccio neoclassico[75], che la protezione della privacy determinasse inefficienze economiche, in quanto la sottrazione di informazioni potenzialmente rilevanti ad alcuni agenti economici avrebbe impedito la formazione di decisioni economicamente efficienti.

A tale proposito, Posner concepì la privacy come strumento di occultamento alla società intera di informazioni rilevanti da parte dell'individuo; nell'ottica del magistrato ed economista statunitense, l'individuo si rappresenterebbe cioè in maniera non veritiera, ingenerando inefficienze allocative nel sistema economico. In sostanza, la normativa a tutela della privacy trasferirebbe il costo delle caratteristiche negative di un dato agente economico al resto degli attori presenti sul mercato[76]-[77]. Sulla medesima linea si posiziona Stigler, secondo il quale una legislazione restrittiva in ordine alla gestione dei dati personali ridurrebbe la qualità delle informazioni a disposizione degli agenti coinvolti nelle transazioni, a scapito, ad esempio, dei lavoratori con maggiore produttività. Secondo Stigler, gli individui hanno infatti un interesse a divulgare propri dati personali solo nel caso in cui questi delineino un'immagine positiva di loro stessi. Tale aspetto finirebbe per penalizzare i soggetti più meritevoli, dato che le loro qualità positive non

---

74 *Ibid.*

75 Secondo l'approccio teorico neoclassico, i mercati sono perfettamente competitivi, in quanto popolati da agenti economici che operano detenendo informazioni complete e simmetriche La disponibilità di tutte le informazioni rilevanti da parte di tutti gli agenti economici presenti sul mercato è in grado di assicurare, secondo tale approccio, il conseguimento autonomo dell'efficienza economica da parte dei mercati. A titolo esemplificativo, si rammenta che, in un'ottica neoclassica, ogni consumatore conosce il prezzo a cui ogni impresa in un dato mercato vende il proprio prodotto e che tale trasparenza informativa fà sì che la concorrenza spinga i prezzi verso il basso, compatibilmente con la tecnologia produttiva disponibile, a vantaggio del benessere dei consumatori.

76 R.A. Posner, *The Right of Privacy*, cit.

77 G.J. Stigler, *The Theory of Price*, New York, 1978.

verrebbero messe in risalto dal mercato[78].

Sia Posner che Stigler sostengono dunque che la privacy genera inefficienze di mercato sotto forma di meccanismi di redistribuzione salariali che opererebbero dall'alto verso il basso, facendo sì che un lavoratore con produttività minore benefici della difficoltà di misurazione delle differenze di produttività fra individui in un contesto regolamentare particolarmente rigido in termini di privacy, così trasferendo il costo di una caratteristica negativa - come sostenuto da Posner[79] - da un soggetto ad un altro[80].

Tali posizioni ben esemplificano l'avversione della Scuola di Chicago rispetto ad interventi regolatori da parte dello Stato in tema di trattamento dei dati personali, in quanto i limiti al trasferimento delle informazioni tra agenti sono ritenuti dannosi[81]-[82].

In assoluto, Stigler (1980) ritiene che, nel momento in cui la transazione tra agenti economici viene intrapresa in modo volontario, non è necessario interferire con essa a tutela di una delle parti: una transazione, se libera da interventi esogeni (normativi), darà luogo alla cessione di un equo ed efficiente ammontare di informazioni tra le parti, sulla base del livello di privacy desiderato. Stigler illustra il meccanismo secondo il quale la controparte offre servizi a prezzi più alti all'individuo che cela i propri dati (e

[78] G.J. Stigler, *An Introduction to Privacy in Economics and Politics*, in *The Journal of Legal Studies* 9, no. 4, 1980, 630:«*When it becomes more difficult to measure differences among individuals, their treatment becomes more uniform. Lower and higher risk credit are treated as average risk credit, and similarly with the traits of workers, students, and others. It has become a little easier to default on consumer credit, to embezzle funds, and to shirk duties*».

[79] R.A. Posner, *The Economics of Privacy*, in *The American Economic Review* (American Economic Association, 1981, 405: «*To relate the economics of privacy to the economics of information in as clear a fashion as possible, consider the example of the employer searching across employees and the employee searching across employers. The employer is looking for certain traits in an employee that may not be obvious, things like honesty, diligence, loyalty, and good physical and mental health. To the extent that the employee is deficient in one or more of these characteristics, he has an incentive- strictly analogous to the incentive of a seller of goods to conceal product defects- to conceal these deficiencies. That is, he has an incentive to invoke a "right of privacy" if the employer tries to "pry" into his private life*».

[80] L. Brandimarte - A. Acquisti, *op. cit,* 552.

[81] R.A. Posner, *The Right of Privacy*, cit., 402 ss.

[82] Non mancano peraltro passaggi controversi nell'analisi sulla redistribuzione salariale proposta da Posner (nel 1981). Come in R.A. Posner, *The Economics of Privacy*, cit., 407: «[...] *The principal beneficiaries of such legislation are people with more arrests or convictions, or poorer credit records (more judgments, bankruptcies, etc.), than the average person. These groups are presumably not cohesive enough to overcome the free-rider problems that plague efforts to form effective political coalitions, but they overlap strongly with racial and ethnic groups, namely black and Hispanic Americans, which are politically organized. Given laws that forbid discrimination against members of these racial and ethnic groups, it may be in their interest to press for passage of laws that also forbid "discrimination" against people with poor credit records and lengthy criminal records. If employers and creditors are unable to use these criteria to sift out poor employment risks and poor credit risks, respectively, a redistribution of wealth from whites to members of these racial and ethnic groups may result*».

pertanto anche caratteristiche indesiderabili)[83].

Negare ad altri agenti economici le proprie informazioni personali è, secondo Stigler, causa di inefficienze: come già detto, il costo di eventuali "pecche" viene traferito su altri soggetti, mentre «si ritarda il processo in cui imprese e lavoratori si incontrano su livelli di efficienza»[84]. Nello specifico, la privacy:

«*it reduces the amount of information in the market, and hence the efficiency with which the market-whether the market for labor, or spouses, or friends-allocates resources*»[85].

In risposta all'avversione nei confronti di una disciplina eccessivamente stringente a tutela della privacy, percepita come inversamente redistributiva da parte della Scuola di Chicago, Hirshleifer – nel 1980 – critica invece duramente le posizioni di Posner e Stigler. Hirshleifer li accusa infatti di aver tenuto in considerazione solo alcuni degli aspetti relativi alla privacy e di aver isolato tale elemento esclusivamente nella sua accezione di mercato. La semplificazione delle relazioni che hanno al centro questioni relative alla privacy, sostiene Hirshleifer, è sì utilizzabile ai fini della teorizzazione di modelli, ma all'appiattimento delle relazioni tra individui nel solo perimetro della logica di mercato[86] sfuggono inevitabilmente alcune delle dinamiche umane che sono alla base delle citate transazioni[87].

Già nel 1971, Hirshleifer[88] - adottando la prospettiva del pianificatore intento alla massimizzazione del benessere sociale[89] - aveva osservato come, pur avendo effetti redistributivi, l'investimento nella raccolta delle informazioni private fosse inefficiente, causando sovrainvestimenti nella raccolta delle stesse[90].

Inoltre, Hirshleifer sostiene che, anche nel caso in cui le informazioni riguardanti i

---

[83] G.J. Stigler, *An Introduction to Privacy in Economics and Politics*, cit., 625-626: «*Yet if all credit-history information, for example, were "owned" by the debtor, and there were not a special difficulty in enforcing this ownership because of the public good character of information, this inherent partnership in producing information would create no special problems. I would have an established credit record with the merchant with whom I customarily dealt, and be charged for credit according to the cost of dealing with me (including the cost of learning my payment habits). Another merchant, to whom I denied access to my regular merchant's information, would charge for credit appropriately to his ignorance of my credit worthiness, so in general it would pay me to ask the regular merchant to supply the credit record to others. This would be true even if I were a poor credit risk: the new merchant would extend credit only at high charges to those who refused to reveal their previous records. In the long run, in a sequence of many repetitive transactions, even a poor credit risk can do no better than to deal with informed creditors.* […] *The economy of the multiple use of the same information should be accommodated no matter how the ownership of the information is assigned. The failure of contracts to emerge which specify that the creditor may not sell the consumer credit information is in the interest of debtors, for whom credit would otherwise be more expensive*».

[84] A. Acquisti, *Privacy, cit.*, 345.

[85] R.A. Posner, *The Economics of Privacy*, *cit.* 406.

[86] Stigler e Posner vedono gli individui come agenti economici freddi, razionali e "*utility maximizers*".

[87] J. Hirshleifer, *Privacy: Its Origin, Function, and Future*, in *The Journal of Legal Studies* 9, no. 4, 1980, 649-650.

[88] J. Hirshleifer, *The Private and Social Value of Information and the Reward to Inventive Activity*, in *The American Economic Review* 61, no. 4, 1980, 561 ss.

[89] L L. Brandimarte - A. Acquisti, *op. cit,* 553.

[90] J. Hirshleifer, *The Private and Social Value of Information and the Reward to Inventive Activity,* cit.: «*When private information fails to lead to improved productive alignments [...], it is evident that the individual's source of gain can only be at the expense of his fellows. But even where the information is disseminated and does lead to improved productive commitments, the distributive transfer gain will surely be far greater than the relatively minor productive gain the individual might reap from the redirection of his own real investment commitments*».

consumatori dovessero essere acquisite a costo zero da parte del venditore, l'incentivo dello stesso a massimizzare i profitti per mezzo della *profilazione* del consumatore potrebbe essere in contrasto con l'interesse pubblico[91]. Infatti, ad alcuni consumatori potrebbe essere praticato un prezzo fuori mercato, con la conseguente esclusione degli stessi dal consumo di beni che l'efficienza sociale richiederebbe, al contrario, che essi consumino[92].

Negli anni '90, l'economia della privacy ha destato nuovamente attenzione, con la pubblicazione di una seconda ondata di studi. La diffusione delle *Information and Communication Technologies* (ICT) congiuntamente all'affermazione di Internet, alle opportunità di sviluppo dei mercati ad esso legati e all'esplosione dell'uso secondario dei dati personali, hanno fatto sì che fosse necessario un ripensamento – in chiave moderna – dei *trade-off* associati alla protezione e alla rivelazione dei dati personali.

Varian[93], nel 1996, parla di privacy nell'era dell'ICT e delle continue sollecitazioni a cui le imprese sottopongono gli individui, nell'intento di rilevare le loro preferenze. Parlando dell'insorgere di una nuova forma di "fastidio"[94], l'autore sostiene che il continuo bombardamento di informazioni non è necessariamente profittevole[95].

L'attenzione degli individui rischia quindi di diventare un boomerang, l'attività pubblicitaria finisce per essere percepita come fonte di "fastidio", generando eccessivi costi di transazione (sotto forma di costi di ricerca delle informazioni riguardanti gli agenti), facendo sì che – al netto dell'ammontare di informazioni scambiate in termini assoluti – vengano in realtà scambiate poche informazioni utili. Pur isolando tale dimensione, Varian[96] riconosce come sia comunque nell'interesse del consumatore che il venditore abbia alcune informazioni che lo riguardano, ad esempio affinché gli vengano proposti i beni che hanno attirato la sua attenzione, ma non quelli etichettati come non graditi.

Non è però possibile ignorare come il nuovo contesto disegnato dalle emergenti *Information and Communication Technologies* determini l'insorgere, in capo all'individuo, di

---

91 Come sostenuto in: A. Acquisti - C.R. Taylor - L. Wagman, *op. cit,* 10: «*Hirshleifer shows that, given equilibrium prices, the private benefit of information acquisition may outweigh its social benefit*»..

92 L. Brandimarte - A. Acquisti, *op. cit,* 553.

93 H.R. Varian, *Economic Aspects of Personal Privacy*, in Internet Policy and Economics, 2009, cit. 101-109.

94 Inteso come "*Right to be annoyed*".

95 H.R. Varian, *Economic Aspects of Personal Privacy*, *cit*., 102: «*When many people talk about "privacy rights," they really are talking about the "right not to be annoyed." I don't really care if someone has my telephone number as long as they don't call me during dinner and try to sell me insurance. Similarly, I don't care if someone has my address, as long as they don't send me lots of official- looking letters offering to refinance my house or sell me mortgage insurance. In this case, the annoyance is in the form of a distraction – the seller uses more of my "attention" than I would like. In the "information age," attention is becoming a more and more valuable commodity, and ways to economize on attention may be quite valuable. Junk mail, junk phone calls, and junk e-mail are annoying and costly to consumers. In the context of the apple example described (in the notes , e2d.), it is as though the seller of apples has to tell me about each of the different kinds of apples that he has to sell before I am able to purchase. It is important to recognize that this form of annoyance – essentially excess search costs – arises because the seller has too little information about the buyer. If the seller knows precisely whether or not I am interested in buying insurance or refinancing my mortgage, he can make a much better decision about whether or not to provide me with information about his product*».

96 H.R. Varian, *Economic Aspects of Personal Privacy*, cit., 103: «*In this context, the more the seller knows about my preferences, the better it is. If, for example, I am interested in buying a computer printer, it may well be in my interest and in the seller's interest for this fact to be known. If I am only interested in a laser printer, this is even more valuable information, as it further reduces search costs for both buyer and seller. If I already have a laser printer that I am happy with, the seller may find that valuable to know as he will not have to incur costs trying in vain to sell me a new printer*».

costi potenziali nuovi rispetto a quelli precedentemente analizzati da Stigler e Posner a fronte dell'emersione di un mercato secondario dei dati. La possibilità che questi, precedentemente ceduti ad un'impresa affinché ne venisse fatto un determinato uso, possano invece essere rivenduti a terzi per fini differenti fa sì che Varian parli di alcune esternalità. Secondo l'autore, queste ultime possono essere mitigate nella misura in cui l'informazione relativa all'individuo venga ceduta dal primo agente che l'ha acquisita al futuro acquirente, previo chiarimento di una serie di "regole di ingaggio", affinché al consumatore vengano cioè offerti esclusivamente beni e servizi di suo interesse ed il "fastidio" da esso percepito possa quindi essere mitigato[97].

Secondo Varian, si giunge dunque ad una sorta di paradosso per il quale i consumatori che risentiranno di maggiori costi legati alla privacy saranno quelli sui quali è stato scambiato un numero minore di informazioni: avendo i rivenditori un'informazione scarsamente dettagliata nei loro riguardi, è infatti possibile che la profilazione dell'utente sia avvenuta con minore precisione, generando costi (o comunque nessuna suddivisione dei profitti[98]) in capo al consumatore sotto forma di maggior livello di "*annoyance*" (fastidio), dovuto al fatto che verranno ad essi offerti beni e servizi non graditi. Al contempo, Varian riconosce come naturale l'interesse dell'individuo a celare parte delle proprie informazioni personali, come quelle che, ad esempio, potrebbero svelare la propria disponibilità a pagare per un determinato bene.

Nello specifico, il costo che il consumatore dovrà affrontare in relazione alla rivendita di proprie informazioni sul mercato secondario dei dati si traduce in esternalità che possono, ad esempio, assumere la forma di spam o – come illustrato da Andrew Odlyzko[99] nel 2003 (tale aspetto verrà trattato, nello specifico, nel capitolo successivo) – di "*adverse price discimination*" a spese del consumatore.

Un ulteriore aggiornamento delle tesi avanzate in materia di privacy da parte degli esponenti più sopra citati della Scuola di Chicago è rappresentato dalla rivisitazione del teorema di Coase[100] da parte di Eli M. Noam[101]. Secondo quanto teorizzato da Coase, anche in presenza di esternalità, qualora i costi di negoziazione e di transazione siano nulli, la contrattazione tra le parti porta ad una soluzione efficiente[102] (in termini paretiani) indipendentemente dall'attore che detiene i diritti legali o di proprietà. Nel caso delle transazioni che riguardano dati personali, facendo riferimento ai mezzi tecnologici oggi disponibili (in particolare, in ragione della possibilità di criptare le informazioni personali) Noam ha riproposto l'ottica di Coase affermando che tra una parte il cui interesse è proteggere i propri dati ed un'altra il cui interesse è quello di ottenere tali informazioni, prevarrà (indipendentemente dal soggetto individuato dalla legge come legittimo detentore del dato personale) la parte con un interesse maggiore rispetto

97 *Ibid.*

98 A. Acquisti, *The Economics of Personal Data and the Economics of Privacy*, cit.

99 A. Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet*, in in *Proceedings of the 5th International Conference on Electronic Commerce - ICEC '03*, New York, 2003, 355-366.

100 R.H. Coase, *The Problem of Social Cost*, in *Journal of Law & Economics,* 3, 1960, 1 ss.

101 E. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, cit., 21-33.

102 J. Sloman - D. Garratt, *Microeconomia*, Bologna, 2004.

all'altra[103].

Va tuttavia rilevato come, in questo articolo del 1996 firmato da Noam, l'aspetto tecnologico non venga considerato quale determinante degli esiti della transazione che ha ad oggetto i dati personali; la crittografia è vista infatti solo come un mezzo tramite il quale è possibile realizzare uno scambio tra le parti, senza che nessuno possa appropriarsi dei dati del consumatore senza dare nulla in cambio. La tecnologia in questo caso costituisce solo un abilitante del trasferimento di ricchezza[104].

Ulteriori autori – sempre partendo dall'assunto proposto da Coase, ed in chiave critica rispetto alle argomentazioni proposte dalla Scuola di Chicago - hanno proposto differenti valutazioni delle dinamiche economiche scaturenti da questioni relative alla privacy. Ad esempio, Kahn, McAndrews e Roberds[105] hanno dimostrato che un certo grado di flessibilità contrattuale tra le parti, se accompagnato da diritti chiaramente definiti, fa sì che si possa ottenere il migliore dei risultati socialmente conseguibili. Tuttavia, gli stessi hanno evidenziato, in un lavoro congiunto del 2001, come, all'epoca, né la legge né la tecnologia attribuissero in maniera univoca i diritti legati alle transazioni di informazioni personali. Essi hanno inoltre segnalato che tale incertezza avrebbe generato una corsa allo sviluppo tecnologico nell'intento – da parte di alcuni attori - di impossessarsi dei dati altrui[106].

Gli autori sottolineano come il diritto alla privacy, le dinamiche economiche ad esso legate, il volume delle transazioni incentrate sullo scambio di dati, la capacità di aggregazione dei dati e le pratiche a cui potrà dar luogo l'incrocio degli stessi, avranno una rilevanza sempre maggiore man mano che la tecnologia evolverà.

Dall'analisi dei riflessi tecnologici delle dinamiche economiche prende poi forma la teoria avanzata da Luadon[107]. L'autore fa presente come la "crisi della privacy per ciò che concerne le informazioni personali" non sia da addebitare esclusivamente all'avanzamento tecnologico, ma rappresenti, invece, una vera e propria forma di fallimento di mercato. Il problema, secondo Laudon, è da rintracciare nel fatto che legalmente,

---

103 E. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, cit. Nello specifico: «[…] *Coase argues that in a conflict between the preferences of two people (but also rich), the final outcome will be determined by economic calculus and (as long as there are low transaction costs) result in the same outcome regardless of the allocation of rights. The reason is that people do not just stop dead in their tracks after some allocation is made, but they go on madly in optimizing their condition.* […] *Let us look at privacy, using the example of a credit card billing record, and telemarketer who tries to sell a consumer something after first checking out her shopping habits as recorded on the credit card bills. Both the consumer and a third party vendor attribute a certain value to the information.* […] *Suppose* […] *the consumer gets smart and starts to encrypt the information. In that case, it is now the telemarketer who will try to bribe the consumer to get the information. […] The existence of encryption.n may largely determine who has to pay whom, not whether something will happen*»

104 *Ibid.* Nello specifico: «[…] *Encryption does not necessarily determine whether access to private information actually take place, it only affects the final wealth distribution. This interactive concept is often difficult to grasp if one is used to think in absolutes. A rule is a rule, etc. but the analysis shows that encryption does not create privacy. It simply means that the consumers will get paid to give it up. In the past, such transactions were not possible. Encryption now creates barriers, which force outsiders to pay for what they used to get free. At the same time, the emergence of micro-transactions will make it possible for data miners to compensate consumers for their information*».

105 C.M. Kahn - J. McAndrews - W. Roberds, *A Theory of Transactions Privacy*, in *FRB Atlanta Working Paper,* No. 2000-22, 2001, 25.

106 *Ibid.*

107 K.C. Laudon, *Markets and Privacy*, in *Communications of the ACM* 39, no. 9, 1996, 92-104.

all'individuo non è riconosciuto alcun diritto di proprietà, non essendo consentito lo scambio dei dati personali quali merci dalle quali ricavare un compenso[108].

Per ovviare a tale problema, Laudon propose la creazione di un mercato nazionale delle informazioni (National Information Market – NIM) nel quale poter scambiare dati personali e dove gli individui avrebbero potuto depositare le proprie informazioni su base volontaria[109].

Contestualmente, secondo lo schema ideato da Laudon, si sarebbe dovuta concedere agli individui la possibilità di traferire i diritti sui propri dati in cambio di forme di compensazione. E questo secondo uno schema tripartito che avrebbe dovuto fondarsi sulle forze che dominano il mercato, su una forte regolazione (tramite la creazione di un'autorità di regolazione del mercato dei dati personali[110]) e sull'uso massiccio delle tecnologie esistenti per poter meglio definire i diritti ed assegnare le compensazioni. Tale modello, sviluppando l'idea di base per la quale un sistema di assegnazione dei diritti di proprietà avrebbe tutelato gli individui, favorendo al contempo gli interessi delle imprese, avrebbe garantito una maggiore efficienza e ridotto gli abusi[111].

Col risultato che:

«*The* […] *overall privacy invasion will decline and there will be a net increase in privacy because the cost of invading privacy will go up. People will have a greater understanding of the flow of information in the society*».[112]

Laudon crede dunque, in accordo con alcuni degli economisti appartenenti alla Scuola di Chicago già citati, che la protezione della privacy in termini puramente legali non risponda alle esigenze emerse. Criticando inoltre chi voleva estendere il teorema di Coase al mercato dei dati, Laudon sostiene l'inefficacia della sua applicazione alle transazioni che possono sfociare in eventi di violazione della privacy, proprio perché non disincentivante rispetto a prevaricazioni che può subire l'individuo in tal senso[113].

Laudon sostiene che la sua soluzione permette una riduzione dei costi in capo ai consumatori ed un aumento del benessere sociale attraverso la seguente soluzione:

«Under a regime in which individuals own their personal information, transaction costs may rise but only as far as necessary to pay for the cost of invading privacy. An NIM raises the cost of using personal information for reasons other than those for which it was gathered. This added cost discourages the obnoxious use of information that could undermine the foundations of a free society if left unchecked. There should be no free lunch when it comes to invading privacy. An NIM will result in less use of unsolicited communications—a key source of privacy concerns. Many other obnoxious uses of personal information will also decline. But an NIM will also lead to cost savings as firms use the latest technology to target their communications to smaller groups, devise new ways to market products

---

108 K. Laudon, *Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information*, 1997: «*Under current law, the ownership right to personal information is given to the collector of that information, and not to the individual to whom the information refers. Individuals have no property rights in their own personal information. As a result, they cannot participate in the flourishing market for personal information, i-e., they receive no compensation for the uses of their personal information*».

109 K.C. Laudon, *Markets and Privacy,* cit, 99.

110 *Ibid,*103.

111 *Ibid,* 101.

112 *Ibid,* 102.

113 *Ibid.*

and get market information, and compete with one another on their privacy-related corporate practices. Overall social welfare will increase».[114]

Analizzando la proposta di Laudon – che ipotizza un sistema, ben definito, di diritti di proprietà sulle informazioni personali – Acquisti[115] riconosce come la stessa sia la dimostrazione che tra le soluzioni di stampo regolamentare/normativo[116] e le soluzioni di mercato[117] alle problematiche di privacy non vi sia un vuoto incolmabile, ma che piuttosto vi sia, a cavallo tra le due visioni, uno spettro di possibili risposte. Nonostante l'attribuzione dei diritti di proprietà porti generalmente ad un miglioramento del benessere, concedere ai consumatori il diritto di vendere i propri dati personali può, a detta dell'autore, minare il surplus del consumatore[118].

4. Profilazione dei consumatori e pratiche di discriminazione di prezzo nell'era dell'economia digitale

La definitiva affermazione di Internet e la conseguente proliferazione delle transazioni in rete, congiuntamente all'evoluzione degli strumenti informatici in grado di aggregare e analizzare un'ingente mole di dati, spesso destrutturati, relativi ai consumi degli individui, hanno fatto sì che si moltiplicassero i database contenenti informazioni sui consumatori. Le aziende hanno così trovato naturale *targhettizzare* gli individui, vale a dire approssimarne al meglio caratteristiche e propensioni di acquisto, al fine di proporre loro offerte personalizzate per massimizzare vendite e profitti. Come afferma Varian[119], osservare e registrare comportamenti precedentemente non rilevabili porta infatti – grazie all'uso di alcuni strumenti informatici - al compimento di transazioni e contratti più efficienti, grazie alla disponibilità di un maggior numero di informazioni[120]-[121].

114 *Ibid,* 103.

115 A. Acquisti - C.R. Taylor - L. Wagman, *op. cit,* 453.

116 *Ibid.* In particolare, viene auspicata una rigida protezione normativa a tutela della privacy e dei dati personali.

117 Non viene prevista alcuna protezione normativa delle privacy. È tutto rimesso al comportamento del consumatore sul mercato, sulle politiche di gestione dei dati che ogni impresa si impone sulla base della concorrenza esterna.

118 K.C. Laudon, *Markets and Privacy,* cit.; A. Acquisti - C.R. Taylor - L. Wagman, *op. cit,* 453.

119 H.R. Varian, *Computer Mediated Transactions*, in *The American Economic Review,* American Economic Association, 2010, 2.

120 *Ibid,* 2.: «[...] *Computer in the middle of a transaction can observe and verify many aspects of a transaction. The record produced by the computer can allow the contracting parties to condition the contract on terms that were previously unobservable, thereby allowing for more efficient transactions. I am not claiming that increased observability will necessarily lead to more efficient contracts.* […] *I am only claiming that additional information allows for more efficient contracts. Of course, the study of contracts is a highly developed field in economics, and it is hardly novel to suggest that contractual form depends on what is observable*».

121 *Ibid.*: «*What is interesting, I think, is the way that progress in information technology enables new contractual forms. Consider, for example, a rental-car agency that buys insurance based on accident rates, and that accident rates in turn depend on the speed at which a vehicle is operated. All renters would prefer to drive within the speed limit if they were compensated with a lower rental fee. However, if there is no way to monitor the speed of the rental car, such a contractual provision is unenforceable. Putting a computer transmitter in the trunk of the car that records the vehicle's speed makes the contract enforceable and offers a Pareto improvement on the original arrangements*»

L'economia digitale si fonda oggi sull'uso di grandi quantità di dati meno strutturati che in passato e disponibili su larga scala, in *real time*[122] (i c.d. Big Data), impiegati al fine di comprendere quali siano i prodotti ed i servizi da proporre ad uno specifico consumatore, ovvero a *cluster* di essi. Si può in proposito affermare, come sostenuto da Acquisti, che l'economia digitale è in una certa misura finanziata[123] proprio attraverso questo genere di pratiche. Infatti, se è vero che – da un lato - i motori di ricerca affinano, anche nell'interesse dell'utente finale, i risultati delle ricerche compiute dagli individui sulla base delle *query* già effettuate dagli stessi, è altrettanto vero che – dall'altro - i venditori (ovvero le piattaforme di e-commerce, i *marketplace)* incrementano le proprie vendite tramite l'analisi degli acquisti compiuti dai consumatori e delle loro attività di navigazione[124], mentre i social network si affidano alla vendita dei dati ceduti loro dai propri sottoscrittori al fine di generare ricavi.

Ovviamente, l'imporsi del paradigma dei *Big Data*[125]-[126]-[127], frutto dell'avanzamento tecnologico e della conseguente riduzione dei costi relativi alla raccolta ed alla elaborazione dei dati, ha generato un certo numero di benefici privati ed esternalità positive, nonché di costi sociali ed esternalità negative. Se da un lato è indiscutibile che la rivoluzione dei *Big Data* abbia contribuito ad un aumento dell'efficienza economica sia per le organizzazioni (che hanno sperimentato un miglioramento delle operazioni, dell'allocazione delle risorse ed un più facile accesso all'innovazione), sia per gli individui (che, ad esempio, sperimenteranno nel prossimo futuro i benefici derivanti dal monitoraggio

---

122 E che, per giunta, riguardano attività precedentemente difficili da rilevare.

123 A. Acquisti - C.R. Taylor - L. Wagman, *op. cit.*

124 H.R. Varian, *Computer Mediated Transactions*, *cit.* 6. In particolare, vengono condotte analisi sui dati degli utenti affinché possano essere sottoposti alla loro attenzione prodotti più appetibili e meglio rispondenti alle preferenze degli stessi.

125 «*Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation*»: definizione fornita dal glossario della Gartner, disponibile al seguente indirizzo: www.gartner.com/it-glossary/big-data.

126 I *data scientist* considerano i Big Data come composti da più dimensioni. Ci sono autori che ne prendono addirittura in considerazione sette. Tuttavia, a titolo esemplificativo, verranno qui prese in considerazione esclusivamente le 4 dimensioni inizialmente rilevate, ossia: volume, velocità, varietà, veridicità:

- Volume: un'enorme quantità di dati strutturati e destrutturati viene creata da una vasta gamma di fonti eterogenee;
- Velocità (dati veloci): alcuni dati sono *time sensitive* e la velocità può quindi risultare un fattore chiave affinché abbia senso compiere determinate analisi sugli stessi. In questi casi, i dati devono essere elaborati e analizzati rapidamente (oggi la tecnologia consente di analizzare i dati mentre vengono generati, senza la necessità che essi vengano collocati in un database);
- Varietà: i dati sono disponibili in più formati e sono di diverso genere: possono essere dati numerici strutturati (ordinati in maniera tradizionale all'interno di un database), oppure non strutturati: testo all'interno di documenti, e-mail, o – ancora - video, audio, transazioni finanziarie, commenti pubblicati sui social network;
- Veridicità (*veracity*): ci si riferisce a tale dimensione in relazione alla veridicità dei dati.

Per un ulteriore approfondimento, si veda: S. Fosso Wamba et al., *How "Big Data" Can Make Big Impact: Findings from a Systematic Review and a Longitudinal Case Study*, in *International Journal of Production Economics* 165 (July 2015): 234–46, doi:10.1016/j.ijpe.2014.12.031.

127 Per un ulteriore approfondimento, si consulti la definizione di Big Data elaborata in: L. Einav - J. Levin, *Economics in the Age of Big Data*, in *Science* 346, no. 621. 2014.

delle proprie condizioni di salute attraverso tecniche di aggregazione di dati), è altrettanto vero che le imprese avranno di fatto accesso ad una sempre maggiore quantità di «*transactional data*» ottenuti da una molteplicità di fonti[128]. Tali dati, come riportato da Nir Kshetri[129], vengono definiti da Burrows e Savage come «*a crucial part of the informational infrastructures of contemporary capitalism*»[130] e possono essere impiegati per dar luogo alla personalizzazione delle offerte rivolte ai consumatori, migliorando così il benessere di questi ultimi e massimizzando, al contempo, i profitti delle imprese; al contrario, essi possono essere utilizzati per consentire alle imprese di mettere a punto strategie promozionali di natura predatoria, che comprimono il benessere del consumatore.
Come affermato da Varian:
«[…] *Computer mediated transactions allow for customization and personalization of the interactions by basing current transactions on earlier transactions or other relevant information. Instead of a "one size fits all" model, the Web offers a "market of one." Amazon, for example, makes suggestions of things to buy based on your previous purchases, or on purchases of consumers like you. These suggestions can be based on "recommender systems" of various sorts. Not only content, but prices may also be personalized, leading to various forms of differential pricing*».[131]- [132]
Le aziende trovano infatti redditizio segmentare i propri clienti sulla base della domanda che essi esprimono, ed attuare corrispondenti forme di discriminazione di prezzo.
È opportuno, a questo punto, fare chiarezza sulle formule ad oggi individuate di tale pratica per la quale la medesima merce viene venduta a prezzi differenti a consumatori diversi[133].
A tale scopo, al fine di verificare se si è in presenza di discriminazione di prezzo, anche

[128] H.R. Varian, *Computer Mediated Transactions,* cit.

[129] N. Kshetri, *Big Data's Impact on Privacy, Security and Consumer Welfare*, in *Telecommunications Policy* 38, no. 11, 2014.

[130] R. Burrows - M. Savage, *After the Crisis? Big Data and the Methodological Challenges of Empirical Sociology*, in *Big Data & Society* 1, no. 1, 2014, 2.

[131] H.R. Varian, *Computer Mediated Transactions*, cit., 6.

[132] Si veda anche: H.R. Varian, *Competition and Market Power*, in H.R. Varian - J. Farrell - C. Shapiro, *The Economics of Information Technology: An Introduction*, Cambridge, 2004.

[133] L.M.B. Cabral, *Economia Industriale*, Roma, 2002: «La pratica di fissare prezzi diversi per lo stesso bene (o per beni sostanzialmente identici, ndr.) in funzione della quantità acquistata, delle caratteristiche dell'acquirente, o di certe clausole contrattuali. […] Nella definizione di discriminazione di prezzo abbiamo specificato "prezzi diversi per lo stesso bene". Ma possiamo dire, ad esempio, che il prezzo di BMW negli Stati Uniti sia lo stesso identico prodotto di una BMW in Germania? […] Dal punto di vista del produttore, […] vendere un'auto tedesca negli Stati Uniti costa di più che venderla in Germania, a causa dei costi di trasporto e dei dazi doganali. […] (Perciò, *ndr.*), il fatto che il prezzo di una BMW sia più alto negli Stati Uniti che in Germania non è sufficiente a parlare di discriminazione di prezzo».

Varian[134-135-136-137] ha preso in prestito la definizione offerta da Stigler in "Theory of Price"[138]: si è in presenza di una pratica di discriminazione di prezzo se il rapporto tra i prezzi di due o più prodotti simili nei vari mercati è diverso dal rapporto tra i rispettivi costi marginali. La discriminazione può inoltre verificarsi nei confronti dello stesso gruppo di consumatori (ai quali potranno praticarsi prezzi diversi a seconda della quantità acquistata), tra diversi gruppi di consumatori, o tra mercati diversi isolati gli uni dagli altri[139] e si traduce nella vendita della stessa merce a due o più prezzi differenti[140]. L'evoluzione della tecnologia ha reso possibile uno *shift* progressivo tra i vari gradi di discriminazione di prezzo. L'impresa potrà infatti porre in essere diverse forme di discriminazione sulla base dei comportamenti ad essa noti dei consumatori. Qualora questi siano osservabili, un venditore potrà stabilire prezzi diversi sulla base degli stessi[141] e praticarli a segmenti differenti di consumatori[142], vale a dire, a segmenti di consumatori costruiti sulla base di caratteristiche osservabili comuni a gruppi demografici diversi[143]. È questa la discriminazione di prezzo di terzo grado, nel perimetro della quale il venditore disporrà di alcune informazioni riguardanti le preferenze dei consumatori, ma non potrà determinare le caratteristiche individuali di ciascun compratore[144], e potrà conseguentemente attuare forme di discriminazione di prezzo quali, ad esempio, sconti riservati a membri di determinate associazioni ovvero a soggetti appartenenti ad una determinata fascia anagrafica. Diversamente, - come nell'esempio delle classi ferroviarie in nota 148 – nel momento in cui sono i consumatori stessi ad auto-selezionarsi e a compiere una scelta tra diverse versioni ovvero tra diverse quantità di uno stesso bene o servizio, si è in presenza di una discriminazione di secondo grado. Se invece il venditore riesce a fissare prezzi diversi per ogni acquirente e per ogni quantità di bene acquistata, in modo da estrare la totalità del surplus del consumatore, si verifica una discriminazione di prezzo di primo grado, conosciuta anche come discriminazione

134 H.R. Varian, *Price Discrimination - Chapter 10*, in in *Handbook of Industrial Organization*, vol. 1, New York, 1989, 598 ss.

135 H.R. Varian - J. Joseph V. Farrell - C. Shapiro, *op. cit.*

136 A tale riguardo, Varian ha suggerito l'esistenza di un "terzo teorema del benessere" che si applica a casi (evidentemente estremi) caratterizzati da discriminazione di prezzo perfetta e libertà di ingresso: la discriminazione di prezzo perfetta dà luogo alla quantità ottimale di output venduto, mentre la libertà di entrata spinge i profitti a zero, conferendo tutti i vantaggi ai consumatori. Da: R. Burrows - M. Savage, *op. cit.*

137 H.R. Varian (in: C*omputer Mediated Transactions,* cit.) fa tuttavia notare come tale definizione non aderisca alla realtà per due diversi motivi: i diversi prezzi addebitati ai consumatori potrebbero in realtà essere attribuibili ai costi di trasporto, o ai costi di vendita del bene; inoltre, la discriminazione di prezzo potrebbe essere presente anche quando tutti i consumatori pagano lo stesso prezzo.

138 C.J. Stigler, *The Theory of Price,* cit.

139 M. Utton, *Market Dominance and Antitrust Policy*, Cheltenham, 2003.

140 C.J. Stigler, *The Theory of Price*, cit.; Cabral, *op. cit.*

141 L. Cabral, *op. cit.*

142 A. Acquisti, *Price Discrimination, Privacy Technologies, and User Acceptance*, in *Proceedings of the CHI2006 Workshop on Privacy-Enhanced Personalization*, Montrèal, 2006, 1-2.

143 Executive Office of the President of the United States, *Big Data and Differential Pricing*, 2015, spec. 4 e 9-10.

144 L. Cabral, *op. cit.*

perfetta[145]. In quest'ultimo caso, i prezzi rispecchiano i gusti e le preferenze dei consumatori, che possono essere desunti dall'osservazione del comportamento degli stessi, o rilevabili dalla loro "purchase history"[146].

In un contesto come quello dell'*e-commerce*, grazie all'uso di strumenti tecnologici che permettono una più accurata profilazione del consumatore, si sta passando dalla definizione di prezzi rivolti ad interi, seppur ben definiti, gruppi demografici, alla *targhettizzazione* del singolo. Il passaggio dalla segmentazione del mercato alla personalizzazione del prezzo corrisponde dunque al recedere di formule discriminatorie di terzo grado, a fronte dell'affermazione di una tipologia di discriminazione molto vicina a quella di primo grado[147].

La pratica della discriminazione di prezzo determina però dei costi a carico dei consumatori: essa potrebbe infatti incentivare gli agenti economici a degradare in modo inefficiente la qualità del prodotto venduto. Un esempio storico di tale degradazione del servizio ingenerata da un obiettivo di discriminazione di prezzo, a sua volta finalizzato all'accaparramento del surplus del consumatore, ci è fornita da Varian[148]. Un equivalente in chiave moderna di tale pratica potrebbe essere quello relativo alla possibilità di degradare la velocità della connessione Internet da parte degli ISP, al fine di dar luogo ad una gamma di offerte differenziate del medesimo servizio immesso sul mercato, a prezzi corrispondentemente diversi. I venditori potranno così trarre profitto a spese dei clienti di fascia alta, degradando il prodotto di fascia bassa, nonostante la riduzione del livello qualitativo risulti essere un'operazione costosa. Ulteriore esempio di tali pratiche di segmentazione è dato dalla produzione di più versioni dello stesso prodotto (c.d. *versioning*); le imprese fanno così in modo che i consumatori si auto-selezionino[149]

145 A. Acquisti, *Price Discrimination, Privacy Technologies, and User Acceptance,* cit., 54.

146 Executive Office of the President of the United States, *Big Data and Differential Pricing,* cit., 8 ss.

147 L. Cabral, *op. cit.*.

148 I primi operatori ferroviari intenti ad aumentare i propri profitti proponendo un prezzo maggiore ai clienti più facoltosi a fronte della fornitura di un servizio di trasporto sostanzialmente indifferenziato, al fine di poter discriminare le diverse disponibilità a pagare dei propri utenti, scelsero di eliminare il tetto dei vagoni di terza classe, per determinare un più tangibile divario qualitativo tra i servizi offerti in prima e terza classe e poter quindi aumentare la differenza di prezzo tra i biglietti delle varie classi; in Cabral, op. cit., *Ibid.*

149 L'autoselezione è una caratteristica della discriminazione di terzo grado: «l'impresa suddivide i consumatori in gruppi, ciascuno con una curva di domanda a elasticità diversa (ossia una differente sensibilità di variazione della quantità domandata al variare del prezzo), applicando prezzi diversi per ogni gruppo (più alti per quelli con elasticità minore). Per poter applicare in maniera efficace questo tipo di discriminazione di prezzo devono darsi due condizioni. In primo luogo l'impresa deve conoscere le caratteristiche della domanda dei diversi gruppi (o riuscire a sviluppare meccanismi di autoselezione dei consumatori, per es. rendendo, su un treno, la seconda classe più scomoda della prima)», dalla voce: "prezzo, discriminazione di", Enciclopedia Treccani.

e paghino prezzi differenti per versioni diverse del medesimo bene[150], nonostante sia più efficiente - in termini di costi produttivi – immettere su mercato un solo modello dello stesso[151]. Ad esempio, nel 1990, IBM ha venduto due versioni della stampante "LaserPrinter E", e l'unica differenza tra i due modelli era data dalla presenza di un chip che, nella versione più economica, rendeva la stampa più lenta rispetto al top di gamma[152]-[153].

Sebbene l'intenzionale rallentamento della stampa possa sembra irrazionale, l'eliminazione di alcune caratteristiche di un prodotto può facilitare la discriminazione di prezzo e paradossalmente aumentare il benessere sia delle imprese che dei consumatori, qualora il venditore riesca, attraverso tale pratica, a raggiunger un numero maggiore di clienti ai quali, altrimenti, non avrebbe potuto vendere il bene o il servizio desiderati. Tale pratica è peraltro enormemente diffusa per i beni catalogabili come "*information goods*"[154], ossia quei beni i cui costi di riproduzione sono in genere modesti rispetto al prezzo[155]. Per tali prodotti, le imprese rendono disponibili versioni differenti (nel caso dell'editoria, edizioni degli stessi libri, ma con copertina rigida, tascabile, e-book), oppure aggiungono e rimuovono funzionalità (limitazioni delle azioni che il singolo utente può effettuare) come parte integrante della strategia della linea di prodotti[156]. Tali strategie rappresentano comunque un rischio per le imprese e, alla luce delle difficoltà di previsione di acquisto di modelli simili da parte di utenti differenti, nonché del contestuale imporsi dell'uso massivo dei big data (con relativa *targhettizzazione* più accurata del consumatore e previsione della sua disponibilità a pagare), è molto probabile che le imprese preferiscano intraprendere le strada della "personalizzazione dei prezzi" e abbandonare quella del *versioning*. Va però fatto presente, come sostenuto nel

[150] La letteratura economica segnala come gli attori economici tradizionali possano constatare l'eterogeneità dei consumatori offrendo loro menù di prodotti e prezzi (differenti combinazioni quantità prezzo) – vale a dire attraverso una forma di autoselezione degli stessi- o, al contrario, osservarla direttamente. Un'impresa potrà dunque fissare un prezzo sulla base delle caratteristiche contrattuali del consumatore. In entrambi i casi, l'impresa cercherà di assegnare un prezzo ai propri prodotti in funzione della sottostante elasticità della domanda espressa da ciascun individuo, con l'intento di estrarre più surplus ed aumentare le vendite nei confronti dei consumatori che mostrano una maggiore elasticità. A tale riguardo si veda: H.R. Varian, *Price Discrimination - Chapter 10*, cit.

[151] Executive Office of the President of the United States, B*ig Data and Differential Pricing, cit.* 5: *«That is, IBM has added chips to the LaserPrinter E that serve as counters or idlers, chips that perform no function other than to make the machine pause and hence print more slowly*».

[152] R.J. Deneckere - R. Preston McAfee, *Damaged Goods*, in *Journal of Economics and Management Strategy* 5, no. 2, 1996, 153-154.

[153] «*A business practice in which a company produces different models of the same product, and then charges different prices for each model. Versioning a product gives the consumer the option of purchasing a higher valued model for more money or a lower valued model for less money. In this way, the business is attempting to attract higher prices based on the value a customer perceives*», da: Investopedia.

[154] «*Information good in economics and law is a type commodity whose market value is derived from information it contains. Examples include CDs containing pieces of music, DVDs containing movie content, and books containing short stories. Information goods are in contrast to material goods such as clothes, food, and cars. These can exist in either digitized form or analog format*», dalla voce: "*Information good*" di Wikipedia. Disponibile all'indirizzo: www.en.wikipedia.org/wiki/Information_good.

[155] L.A. Stole, *Price Discrimination and Competition, Chapter 34*, in *Handbook of Industrial Organization*, vol. 3, Amsterdam, 2007, 2221–2299.

[156] Executive Office of the President of the United States, *Big Data and Differential Pricing*, *cit.*

report redatto dalla Casa Bianca su "Big Data and Differential Pricing", che il *versioning* ha il vantaggio di ridurre gli effetti negativi della discriminazione di prezzo tramite big data, nel momento in cui i dati degli utenti vengono impiegati per dar vita a strategie di *versioning* basate sulla "personalizzazione di massa". E questo vale in particolare per gli "*information goods*", in ragione del fatto che possono essere personalizzati a fronte di un costo incrementale relativamente basso[157].

D'altronde, è inevitabile che si vada in questa direzione: la diminuzione del costo della *data collection* a livello di singolo utente ha reso più facile, per i venditori, identificare nuovi segmenti di clienti e rivolgersi a quei *cluster* con campagne di marketing ad-hoc.

I primi casi di discriminazione di prezzo sono stati registrati intorno ai primi anni 2000; di notevole chiarezza fu quello documentato da Streitfeld[158] nel settembre del 2000 sul Washington Post: un cliente di Amazon.com aveva acquistato un DVD a 24,49 $, notando però che il prezzo dello stesso prodotto, nel corso della settimana successiva all'acquisto, era salito a 26,24 $. Tuttavia, una volta eliminati i *cookies* e rimossi dal proprio computer i *tag* elettronici che lo identificavano come cliente abituale, il prezzo è tornato ad essere di 22,74 $. Ulteriore Un più recente caso ha coinvolto nel 2009 Microsoft ed il suo Bing Cashback. Pur essendo stato ideato come servizio rivolto ai consumatori affinché potessero ottenere un risparmio nelle loro transazioni online, sembra che alcuni siti di venditori terzi, utilizzando l'URL di provenienza dei consumatori, praticassero forme di discriminazione di prezzo a svantaggio dei visitatori reindirizzati da Bing[159].

Il fatto che si siano registrati casi simili, ha fatto emergere una copiosa letteratura al riguardo. La constatazione che il livello di privacy degli individui sia condizionato dal fatto che gli individui lasciano dietro di sé indelebili tracce elettroniche, ha infatti influenzato la ricerca, che si è discostata dalle posizioni più liberiste espresse degli autori precedenti (soprattutto dalla visione della scuola di Chicago, in base alla quale il consumatore è razionale) ed ha cominciato a prendere in considerazione la possibilità che gli individui non agiscano secondo i canoni propri degli agenti economici puramente razionali[160] (tesi, questa, illustrata, tra gli altri, nei lavori di Taylor[161], Varian e Acquisti[162]) e che pertanto, le regole del mercato potrebbero non essere sufficienti a garantire la protezione della privacy.

Ad innescare il vero cambiamento in termini di percezione di ciò che sarebbe potuto avvenire qualora un venditore avesse potuto manipolare e aggregare i dati dei consumatori, è stata l'accresciuta capacità di lavorazione dei dati riguardanti le preferenze ed i comportamenti degli individui: tale aspetto ha infatti incoraggiato – secondo alcuni

157 *Ibid.*

158 D. Streitfeld, *On the Web, Price Tags Blur*, in *The Washington Post*, 2000.

159 A. Acquisti, *The Economics of Personal Data and the Economics of Privacy*, cit, 29-30.

160 Si veda, a tale riguardo: ad A. Acquisti, *Privacy,* cit, 346 ss.

161 C.R. Taylor, *Consumer Privacy and the Market for Customer Information*, in *The RAND Journal of Economics* 35, no. 4, 2004, 631-650.

162 A. Acquisti - H.R. Varian, *Conditioning Prices on Purchase History*, in *Marketing Science* 24, no. 3, 2005, 367-381.

autori[163] - il passaggio dalla discriminazione di prezzo di terzo grado, basata su ampie categorie demografiche, alla possibilità di imporre prezzi personalizzati al singolo utente finale. A tale riguardo, nel 2000, Paul Krugman scriveva sulle colonne del New York Times:

«*Dynamic pricing is a new version of an old practice: price discrimination. It uses a potential buyer's electronic fingerprint -- his record of previous purchases, his address, maybe the other sites he has visited -- to size up how likely he is to balk if the price is high. If the customer looks price-sensitive, he gets a bargain; if he doesn't he pays a premium*»[164].

In tema di progressiva transizione verso forme di discriminazione di primo grado, il modello di Benjamin Reed Shiller[165], nel tentativo di predire quale genere di consumatori sottoscriverà un abbonamento a Neflix, mostra come il solo impiego di informazioni a carattere demografico (usate prima dell'avvento dell'ICT per definire prezzi differenziati) abbia una capacità scarsamente predittiva rispetto all'uso dei dati oggi generati dagli utenti che sfruttano la rete internet. Ad oggi Netflix compie una discriminazione di prezzo di secondo grado (facendo cioè sì che gli utenti si auto-selezionino attraverso l'acquisto di pacchetti di diverso prezzo), mentre Shiller ipotizza - stimando il valore dei prezzi di riserva dei consumatori tramite un modello edonistico di valutazione degli stessi - in che modo si potrebbe praticare una discriminazione di primo grado per mezzo dei moderni data set che oggi mappano i comportamenti e le preferenze degli individui (quindi dei big data), dando luogo ad un notevole incremento dei profitti e alla contemporanea riduzione dell'8% del surplus del consumatore[166]-[167].

In tal senso, la simulazione condotta da Shiller mostra come, nel caso in cui vengano esclusivamente impiegati dati demografici per praticare una discriminazione di prezzo, Netflix possa godere di un aumento dei profitti pari allo 0,8%, mentre, aggregando le informazioni generate dalla navigazione su internet da parte dei consumatori, si possa giungere ad un aumento dei profitti pari al 12,2% - facendo peraltro sì che alcuni utenti

---

163 Si veda, a tale riguardo: A. Acquisti, *Privacy,* cit, 346 ss.

164 P. Krugman, *Reckonings; What Price Fairness?*, in *The New York Times*, 2000.

165 B.R. Shiller et al., *First-Degree Price Discrimination Using Big Data*, 2014.

166 *Ibid.*, 1: «*If cost were no concern, then firms might hire private investigators to follow around every consumer all day every day, seeing which behaviors known buyers disproportionately do.* (But, nowadays times are changed. In the past, ed.) *personalized pricing has been extremely rare in practice, because profitable personalize pricing requires information on individuals' reservation values, which, simply put, was unavailable.* […] (Today, ed.) *Large datasets on individual behavior, popularly referred to as "big data," are available and may reveal information which can be used to form a hedonic estimate of individuals' reservation values.* […] *Many of these data, however, can now be captured at very low cost. Web-browsing, which reflects latent interests, is easily captured by ISPs, browsers, internet backbone providers, mo- bile phone operating systems, and large data brokers,* […] *that use "history sniffing." Any one of them could sell users' browsing histories. Widespread use of personalized pricing may have large effects on the overall economy. One goal of (Shiller's , ed.) paper is to demonstrate that first-degree PD is now feasible and may soon be widely employed, suggesting we need research on general equilibrium models assuming near-universal first-degree PD*».

167 *Ibid,* 2. Shiller, precisa: «*By increasing profits of firms with monopoly power, it increases the incentives to innovate and differentiate. Its use also changes the impacts of mergers in concentrated industries, and the impacts of privacy and data property rights laws. Such pricing may also cause consumers to waste effort masking themselves as low valuation consumers. Or, in an extreme, albeit unlikely scenario, consumers could reduce labor effort, knowing that earning higher wages would result in being charged higher prices. These are some of the effects that might occur if personalized pricing is widely used. And widely it might - Graddy shows another form of PD is used even in a seemingly perfectly competitive market*».

paghino il doppio di altri[168].

Tramite tale modello, Shiller ha potuto contemperare gli esiti di diversi modelli, isolando - date le innumerevoli fonti di dati - quali variabili sarebbero state significative nella regressione e giungendo ai risultati precedentemente illustrati[169].

Peraltro, affiancando al tema della discriminazione quello della posizione relativa degli agenti economici, mette conto ricordare che le informazioni usate per dar luogo ad una vendita in cui viene praticata una discriminazione di prezzo non sono di natura simmetrica (proprio come sostenuto in precedenza rispetto alla posizione del *data collector* rispetto all'utente). Il venditore è infatti in possesso di più informazioni sul compratore rispetto al contrario e, attraverso la pratica della profilazione, sovverte il potere di contrattazione svelando il prezzo di riserva del consumatore, senza rivelare il proprio[170].

Si potrebbe in proposito commentare con Helen Nissembaum[171]:

«*information is a more effective tool in the hands of the strong than in those of the weak*»[172].

Già nel 2004, Taylor[173] aveva intuito come, per le imprese, il valore generato dalle informazioni personali dei consumatori dipendesse dalla capacità dei detentori dei dati di inferirne le preferenze degli individui e derivarne - tramite pratiche di discriminazione di prezzo – prezzi "personalizzati" che il consumatore avrebbe rifiutato con difficoltà. Il fattore abilitante di tali strategie è evidentemente rappresentato dagli strumenti tecnologici a disposizione dei consumatori e delle imprese. Come sostiene Taylor, se il consumatore non riesce a difendersi rispetto al tentativo perpetrato dalle imprese di carpire quanti più dati personali disponibili, sarà allora possibile per queste estrarre il massimo del surplus del consumatore.

Su un ulteriore fronte, Taylor afferma inoltre che, se le informazioni riguardanti i con-

---

168 *Ibid.*, 1: «[…] (In his paper, Shiller estimated, ed.) *the profit gained from personalized pricing when nearly 5000 web-browsing variables are used to estimate individuals' reservation values for Netflix. Of course, this alone cannot prove a break from the past. So, as a comparison,* (Shiller computes, ed.) *the analogous profit gained from first-degree PD when only demographics, which have long been available, are used as explanatory variables.* […] *A new econometric method is introduced, Ordered-choice Model Averaging (OMA), blending economic modeling with advances in machine learning to estimate optimal prices and overcome problems from over-fitting and high dimensionality, essential issues for big data*».

169 *Ibid.*: «[…] *Web browsing data* […] *help predict which consumers subscribe to Netflix. Without any information, each individual's probability of subscribing is the same, about 16%. Including standard demographics, such as race, age, income, children, in a Probit model improves prediction modestly - individual predicted probabilities of subscribing range from 6% to 30%. Adding the full set of variables in the OMA method, including web* browsing histories and variables derived from them, substantially improves prediction - predicted probabilities range from close to zero to 99.8%.

[…] (Shiller finds out, ed.) *that web browsing behavior substantially raises the amount by which person-specific pricing increases profits relative to second-degree PD - 12.18% if using all data to tailor prices, but only 0.79% using demographics alone. Web browsing data hence make personalized pricing more appealing to firms and likely to be implemented, thus impacting consumers. Aggregate consumer surplus is estimated to fall by 8%. Substantial equity concerns arise - some consumers pay about double the price some others do for the same product*».

170 M. MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, in *I/S: A Journal of Law and Policy for the Information Society,* 6, 2010.

171 H.F. Nissenbaum, *Privacy in Context : Technology, Policy, and the Integrity of Social Life*, Stanford, 2010, 211.

172 *Ibid,* 210. L'autrice aggiunge che una "economia Orwelliana" è un'economia in cui: «*sellers charge different prices to different buyers. In this scenario, dynamic pricing responds to personal characteristics such as wealth (ability to pay), urgency of need, vulnerability to certain enticements, or marketing approaches*».

173 C.R. Taylor, C*onsumer Privacy and the Market for Customer Information,* cit, 631-650.

sumatori vengono rivendute a terzi, l'efficienza sociale può risultarne ridotta. Al contrario, nel 2001, Calzolari e Pavan[174] – nel tentativo di mostrare come lo scambio delle informazioni personali dei consumatori tra un'impresa ed un'altra possa invece ridurre le distorsioni informative caratterizzanti il mercato[175] – affermano che la trasmissione dei dati dei consumatori tra imprese non genera una diminuzione del surplus del consumatore, ma porti ad un miglioramento del benessere generale. Idea invece contestata da Taylor[176].

Sempre Taylor, nel 2004[177] afferma che, in relazione allo scambio tra imprese di informazioni relative ai consumatori, si verifica un duplice effetto in ordine a benefici e costi sociali ad esso associati. I primi risulteranno inferiori in ragione della diminuzione degli scambi e delle maggiori perdite secche connessi all'imposizione dei "prezzi dinamici": i consumatori che non saranno in grado di compiere valutazioni sofisticate decideranno infatti di non acquistare, mentre, al contrario, i consumatori in grado di compiere valutazioni più sofisticate, porranno in essere comportamenti strategici anticipando la vendita dei propri dati personali ed assumendo la decisione di non comprare quei beni i cui prezzi saranno reputati eccessivamente alti, causando, dunque, un danno al mercato dei dati personali[178]. Per quanto riguarda i costi sociali, essi saranno più alti a causa degli sforzi delle imprese nell'intento di raccogliere le informazioni private dei consumatori.

In tal senso, Taylor, anticipando quanto avrebbero poi sostenuto Acquisti e Varian nel 2005, afferma:

«[…] *Dynamic pricing is optimal for the monopolist when consumers are naive but not when they are sophisticated*».[179]

Guardando ora alla posizione dei consumatori in un contesto di sempre più generalizzato ricorso a pratiche discriminatorie di primo grado, occorre ricordare che, partendo dal presupposto che il benessere economico collettivo dipende dall'abilità dei consumatori di prevedere come possano essere impiegati i propri dati personali, Acquisti e Varian[180] sostengono che le tecnologie ("*anonymizing technologies*"[181]) oggi a disposizione degli individui permettano ai consumatori razionali di "alleggerire" le strategie di invasione della privacy messe in campo dalle imprese. In tale ottica, proprio al fine di

[174] Calzolari e Pavan supportano le ragioni della scuola di Chicago e di come al verificarsi di certe condizioni, il venditore potrebbe decidere di proteggere l'informazione del consumatore e che anche in assenza d un intervento normativo -il mercato tende a generare una distribuzione efficiente dei dati personali senza alcun intervento regolatorio.

[175] G. Calzolari - A. Pavan, *Optimal Design of Privacy Policies*, 2001.

[176] C.R. Taylor, *Consumer Privacy and the Market for Customer Information*, cit., 634: «*Calzolari and Pavan do not consider the possibility of naïve consumers. Also, most of their analysis is couched in the context of full commitment, where they consider the design of an abstract information transmission mechanism rather than explicit sale of a customer list. In essence, one can view Calzolari and Pavan as studying the question concerning the ex ante optimal design of an information-sharing agreement between two firms,* (ignoring, *ed.*) *the analysis* (of, *ed.*) *concerns* (about, *ed.*)*the ex post sale of customer information in the absence of any prior agreement*».

[177] *Ibid.*

[178] M. Peitz - J. Waldfogel, *The Oxford Handbook of the Digital Economy*, Oxford, 2013, 556.

[179] C.R. Taylor, *Consumer Privacy and the Market for Customer Information*, cit, 634.

[180] A. Acquisti - H.R. Varian, *op. cit.*

[181] *Ibid,* 368.

non rendere controproducente l'attività di *data collection,* i detentori dei dati dovrebbero adattarsi a tale realtà ed offrire servizi personalizzati agli individui[182].

Tuttavia, nonostante le contromisure approntabili da parte dei consumatori razionali, Taylor[183] dimostra però come le imprese mantengano un incentivo ad investire una quantità di risorse nelle attività di *data collection* superiore al livello socialmente ottimale. Per giunta, Shiller afferma come nemmeno i consumatori razionali delineati da Acquisiti e Varian, o Villas-Boas possano sottrarsi agli effetti della discriminazione di prezzo dovuta alla profilazione[184].

Inoltre, Hann, Hui, Lee, e Png[185], riprendendo la definizione di "*strategic complement*" elaborata da Bulow ed altri[186] nel 1985, hanno teorizzato che, in un mercato popolato da imprese che fanno uso di campagne pubblicitarie più o meno ortodosse e da diverse tipologie di consumatori, con una maggiore o minore avversione rispetto all'invasività del marketing, emergono due tendenze di segno opposto: da un lato si registra l'uso di tecnologie da parte dei consumatori, al fine di sfuggire alle campagne di marketing, dall'altro, un incremento degli sforzi delle imprese a porre in essere tecniche di marketing più "martellanti". I due elementi – l'atteggiamento ostile dei consumatori rispetto al marketing promosso dalle imprese e l'accresciuta necessità per le stesse di far breccia nelle preferenze degli individui – possono essere catalogati quali "complementi strategici", nel senso che all'inasprirsi dell'atteggiamento dei consumatori corrisponde la

---

182 A. Acquisti - H.R. Varian, *op. cit.* spec. 368, 371 e 376: «[...] *The seller can use customer information not only for price discrimination but also to offer enhanced, personalized services and by addressing a larger spectrum of responses by individual consumers that include both delaying purchases and adopting anonymizing technologies.* [...] *Sellers condition prices - if they can offer personalized enhanced services – (will worth, ed.)* […] *high-value and low-value consumers value differently.* […] *The seller can induce the necessary change in consumer valuations by offering various forms of personalized enhanced services to prior purchasers, such as personalized discount coupons (common in supermarket loyalty clubs), lowered transactions costs (such as one-click shopping), or personalized services (such as personalized recommendations).* […] *The assumption of personalization plays a critical role in our model because it rules out merely offering enhanced services (i.e., a more valuable product) to all consumers. By its nature, a personalized service can only be offered once the seller has information about a consumer who has purchased before.* [...] *In the real world, offers to "new customers only" can typically be utilized by "old customers" if they are willing to sacrifice other benefits that they get from being repeat customers. These benefits are exactly what drives our model: Customers are not willing to sacrifice their personalized enhanced services to get a lower price*»

183 C. R. Taylor, *Privacy and Information Acquisition in Competitive Market*, in *Berkeley Program in Law & Economics*, Working Paper, 2 gennaio 2004, 8.

184 B.R. Shiller et al., *First-Degree Price Discrimination Using Big Data*, cit., 4: «*Since consumers can avoid higher prices using one very simple heuristic: "don't buy at high prices", such pricing appears more of a flavor of second-degree price discrimination than it does personalized pricing in the spirit of first-degree price discrimination.*
By contrast, tailored pricing based on many unrelated variables is not subject to the same criticism. First, with bounded rationality consumers may not be able to avoid being charged high prices. I find, for example, that Netflix should charge lower prices to individuals that use the internet during the day on Tuesdays and Thursdays, and higher prices to those that visit Wikipedia.org, patterns consumers may not recognize. Moreover, with many variables, there likely are no simple heuristics consumers can follow to avoid being charged high prices. Furthermore, heuristics for one product may not apply to other products, so efforts to get a lower price on one product may result in a higher price for another. Even if consumers did understand which behaviors result in low prices, they might prefer to ignore them rather than change potentially thousands of behaviors just to receive a lower quoted price for one product. Finally, firms could charge high prices to any consumers not revealing their web browsing data, providing the incentive for consumers to reveal them»

185 I.-H. Hann et al., *Consumer Privacy and Marketing Avoidance*, 2005.

186 J.I. Bulow - J.D. Geanakoplos - P.D. Klemperer, *Multimarket Oligopoly: Strategic Substitutes and Complements*, in *Journal of Political Economy* 93, no. 3, 1985, 488-511 .

frequenza delle campagne pubblicitarie indesiderate[187-188].

Il fatto che le imprese continuino a mettere in atto tali pratiche nonostante siano stati illustrati meccanismi perversi come quello individuato da Hann, Hui, Lee e Png e, sebbene autori come Taylor[189], e Varian e Acquisti[190] abbiano mostrato che i consumatori razionali possono porre in essere meccanismi di difesa rispetto alle tecniche di profilazione (generando maggiori costi per le imprese), fa pensare che il valore dei dati acquisiti e dei benefici che possono derivarne - in termini di pratiche di discriminazione di prezzo più puntuali ovvero di una maggiore di capacità predittiva dei consumi futuri – siano maggiori rispetto ai costi. Si pensi, a mero titolo di esempio, alla fornitura di servizi gratuiti da parte di Google in cambio di informazioni.

Per tornare quindi sul fronte del consumatore, in tale contesto di estremo interesse all'acquisizione dei suoi dati personali da parte delle imprese, si rammenta che un consumatore che cede parte della propria privacy fronteggia un *trade-off* nelle seguenti condizioni:

«There is, indeed, evidence that consumers face known decision making hurdles when facing privacy trade-offs, such as (a) incomplete information, (b) bounded cognitive ability to process the available information, and (c) a number heuristics (or cognitive and behavioral biases) which lead to systematic deviations from theoretically rational decision making (sometimes, various combinations of these factors affect consumer decision making at the same time)».[191]

In questo contesto, le valutazioni degli individui sulla cessione o meno di porzioni della propria *information privacy* si fondano, da un lato, su informazioni incomplete riguardo l'uso che verrà fatto di loro dati personali, ma soprattutto, sull'incapacità di assegnare ai dati e alle informazioni personale il valore corrispondente. Un valore che l'individuo percepisce come residuale, ma che le imprese ben comprendono poiché, nell'era dei

---

187 K.-L. Hui - I. Png, *op. cit.*, 27: *«For instance, to avoid telemarketing solicitations, consumers can conceal (e.g., by registering with do-not-call lists) or deflect (e.g., by screening incoming telephone calls). Sellers cannot distinguish the consumer types ex ante. Ideally, they would promote only to high-type consumers. Instead, they incur costs to solicit the entire consumer population, and then discover consumer types ex post. Seller solicitations are a strategic complement* […] *with concealment by low-type consumers, i.e., if the cost of concealment measures were to fall, low-type consumers would increase concealment, and sellers would increase marketing.* […] *However, from a welfare perspective, consumer concealment is less favorable then deflection, because it concentrates the seller solicitations on a smaller number of consumers. A consumer needs only one solicitation to enjoy the product, and additional solicitations simply add to harm. Accordingly, concentrating the solicitations raises the expected harm relatively more than the benefit».*

188 I.-H. Hann et al., *op. cit.,* 21 ss: «*seller marketing is a strategic complement with consumer concealment. Hence, consumer measures to conceal themselves from marketing will increase its cost-effectiveness and lead sellers to market more* […] *: consumer efforts to conceal themselves and to deflect solicitations have a crucial impact on sellers' marketing strategy. Under reasonable conditions, seller marketing is a strategic complement with consumer concealment. So, policies that encourage consumers to conceal their identities would lead sellers to increase marketing. By contrast, policies that encourage consumers to deflect seller marketing would lead sellers to reduce marketing. There is a clear need for public policy. The free market does not work well. To the extent of the externality from the sellers to consumers, the equilibrium levels of marketing (chosen by sellers) and concealment and deflection (chosen by consumers) exceed the social optimum. Further, if the harm caused by marketing is higher, consumers would increase both concealment and deflection, and sellers respond by increasing their marketing».*

189 C.R. Taylor, *Privacy and Information Acquisition in Competitive Markets*, cit.

190 Si vedano sezioni 3.2.3, 4, 4.2.3 e 5 di: A. Acquisti - H.R. Varian, *op. cit.*

191 A. Acquisti, *From the Economics of Privacy to the Economics of Big Data*, in S. Bender, J. Lane, H. Nissenbaum, V. Stodden, *Privacy, Big Data, and the Public Good: Frameworks for Engagement,* 76, Cambridge, 2014, 17-18: www.repository.cmu.edu/heinzworks/339.

Big Data, le informazioni sui consumatori sono di vitale importanza affinché le stesse rimangano competitive nel perimetro di una triplice strategia che permetta di indirizzare annunci mirati, dia luogo alla personalizzazione dei prodotti e possa proporre "prezzi su misura" (*tailored prices*[192]).

[192] *Ibid.*

Sharing economy: l'esperienza italiana della XVII legislatura alla luce degli orientamenti europei*

Guido d'Ippolito

Abstract:

L'articolo esamina due proposte in materia di *sharing economy* presentante al Parlamento italiano nel corso della XVII legislatura. Premessa una ricostruzione generale in materia di *sharing economy*, con particolare riferimento al ruolo delle piattaforme digitali, si passerà all'esame delle proposte di legge nn. 3564 alla Camera dei Deputati e 2268 al Senato della Repubblica. Al fine di permettere un'analisi più approfondita, utile per divenire la base di nuove riflessioni e ulteriori proposte di legge nel corso della XVIII legislatura, le due proposte italiane sono esaminate anche alla luce dei criteri individuati nel 2016 dalla Comunicazione della Commissione europea su: «*Un'agenda europea per l'economia collaborativa*».

The article examines the new economic system known as sharing economy, particularly referring to two Italian bills pending during the 17th legislature: nn. 3564 at the Camera dei Deputati and 2268 at the Senato della Repubblica. Starting from the role of the digital platforms, the two bills are analysed comparing them to the guidance expressed in 2016 by the European Commission in to the Communication on "A European agenda for the collaborative economy".

Sommario

1. Introduzione - 1.1. La comunicazione della Commissione europea e i soggetti della *sharing economy* - 1.2. La necessità di un intervento normativo - 2. I soggetti della *sharing economy* - 3. Le piattaforme digitali - 3.1. La ricerca di un *level playing field* - 3.2. La responsabilità degli intermediari - 4. L'esperienza italiana - 4.1. La proposta alla Camera dei Deputati - 4.1.1. Regime autorizzatorio e "documento di politica aziendale" - 4.1.2. Fiscalità e protezione dei dati personali - 4.1.3. Incentivi alla *sharing economy* - 4.2. La proposta al Senato della Repubblica - 4.2.1. Regime autorizzatorio e condizioni contrattuali - 4.2.2. Tutele in materia alimentare, trattamento fiscale e misure di incentivo - 5. Un'agenda europea per l'economia collaborativa - 5.1. Autorizzazioni e licenze - 5.2. Prestatori di servizi professionali, non professionali e responsabilità delle piattaforme - 5.3. Applicazione delle normative a tutela di consumatori e utenti - 5.4. Rapporto di lavoro e fiscalità - 6. Conclusioni

Keywords: Sharing economy, Economia collaborativa, Digital platforms, Parlamento italiano, Commissione UE

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

1. Introduzione

Tra le sfide più complesse e innovative che il diritto dei giorni nostri è chiamato ad affrontare vi è senza dubbio quella della c.d. *sharing economy*, anche tradotta come "economia collaborativa"[1].

In senso generale il concetto di *sharing economy* fa riferimento a un «nuovo modello economico e culturale […] basato sull'utilizzo e sullo scambio di beni e servizi piuttosto che sul loro acquisto»[2]. Elemento centrale è quindi la condivisione di un bene o un servizio, messo a disposizione di una moltitudine di soggetti, spostando quindi l'attenzione dall'istituto della proprietà a quello dell'accesso[3].

A partire da tale nucleo centrale, questo nuovo modello economico si è esteso facendo del termine *sharing economy* un'etichetta generale (*umbrella term*) riassuntiva di più fenomeni coinvolgenti attività di scambio di beni e servizi in senso ampio. In questo modo, l'espressione *sharing economy* può essere usata per far riferimento ai «modelli imprenditoriali in cui le attività sono facilitate da piattaforme di collaborazione che creano un mercato aperto di beni o servizi spesso forniti da privati»[4].

Dunque, solo la condivisione, come anche lo scambio o la cessione di beni, non sembrerebbe attività sufficiente per poter parlare di *sharing economy* o, quanto meno, non sembrerebbe un'attività a tal punto nuova o significativa da modificare in modo evidente le dinamiche sociali e attirare così l'attenzione dei giuristi. L'ulteriore elemento di cui si ha bisogno per passare dalla semplice messa a disposizione di un bene – che sia a titolo oneroso o gratuito, con un contratto di permuta piuttosto che di vendita o altro

[1] Sebbene le due terminologie siano qui usate indifferentemente, è opportuno ricordare che tali termini non sono esattamente sovrapponibili. Col termine "economia collaborativa" si intende infatti «un sistema economico di reti e mercati decentralizzati che libera e abilita il valore di risorse sottoutilizzate creando una corrispondenza tra chi dispone e chi ha bisogno delle risorse senza ricorrere ad intermediari tradizionali». Diversamente, il concetto di *sharing economy* è più ampio individuando «un sistema economico basato sulla condivisione di beni o servizi sottoutilizzati, gratuitamente o a pagamento, effettuato direttamente dai singoli». Si veda a tal riguardo: N. Rampazzo, *Rifkin e Uber. Dall'età dell'accesso all'economia dell'eccesso*, in *Il diritto dell'informazione e dell'Informatica*, 6, 2015, 957 ss.

[2] Proposta di legge, atto Camera n. 3564, *Disciplina delle piattaforme digitali per la condivisione di beni e servizi e disposizioni per la promozione dell'economia della condivisione*, presentata il 27 gennaio 2016 e disponibile al seguente link: www.camera.it/leg17/126?idDocumento=3564

[3] «Appare fortemente in crisi, come buona parte degli istituti giuridici statici e meno flessibili all'innovazione anche concettuale, il paradigma proprietario esclusivo ed assoluto, insidiato dal prepotente affermarsi dell'utilità diffusa del bene, dell'economia orizzontale e dematerializzata della condivisione o "à la demande", della (talvolta fittizia) disintermediazione, della semplificazione di processi preesistenti (autentico motivo di successo), del consumo collaborativo e delle disruptive technologies»: così N. Rampazzo, *op. cit.*, 957 ss. Si assiste qui a un altro aspetto del passaggio dall'era della proprietà all'era dell'accesso, sulla cui tematica si rinvia a J. Rifkin, *The age of access: The new culture of hypercapitalism, Where all of life is a paid-for experience*, New York, 2000; S. Rodotà, *Il diritto di avere diritti*, Bari, 2013, 105 ss.

[4] Comunicazione della Commissione al Parlamento Europeo al Consiglio al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Un'agenda europea per l'economia collaborativa*, 2 giugno 2016, COM(2016) 356 final, 3, reperibile al link: www.ec.europa.eu/transparency/regdoc/rep/1/2016/IT/1-2016-356-IT-F1-1.PDF

schema contrattuale[5] – alla nuova "economia della condivisione" o "collaborativa"[6] è infatti l'utilizzo di Internet[7] in generale e delle piattaforme digitali in particolare.
Internet – e la realtà interattiva che si è creata dal c.d. Web 2.0 in poi insieme al fenomeno della disintermediazione – è dunque quel fattore abilitante di nuove forme di interazione sociale, rapporti o scambi economici[8]. Più nello specifico, il sempre più ampio utilizzo delle piattaforme digitali o *social* abilita una condivisione che, riprendendo la terminologia propria dei sistemi c.d. *peer to peer (P2P)*, avviene tra "pari" (*peer*), ossia tra soggetti privati posti su uno stesso piano. Questo ha ovvie ripercussioni sulla disciplina consumeristica, basata sulla presenza di un soggetto professionista e uno consumatore posti su piani diversi, e fa emergere la figura di un nuovo soggetto, intermedio tra i due: il c.d. *prosumer*[9].
È quindi la presenza delle cc.dd. piattaforme digitali ad essere quel *quid pluris* che crea un fenomeno *disruptive* sia dal punto di vista economico che giuridico e, quindi, sociale. Infine, è importante osservare come tale sistema economico si innesti sulle nuove dinamiche sociali create da Internet e, in particolare, fa proprio un meccanismo di concorrenza basato sulla *business reputation*. In altre parole, la reputazione digitale dei soggetti coinvolti nella *sharing economy*, attraverso il meccanismo dei *feedback*, acquisisce un suo valore economico che contribuisce alle diffusione delle informazioni[10].

1.1. La comunicazione della Commissione europea e i soggetti della *sharing economy*

Rilevante in materia è la Comunicazione della Commissione al Parlamento Europeo al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni su

[5] Per un approfondimento su tali aspetti si veda D. Di Sabato, *La prassi contrattuale nella sharing economy*, in *Rivista di diritto dell'impresa*, 3, 2016, 451 ss.

[6] L'economia collaborativa può essere definita in diverso modo, anche al fine di focalizzare l'attenzione su un elemento piuttosto che un altro. Avremo così la *peer economy* in senso stretto, che sottolinea come lo scambio o la condivisione avviene tra soggetti privati posti sullo stesso piano e non più tra un soggetto professionista e un consumatore tra i quali sussiste una asimmetria informativa, oppure ancora una *collaborative economy*, *collaborative consumption*. A. Quarta, *Il diritto dei consumatori ai tempi della peer economy. Prestatori di servizi e prosumers: primi spunti*, in *Europa e Diritto Privato*, 2, 1 giugno 2017, 667 ss.

[7] In generale, sul rapporto tra Internet e diritto si vedano, da ultimo: T. E. Frosini, *Internet e democrazia*, in *Il diritto dell'informazione e dell'informatica*, Milano, anno XXXII, 4-5, 2017, 657 ss.; O. Pollicino – T. E. Frosini – E. Apa – M. Bassini (*a cura di*), *Diritti e libertà in internet*, Milano, 2017; F. Faini – S. Pietropaoli, *Scienza giuridica e tecnologie informatiche*, Torino, 2017.

[8] Secondo lo studio svolto dalla Fondazione Nesta l'economia collaborativa può essere intesa come un modello di produzione, scambio e consumo tramite la rete Internet «*to connect distributed groups of people to make better use of goods, skills and other useful things*». Così K. Stokes - E. Clarence - L. Anderson - A. Rinne, *Making Sense of the UK Collaborative Economy*, 2014, disponibile al sito: www.nesta.org.uk/publications/making-sense-uk-collaborative-economy

[9] A. Quarta, *op. cit.*, 667 ss.

[10] N. Rampazzo, *op. cit.,* 957 ss.; Con specifico riferimento al settore del diritto d'autore on line e i cc.dd. *User Generated Content*, sia consentito rinviare a G. d'Ippolito, *L'esigenza di un nuovo bilanciamento per il diritto d'autore: gli user generated content e l'ipotesi di un'eccezione per le opere creative e trasformative*, in *Ciberspazio e diritto*, 3, 2017, 513 ss.

Un'agenda europea per l'economia collaborativa del 2 giugno 2016[11].
All'interno di questo documento, che si preoccupa di delineare i contorni di quei modelli imprenditoriali «in cui le attività sono facilitate da piattaforme di collaborazione che creano un mercato aperto per l'uso temporaneo di beni o servizi spesso forniti da privati»[12], si identificano i soggetti protagonisti della *sharing economy*, ossia: i) i prestatori di servizi, solitamente soggetti privati che condividono beni, risorse, tempo e/o competenze ma anche soggetti professionali (e quindi «*prestatori di servizi professionali*») che si avvalgono della piattaforma per massimizzare la loro attività; ii) gli utenti, che ponendosi come polo alternativo nel rapporto con i prestatori usufruiscono dei beni e servizi da questi messi a disposizione; iii) infine, tra queste due prime categorie vi sono i nuovi soggetti "intermediari", ossia le piattaforme *on line* che mettono in comunicazione prestatori e utenti e che agevolano le transazioni tra di essi e, per questo, definite anche «piattaforme di collaborazione».
Questo nuovo modello economico, che riscopre il ruolo degli scambi tra pari tramite le piattaforme digitali, si impone sempre più come centrale nelle attuali dinamiche sociali ed è rinvenibile in modo trasversale in molti settori produttivi: dall'acquisto *on line* di beni ceduti dai privati tramite piattaforme come Subito.it ai numerosi servizi di trasporto basato sulla condivisione di un'auto o una bicicletta (si pensi a servizi ormai noti come Uber, Car2Go, Enjoy, Obike, FlixBus solo per citare i più famosi), fino a nuove forme di consegna del cibo a domicilio (Foodora, Deliveroo o JustEat) o di condivisione di luoghi di cucina come per gli *home resturants* e molto altro ancora.
In particolare, la Comunicazione della Commissione europea individua cinque settori in cui l'economia collaborativa risulta più rilevante: quello degli alloggi o, meglio, delle locazioni a breve termine (si pensi a servizi come Booking o Airbnb o in generale a servizi di c.d. *CouchSurfing*); quello del trasporto di persone; dei servizi tecnici; professionali (per esempio Patreon); e di finanza collaborativa (famosi sono Kickstarter o Indiegogo)[13].

1.2. La necessità di un intervento normativo

Definito il fenomeno, resta da chiarire sotto quali profili l'economia collaborativa sembrerebbe bisognosa di un intervento di tipo normativo.
In primo luogo, nel caso in cui gli scambi attraverso piattaforme digitali siano posti in essere tra "pari", ossia tra soggetti privati al di fuori della loro attività professionale, risulterebbe inapplicabile la disciplina consumeristica con le sue garanzie e tutele nei

[11] Comunicazione della Commissione al Parlamento Europeo al Consiglio al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Un'agenda europea per l'economia collaborativa*, 2 giugno2016, COM(2016) 356 final, reperibile al link: www.ec.europa.eu/transparency/regdoc/rep/1/2016/IT/1-2016-356-IT-F1-1.PDF

[12] *Ibid.*, 3: «l'espressione "economia collaborativa" si riferisce ai modelli imprenditoriali in cui le attività sono facilitate da piattaforme di collaborazione che creano un mercato aperto per l'uso temporaneo di beni o servizi spesso forniti da privati».

[13] *Ibid.*, 2.

confronti del consumatore quale soggetto debole del rapporto[14].

Ciònonostante anche nel caso in cui gli scambi avvengano tra un soggetto professionale e uno non professionale, non è sempre agevole applicare le tutele relative alla leale concorrenza, la trasparenza e neutralità dei servizi offerti, alle norme in materia di lavoro, fisco, tutela della salute in ambito alimentare e così via. La sfida diventa quindi identificare le caratteristiche e i contorni delle relazioni e attività veicolate dalle piattaforme digitali al fine di sussumerle in una certa normativa. Cosa, questa, non sempre agevole.

Da tali criticità emergerebbe dunque l'esigenza di un intervento di tipo regolatore dei nuovi fenomeni economici e sociali. Esigenza resa sempre più pressante dall'aumentare delle dimensioni e del volume di affari nonché dalla velocità con cui cambiano le tecnologie e si evolvono i servizi.

Nonostante i benefici apportati dalla *sharing economy* quale nuovo modello economico, in assenza di regole chiare e capaci di intercettare le nuove dinamiche sociali si rischierebbe di avallare sempre più usi scorretti o distorti delle piattaforme digitali, creando criticità che vanno dall'alterazione della concorrenza all'eliminazione di tutele e rimedi fino alla generale e progressiva riduzione della fiducia verso tali sistemi.

Esempi di ciò possono essere fenomeni come le recensioni finte dei ristoranti su TripAdvisor[15], la cancellazione delle recensioni negative su strutture alberghiere[16], gli scontri e le proteste dei tassisti nei confronti di Uber[17], il mancato rispetto delle normative sulla conservazione dei cibi da parte degli *home restaurant*, la difficoltà nel qualificare chi lavora in tali ambiti come lavoratore subordinato o il mancato pagamento delle tasse nel paese dove i servizi vengono scambiati.

---

[14] *Ibid*, 2: «l'economia collaborativa spesso solleva questioni relative all'applicazione del quadro normativo vigente, dal momento che rende meno nette le distinzioni tra consumatore e prestatore di servizi, lavoratore subordinato e autonomo, o la prestazione di servizi a titolo professionale e non professionale». A. Quarta, *op. cit*., 667 ss.

[15] Paradigmatico è il caso di *The Shed At Dulwich*, un finto ristorante creato con lo scopo di dimostrare che anche un'attività inesistente, con un sapiente uso dei media e di recensioni false, potesse diventare il primo ristorante di Londra su TripAdvisor. La vicenda è raccontata su: Oobah Butler, *I Made My Shed the Top-Rated Restaurant on TripAdvisor*, in *Vice*, Dec. 6th, 2017: www.vice.com/en_us/article/434gqw/i-made-my-shed-the-top-rated-restaurant-on-tripadvisor

[16] Si veda il caso di Kristie Love che, dopo essere stata vittima di violenza sessuale ad opera di un dipendente della struttura alberghiera presso cui soggiornava, ha visto sistematicamente rimosse le recensioni su TripAdvisor con cui avvisava e denunciava quanto da lei subito: Matthew Haagnov, *TripAdvisor Apologizes for Deleting Review Detailing Rape at Mexican Resort*, in *The New York Times*, Nov. 2nd, 2017: www.nytimes.com/2017/11/02/travel/trip-advisor-rape-mexico.html

[17] Grande seguito ha avuto, anche in Italia, la vicenda degli scontri tra i tassisti e Uber, azienda fornitrice di servizi di trasporto automobilistico privato attraverso un'applicazione mobile, che ha visto anche diversi interventi della magistratura. Tra i tanti contributi in materia, si segnala la rivista Medialaws, n. 1/2018, che dedica all'argomento un focus con i contributi di: V. Zeno-Zencovich, *Uber: Modello economico e implicazioni giuridiche*, 140-143; L. Belviso, *Il caso Uber negli Stati Uniti e in Europa fra mercato, tecnologia e diritto. Obsolescenza regolatoria e ruolo delle Corti*, 144-160; N. Canzian, *Il legislatore tentennante sul servizio di noleggio con conducente: l'incertezza ricostruttiva fra reviviscenza e assenza di una disciplina positiva*, 161-175; M. Colangelo – M. Maggiolino, *Uber and the challenges for antitrust law and regulation*, 176-187; E. Marasà – O. Pollicino, *EU Court of Justice rules that Uber provides a transport service and is not a mere electronic intermediary: regulatory implications and "digital" judicial insulation,* 189-194; F. Becchis – S. Valerio, *Il servizio di Uber tra asset dormienti e valore digitale. Quale regolazione?*, 195-200, disponibili al link: www.medialaws.eu/rivista_category/1-2018/ N. Rampazzo, *op. cit*., 957 ss.

Ecco perché, in sintesi, l'intervento del diritto è da più parti invocato, pur non essendo ancora chiara o univoca la strada da percorrere.

2. I soggetti della *sharing economy*

La Comunicazione della Commissione europea qualifica quelli che sono i protagonisti della *sharing economy*: i prestatori dei servizi, gli utenti di tali servizi e gli intermediari ossia le piattaforme di collaborazione.

Tra questi tre soggetti si creano relazioni che possono portare a risultati diversi in termini di disciplina giuridica applicabile. A tal fine si possono distinguere tre diverse tipologie di interazioni[18].

Un primo tipo di relazione è quella che individua e accomuna i rapporti riconducibili al modello *business to consumer* (B2C), ossia quelli in cui avverso un soggetto professionista si colloca un soggetto consumatore e che permette quindi l'applicazione della normativa contenuta nel codice del consumo. Rientrano in questa categoria le relazioni tra: i) piattaforma e utente; ii) piattaforma e prestatore di servizi non professionale; iii) prestatore di servizi professionale e utente.

In tale categoria è inoltre importante sottolineare che i rapporti che coinvolgono la piattaforma digitale, oltre che dalla normativa consumeristica laddove applicabile[19], sono regolati dalle condizioni contenute all'interno di contratti stabiliti dalle stesse piattaforme ossia nei *Terms and Conditions*.

La seconda categoria è quella che coinvolge le relazioni tra soggetti professionisti, dunque il modello c.d. *business to business* (B2B), in cui le parti sono entrambe soggetti che agiscono con un'attività imprenditoriale e un fine di lucro ma ciò comunque non esclude la possibilità di squilibri nei reciproci rapporti di forza. Abbiamo qui il rapporto tra la piattaforma e il prestatore di servizi professionale.

Infine, l'ultima categoria riguarda le relazioni tra "pari", quelle tipiche della *sharing economy* in senso stretto (ossia della *peer economy*) e che coinvolge i rapporti tra prestatore di servizi non professionale e utente. Tale categoria, essendo riconducibile al modello c.d. *consumer to consumer* (C2C), vede l'inapplicabilità della disciplina consumeristica e si espone al rischio di zone d'ombra o lacune che non sembrerebbero garantire adeguata tutela dei soggetti coinvolti[20].

A questi tre soggetti principali – prestatore di servizi, piattaforma e utente – se ne può aggiungere un ulteriore. Questo può essere considerato come uno dei principali pro-

[18] Tale classificazione è opera di A. Quarta, *op. cit.*, 667 ss.

[19] A quest'ultimo devono essere applicate le regole del d.lgs. 206/2005 in tutte le ipotesi in cui l'utente della piattaforma possa essere considerato un consumatore.

[20] A. Quarta, *op. cit.*, 667 ss: «All'interno di questo gruppo, occorre poi distinguere tra scambi a titolo oneroso, in cui la condivisione di beni e servizi prevede il pagamento di un prezzo, da quelli a titolo gratuito o caratterizzati dalla ripartizione dei costi dell'attività condivisa tra le parti. La distinzione tra questi due tipi di scambio cooperativo (a titolo oneroso; a titolo gratuito o con divisione dei costi) è un esercizio di particolare importanza: nel primo caso, infatti, è più facile rilevare che le parti abbiano concluso un contratto tipico, mentre nel secondo l'interprete si confronta con una "zona grigia", compresa tra il polo delle prestazioni di cortesia e quello dei contratti atipici gratuiti»; D. Di Sabato, *op. cit.*, 451-490.

dotti della *sharing economy* e, prima ancora, dell'interattività resa possibile da Internet e dal venir meno della necessità di ricorrere ad intermediari.
Il consumatore finale, infatti, non è più soltanto un mero fruitore di beni e servizi, un soggetto passivo di fronte a un soggetto attivo. Sempre più spesso e in sempre più ambiti[21] il consumatore, o l'utente in senso ampio, diventa a sua volta produttore di ulteriori contenuti, informazioni, beni o servizi che mette a disposizione on line. Si parla, a tal riguardo, dei c.d. *User Generated Content*, ossia di contenuti prodotti dall'utente[22]. In questo modo lo stesso utente diventa a sua volta punto di partenza di un ulteriore ciclo di scambi.
Si ha così la figura del c.d. *prosumer*, un soggetto a metà strada tra il consumatore e il professionista, ossia quel consumatore che è anche produttore di beni e servizi. Si tratta quindi di un "ibrido" che, ancorché possa creare problemi di inquadramento giuridico, risulta idoneo «a rappresentare la dinamicità che caratterizza il rapporto tra le parti e la loro posizione sul mercato»[23].
Quella della disciplina giuridica del *prosumer* è una tra le sfide che l'economia collaborativa pone al diritto.

3. Le piattaforme digitali

Tra i tre soggetti costitutivi della *sharing economy*, la piattaforma digitale[24] svolge un ruolo di abilitatore degli scambi e delle relazioni tra i soggetti coinvolti.
Secondo l'indagine conoscitiva svolta nel 2016 dall'Autorità per le Garanzie nelle Comunicazioni, le piattaforme digitali sono l'infrastruttura tecnologica tramite le quali soggetti come gli OTT costruiscono i loro servizi. Tra questi i c.d. *consumer communications services*, inizialmente sviluppati per *personal computer* e poi gradualmente adattate all'utilizzo da *device* mobili, ossia le c.d. "app di comunicazione sociale"[25].
Le piattaforme fungono così da canale distributivo di servizi e da raccordo tra i sogget-

[21] G. Finocchiaro, *L'equilibrio titolare/users nel diritto d'autore dell'unione europea*, in *Il Diritto dell'Informazione e dell'Informatica*, 3, 2016, 499 ss.; M. Scialdone, *Il nuovo ruolo degli utenti nella generazione di contenuti creativi*, in *Diritto Mercato Tecnologia*, 4, 2013, 8-19.

[22] G. d'Ippolito, *op. cit.*, 513-571.

[23] A. Quarta, *op. cit.*, 667 ss.

[24] Piattaforma digitale, locuz. sost. f.: «Infrastruttura hardware o software che fornisce servizi e strumenti tecnologici, programmi e applicazioni, per la distribuzione, il *management* e la creazione di contenuti e servizi digitali gratuiti o a pagamento, anche attraverso l'integrazione di più media (*integrated digital platform*). Attraverso le p. m. è possibile costituire ambienti di apprendimento virtuali, sistemi di formazione in *e-learning*, ambienti di lavoro, *management*, ricerca, monitoraggio, nonché *repository* di esperienze e servizi organizzati su più livelli di accesso, per tipologia di utente. La p. d. può essere *open source* o commerciale e può essere strutturata per un pubblico accesso o per un target circoscritto, previa registrazione. Essa può prevedere servizi informativi, interattivi, di *file sharing*, *downloading* e *uploading*, *streaming* nonché di comunicazione e condivisione di materiale multimediale». Enciclopedia Treccani: www.treccani.it/enciclopedia/piattaforma-digitale_%28Lessico-del-XXI-Secolo%29/

[25] Agcom, *Indagine conoscitiva concernente lo sviluppo delle piattaforme digitali e dei servizi di comunicazione elettronica. I consumer communications services*, maggio 2016, Allegato A alla delibera n. 165/16/CONS, p. 4, disponibile sul sito dell'Autorità al seguente link: www.agcom.it/documents/10179/5054337/Allegato+29-6-2016/9d7168c6-6205-47e7-a2d9-23cccdc1df59?version=1.0

ti convolti dall'economia collaborativa coordinando le interazioni tra due o più gruppi distinti, ma interdipendenti, di soggetti[26]. Esse si caratterizzano per essere un esempio tipico della teoria economica delle "piattaforme multi-versante" o *multi-sided market*, ossia piattaforme che: «*create value by bringing two or more different types of economic agents together and facilitating interactions between them that make all agents better off*»[27].

Queste piattaforme si caratterizzano per l'essere sviluppate secondo una logica triangolare che coinvolge almeno tre parti: lo sviluppatore di applicazioni, il consumatore finale, entrambi affiliati a una piattaforma che li mette in comunicazione e ne gestisce le interazioni[28]. Si pensi, come esempio paradigmatico, al funzionamento dei vari *app store*[29].

Tre figure, queste, perfettamente sovrapponibili a quelle tipiche dell'economia collaborativa: il prestatore di servizi, l'utente, entrambi messi in contatto dalla piattaforma di collaborazione.

La mediazione della piattaforma produce esternalità di rete dirette dal lato degli utenti, ossia economie di scala dal lato della domanda. Ma produce anche esternalità di rete indirette dovute all'incremento di valore della piattaforma per i prestatori con l'aumentare degli utenti che la utilizzano[30].

3.1. La ricerca di un *level playing field*

Dal punto di vista normativo, l'attività delle piattaforme digitali[31] sfrutta un quadro giuridico lacunoso dovuto essenzialmente al non essere considerati nell'ambito della definizione di *electronic communication services*.

Tali soggetti sono infatti considerati come operatori c.d. *over the top*, e definiti quindi come fornitori di «*content, a service or an application that is provided to the end user over the open Internet*»[32]. Diversamente, il codice delle comunicazioni elettroniche definisce gli *electronic communications service* come servizi forniti di norma a pagamento, basati sulla responsabilità e controllo dell'operatore sul trasporto del segnale (*convenyance of signal*), a esclusione dei serizi che forniscono contenuti trasmessi utilizzando reti e servizi di

[26] La piattaforma digitale, dunque, «mette in contatto insiemi di utenti fra loro eterogenei, facilitando l'incontro, il collegamento, la realizzazione delle transazioni e delle diverse interazioni tra i medesimi». Così Agcom, *op. cit.*, 37.

[27] *Ibid.*, 37.

[28] *Ibid.,* 37.

[29] Rilevante a tal riguardo è la tematica della c.d. *device neutrality*, oggetto nel corso della XVII Legislatura di un apposito disegno di legge, l'Atto Camera n. 2520, *Disposizioni in materia di fornitura dei servizi della rete internet per la tutela della concorrenza e della libertà di accesso degli utenti*, consultabile al link: www.camera.it/leg17/126?pdl=2520

[30] Agcom, *op. cit.*, 37.

[31] Per una ricognizione sulla normativa italiana in materia di piattaforme digitali si veda: G. Resta, *Digital platforms and the law: contested issues*, in *Medialaws. Rivista di diritto dei media*, 1, 2018, 231 ss.

[32] Berec, *Report on OTT services*, gennaio 2016, 14.

comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti[33].
Quindi, la definizione di OTT non si riferisce a un particolare tipo di servizio ma alla modalità di somministrazione del medesimo, che utilizza la rete e il protocollo IP quale tecnologia di diffusione presso il grande pubblico, indipendentemente dal controllo dell'operatore di rete[34].
In altri termini[35]:
le *telco* tradizionali sono società che forniscono servizi trasmessi tramite l'utilizzo delle proprie infrastrutture di rete o dietro il pagamento di un prezzo per l'utilizzo di infrastrutture di proprietà di soggetti terzi; gli operatori tradizionali, pertanto, erogano *servizi managed*, poiché hanno il controllo sostanziale sull'accesso alla rete fissa o mobile.
Gli OTT, dal canto loro, non dispongono di proprie infrastrutture fisse o mobili, ma si avvalgono della rete Internet e, quindi delle infrastrutture di altri, al fine di fornire servizi online di comunicazione sociale.

3.2. La responsabilità degli intermediari

Le piattaforme digitali, in quanto intermediari, potrebbero rientrare nel regime di responsabilità prevista dagli artt. 12 e ss. della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (c.d. direttiva sul commercio elettronico).
Tali articoli fanno specifico riferimento alla responsabilità degli *Internet service provider (ISP)*[36] ossia dei soggetti che forniscono servizi di connessione, trasmissione, memorizzazione dati, anche attraverso la messa a disposizione delle proprie apparecchiature

[33] Agcom, *op. cit.*, 24 e 27; Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services: «*Electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks*»

[34] «D'altro canto, occorre sottolineare come gli operatori OTT/fornitori di servizi di comunicazione sociale in numerosi casi non dispongono di una infrastruttura di rete preesistente: pertanto, questi utilizzano in via di fatto e in modalità gratuita la rete degli operatori tradizionali al fine di trasmettere i propri servizi tramite protocollo IP», così Agcom, *op. cit.*, 24 ss.

[35] *Ibid.*, 25 e 26

[36] Sul regime di responsabilità degli *Internet Service provider* si rinvia a: R. Petruso, *Responsabilità degli intermediari di Internet e nuovi obblighi di conformazione: robo-takedown, policy of termination, notice and take steps*, in *Europa e Diritto Privato*, 2, 1 giugno 2017, 451 ss.; M. Montanari, *La responsabilità delle piattaforme on-line (il caso Rosanna Cantone)*, in *Il Diritto dell'Informazione e dell'Informatica*, 2, 2017, 254 ss. L. Bugiolacchi, *I presupposti dell'obbligo di rimozione dei contenuti da parte dell'hosting provider tra interpretazione giurisprudenziale e dettato normativo*, in *Responsabilità Civile e Previdenza*, 2, 2017, 536 ss.

per ospitare i siti[37].

Tale disciplina potrebbe quindi essere applicata alle piattaforme digitali nella misura in cui le queste si comportino da intermediari, abilitando le relazioni tra due o più soggetti. Interpretazione questa che, come si vedrà nel prosieguo, è fatta propria dalla Commissione europea.

Si potrebbe quindi sostenere come tali piattaforme possano essere considerati soggetti offerenti servizi di c.d. *hosting* con riferimento alla memorizzazione dei dati dei clienti e la messa a disposizione di uno spazio in cui gli utenti incontrano i prestatori dei servizi sottostanti[38]. In tal senso, le note piattaforme digitali potrebbero essere considerate, in linea di massima, *species* del *genus* dell'*hosting provider*, a sua volta rientrante nella famiglia degli *Internet service provider*, nei limiti in cui tali attività siano svolte in modo esclusivamente automatico e passivo[39].

Tanto più ciò laddove non si esclude comunque la possibilità per le piattaforme di offrire servizi ulteriori passando dallo svolgere un ruolo passivo, di mera intermediazione, a uno attivo, divenendo così oltre che degli *host provider* anche dei *content provider, service provider, cache provider*, fermo restano che alcune di loro possano fornire anche il servizio principale di accesso (c.d. *access provider*).

Dunque, se è vero che qualsiasi servizio offerto in Internet passa inevitabilmente attraverso l'intermediazione di un *provider* che fa transitare i dati sui suoi *server*[40], non sembrerebbe potersi escludere che le modalità di funzionamento delle piattaforme digitali e il loro ruolo di intermediario possano rientrare nella *ratio* propria del regime di responsabilità degli ISP di cui alla direttiva n. 2000/31/Ce.

Applicando questo regime a piattaforme come TripAdvisor, Amazon o Blablacar si giungerebbe alla conclusione che queste non saranno responsabili dei contenuti veicolati sulle loro piattaforme a condizione che non intervengano in alcun modo sui contenuti, non li modifichino o li rendano più o meno accessibili.

---

[37] M. Mensi – P. Falletta, *Il diritto del web. Casi e materiali*, Padova, 2015, 142: «L'ISP è, quindi, essenzialmente un intermediario, che stabilisce un collegamento tra chi intende comunicare un'informazione e i destinatari della stessa». Su tali temi, specie in rapporto al ruolo dei *social network*, si veda, da ultimo: M. R. Allegri, *Ubi social, ibi ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, Milano, 2018, pubblicato in *open access* e liberamente scaricabile al link: www.ojs.francoangeli.it/_omp/index.php/oa/catalog/book/298

[38] «Nel contesto dell'economia collaborativa, l'attività di *hosting* può essere intesa in generale come un'attività riguardante la memorizzazione dei dati dei clienti e la messa a disposizione di uno spazio in cui gli utenti incontrano i prestatori dei servizi sottostanti. Le deroghe di cui agli articoli 12 e 13 della direttiva sul commercio elettronico di solito non si applicano a questo proposito, poiché le piattaforme di collaborazione normalmente non forniscono servizi di semplice trasporto (*mere conduit*) o di memorizzazione temporanea (*caching*) ai sensi di tali disposizioni». Così Comunicazione della Commissione al Parlamento Europeo al Consiglio al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *op. cit.*, 8, nota 24.

[39] E. Tosi, *Contrasti giurisprudenziali in materia di responsabilità civile degli hosting provider - passivi e attivi - tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, social network e aggregatori di contenuti*, in *Rivista di Diritto Industriale*, 1, 2017, 56 ss.

[40] M. Mensi – P. Falletta, *op. cit.*, 142.

4. L'esperienza italiana

Anche nel nostro ordinamento si è tentato di introdurre una disciplina in materia di *sharing economy*. Tentativi che ben possono essere oggi base di partenza per ulteriori riflessioni e iniziative di carattere legislativo.
Nel corso della XVII legislatura sono state presentate diverse proposte di legge su singoli aspetti in materia di *sharing economy*[41], più due proposte con un respiro di ordine generale e che tentano di portare a sistema l'intero fenomeno. Rientrano in quest'ultima categoria le proposte n. 3564 alla Camera dei Deputati e la n. 2268 al Senato della Repubblica.

4.1. La proposta alla Camera dei Deputati

La prima è la proposta di legge n. 3564 del 27 gennaio 2016 in tema di "Disciplina delle piattaforme digitali per la condivisione di beni e servizi e disposizioni per la promozione dell'economia della condivisione"[42].
Tale proposta è volta in primo luogo a regolamentare le piattaforme digitali per la condivisione di beni e servizi[43]. Ciò tramite l'introduzione di un regime autorizzatorio, subordinato alla predisposizione di un documento di politica aziendale, volto a regolamentare i rapporti tra gestori della piattaforma ed utilizzatori. Ancora, la proposta contiene interventi di carattere fiscale, finanziario, e l'attribuzione di nuovi poteri e competenze all'Autorità Garante della Concorrenza e del Mercato[44].
Innanzitutto, l'art. 2, c. 1, lett. a), definisce "economia della condivisione" quella «generata dall'allocazione ottimizzata e condivisa delle risorse di spazio, tempo, beni e servizi tramite piattaforme digitali». La stessa norma sottolinea la natura multi-versante delle piattaforme quando fa riferimento a queste come abilitatori che «mettono in contatto gli utenti e possono offrire servizi di valore aggiunto».

[41] Tra questi gli atti Camera nn. 4283 dell'8 febbraio 2017, Disposizioni concernenti le prestazioni di lavoro con modalità di esecuzione organizzate o coordinate dal committente; 4059 del 27 settembre 2016, Disposizioni per la promozione dell'utilizzo condiviso di veicoli privati (car sharing); 2947 del 10 marzo 2015, Modifica all'articolo 27 della legge 8 marzo 2000, n. 53, in materia di utilizzazione di buoni locali emessi da associazioni senza scopo di lucro; 3752 del 6 aprile 2016, Disciplina dell'attività di ristorazione e ricettiva in abitazione privata; 3254 del 27 luglio 2015, Introduzione del divieto di tariffazione oraria nell'uso condiviso di veicoli privati tra più persone; 2979 del 20 marzo 2015, Concessione di finanziamenti a tasso agevolato per la promozione della mobilità sostenibile, anche attraverso la diffusione di veicoli elettrici, la riorganizzazione dei processi produttivi e lo sviluppo della distribuzione di servizi in modalità condivisa; 2436 del 6 giugno 2014, Modifiche all'art. 23 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, e altre disposizioni per la promozione dell'uso condiviso di autovetture private.

[42] La proposta di legge C. 3564 è consultabile sul sito della Camera dei Deputati al seguente link: www.camera.it/leg17/126?idDocumento=3564

[43] L'art. 1, c. 2, parla di «misure relative alla gestione e all'utilizzo delle piattaforme digitali per la condivisione di beni e di servizi che operano su mercati a due versanti e fornisce strumenti atti a garantire la trasparenza, l'equità fiscale, la leale concorrenza e la tutela dei consumatori».

[44] Servizio Studi Camera dei Deputati, *Disciplina delle piattaforme digitali per la condivisione di beni e servizi e disposizioni per la promozione dell'economia della condivisione A.C. 3564*, Dossier n. 433 - Schede di lettura, 2 maggio 2016, disponibile al link: www.documenti.camera.it/Leg17/Dossier/Pdf/AP0065.Pdf

4.1.1. Regime autorizzatorio e "documento di politica aziendale"

Gli articoli 3 e 4 danno forma al regime autorizzatorio che avrebbe permesso alla piattaforma di svolgere la sua attività di intermediazione. I gestori delle piattaforme digitali si sarebbero quindi dovute dotare di un "documento di politica aziendale" da sottoporre all'approvazione dell'Autorità Garante della Concorrenza e del Mercato (art. 4). L'AGCM, alla quale l'art. 3, c. 1, attribuisce la regolazione e la vigilanza sull'attività delle piattaforme digitali, una volta approvato il "documento di politica aziendale"[45] avrebbe inserito la piattaforma nel "Registro elettronico nazionale" presso di lei istituito (art. 3, c. 2). La mancata iscrizione al Registro è sanzionata in base a quanto previsto dall'art. 10.

Ma soprattutto, elemento di grande importanza della proposta è l'attenzione data alle condizioni contrattuali tra la piattaforma e l'utente. Spesso sono infatti queste le uniche norme che regolano i rapporti tra i soggetti coinvolti. Ciononostante, sarebbe potuto essere utile anche regolare i rapporti contrattuali tra piattaforma e prestatore di servizio, soprattutto non professionale.

L'art. 3, c. 2, prevede precisi vincoli, determina i contenuti obbligatori del documento e individua alcune clausole vietate, costruite sul modello delle clausole vessatorie del codice del consumo, che se apposte «sono nulle e non comportano la nullità dell'intero contratto tra utente operatore e gestore».

Il documento di politica aziendale, che deve essere esplicitamente sottoscritto dagli utenti (art. 4, c. 8), non avrebbe potuto contenere previsioni che avessero imposto, anche indirettamente all'utente operatore:

- forme di esclusiva o di trattamento preferenziale in favore del gestore;
- il controllo dell'esecuzione della prestazione, anche tramite apparati o sistemi *hardware* o *software*;
- la fissazione di tariffe obbligatorie;
- l'esclusione dall'accesso alla piattaforma digitale del gestore o la sua penalizzazione nella presentazione della sua offerta agli utenti fruitori per motivazioni non gravi e oggettive;
- la cessione gratuita non revocabile di propri diritti d'autore;
- il divieto di acquisizione e di utilizzo di informazioni pubbliche del gestore che non siano tutelate da adeguate misure tecniche di protezione;
- l'obbligo di promozione dei servizi del gestore;
- il divieto di commento critico del gestore;
- la condivisione con altri utenti operatori di informazioni, giudizi e analisi;
- l'obbligo di fornire il consenso a cedere a terzi qualunque dato utente.

L'art. 4, c. 5, prevede poi che eventuali transazioni in denaro operate su piattaforme digitali avvengano esclusivamente tramite sistemi di pagamento elettronici nonché modalità di registrazione univoche per evitare la creazione di profili falsi o non riconducibili a uno specifico utente (art. 4, c. 4).

[45] In base all'art. 4, c. 7, il documento di politica aziendale è infatti condizione vincolante per l'iscrizione nel Registro.

Per quanto riguarda la natura del documento di politica aziendale, pur non essendo meglio specificata, l'art. 4, c. 8, sembrerebbe richiamare l'art. 1341 c.c. facendo propendere per la qualificazione di "contratto per adesione", ovvero del contratto destinato a regolare una serie indefinita di rapporti che sia stato predisposto unilateralmente da un contraente[46].

4.1.2. Fiscalità e protezione dei dati personali

L'art. 5 va a toccare un altro tema spesso dibattuto quando si parla di *sharing economy*, ossia quello della fiscalità. Il primo comma prevende innanzitutto che il reddito percepito dagli utenti sia denominato «reddito da attività di economia della condivisione non professionale». Successivamente individua una soglia di 10.000 euro sotto i quali l'imposta sarà fissa del 10% (secondo il modello della c.d. *flat tax*)[47], mentre sopra tale soglia il reddito sarà cumulato con i redditi da lavoro dipendente o autonomo con applicazione dell'aliquota corrispondente.
Altro tema toccato dall'economia digitale è quello della riservatezza e tutela dei dati personali. L'economia digitale è infatti sempre più un'economia c.d. *data driven*, che rinviene nell'utilizzo dei dati personali una grande risorsa.
Non stupisce quindi se l'art. 7 della proposta in commento si occupa di questo tema introducendo il concetto di "dato utente", definito come: «il dato personale di cui sia stato acquisito il consenso […] e il dato prodotto e ottenuto dall'integrazione digitale di oggetti (*internet of things*)».
Oltre ad aspetti poco innovativi, come il riferimento atecnico all'acquisizione del consenso al "dato personale" e non al "trattamento" dello stesso[48], se ne affiancano altri di particolare interesse, come l'esplicita considerazione dei cc.dd. meta-dati, ossia i dati prodotti dalle attività poste in essere dall'utente tramite l'interazione con la piattaforma *social*, come identificativi della persona e quindi trattabili solo previo consenso.
Il c. 2 stabilisce, oltre all'informativa con la richiesta di consenso per la cessione dei dati già prevista dalla normativa sulla *data protection*, la possibilità per l'utente di opporsi alla cessione chiedendo la cancellazione dei dati. Al Garante per la Protezione dei dati personali sarebbe spettato il compito di definire i contenuti minimi di tale informativa e le modalità per la cancellazione dei dati.

4.1.3. Incentivi alla *sharing economy*

Infine, la proposta contiene norme per incentivare la diffusione dell'economia della condivisione: dall'art. 6, che prevede misure annuali per la diffusione dell'economia della condivisione, all'art. 8 sulle linee guida agli enti locali per valorizzare e diffondere le buone pratiche della condivisione, all'art. 9, con le attività di monitoraggio e l'art. 12,

46 Servizio Studi Camera dei Deputati, *cit.*, 4.

47 *Ibid.*, 6.

48 *Ibid.*, 5.

che prevede che le risorse finanziarie derivanti dall'attuazione della proposta siano destinate a corsi di formazione e aggiornamento, convegni, congressi o al finanziamento di politiche di innovazione tecnologica e digitalizzazione del paese.

4.2. La proposta al Senato della Repubblica

La seconda proposta in materia di economia collaborativa è quella presentata il 3 marzo 2016, al Senato della Repubblica: il disegno di legge n. 2268 recante *Disposizioni in materia di sharing economy*.
Tale proposta, sebbene nella sostanza non si discosti molto da quella precedentemente analizzata della quale segue l'impostazione, si differenzia per avere una portata meno ambiziosa e un'ottica più ristretta.
Tale impostazione è riscontrabile già nella relazione di accompagnamento del testo laddove considera la *sharing economy* come un modello caratterizzato dall'ottimizzazione e dal risparmio negli scambi, escludendo così ogni attività che abbia un collegamento con una logica di profitto e di consumo[49].
Su questa linea, l'art. 2, nei commi successivi alle definizioni, inserisce alcune limitazioni all'ambito di applicazione della proposta.
Così, l'attività di condivisione non deve essere svolta professionalmente o consistere in un'attività imprenditoriale (c. 3) e, soprattutto, la proposta prende posizione nell'escludere che tra il gestore della piattaforma e il prestatore (condividente) vi possa essere un rapporto di lavoro subordinato o parasubordinato (c. 4).
Tale norma, sebbene tocchi un ambito sensibile in materia di *sharing economy*, non sembrerebbe però risolutiva. Da una parte affronta un tema che nella proposta della Camera è assente, dall'altra non dà alcuna indicazione in merito al se e quando tra prestatore e gestore della piattaforma si instauri un rapporto di lavoro, ma si limita a dire che se c'è un rapporto di lavoro si esce dall'ambito di applicazione di tale normativa.

4.2.1. Regime autorizzatorio e condizioni contrattuali

Come la proposta della Camera, anche il c. 4 della proposta del Senato pone attenzione alle condizioni generali di contratto usate dalle piattaforme, prevedendo (ancorché in misura ridotta) le stesse clausole vietate. «Sono nulle, ove inserite nelle condizioni generali di contratto, le clausole che impongano, anche indirettamente: a) al condividente, ogni forma di esclusiva a favore del gestore del portale di condivisione; b) al condividente, la fissazione di tariffe predeterminate; c) al condividente, l'obbligo di promozione di altri servizi offerti dal gestore del portale di condivisione; d) al fruitore, il divieto di commento critico relativo al servizio ricevuto; e) al fruitore, il divieto di condivisione con altri fruitori di informazioni, giudizi ed analisi sul servizio ricevuto».
L'art. 4 attribuisce poi all'AGCM le competenze in materia di vigilanza e la tenuta del

[49] Relazione di accompagnamento del disegno di legge n. 2268, Disposizioni in materia di sharing economy, Senato della Repubblica, 2.

"Registro nazionale on line dei portali di condivisione e dei condividenti" al quale i gestori dei portali avrebbero dovuto iscriversi.

4.2.2. Tutele in materia alimentare, trattamento fiscale e misure di incentivo

L'art. 5 introduce come tutela per il consumatore quello del rispetto dei requisiti di sicurezza e igiene minimi da prevedere con apposito regolamento ministeriale. Ciònonostante, la norma sembrerebbe avere come obiettivo non dichiarato quello delle attività legate al settore alimentare, come gli *home restaurant*, e non sembrerebbe applicabile agli altri settori dell'economia collaborativa.
Il secondo comma dell'art. 5 prevede che «salva l'applicazione di specifiche normative di settore, si applica l'articolo 2043 del codice civile». L'inserimento di tale norma si comprende solo grazie alla lettura della relazione di accompagnamento che chiarisce l'obiettivo di tale previsione, ossia «in assenza di tale disposizione il consumatore sarebbe privo di qualsiasi tutela per i danni subiti stante una costante giurisprudenza di legittimità che esclude la risarcibilità del danno nel caso delle prestazioni di cortesia che avvengono tra privati senza la previsione di un corrispettivo»[50]. Tuttavia, pur essendo comprensibile la *ratio* della norma, il problema non è tanto o solo individuare il tipo di responsabilità da applicare, quanto e in via prioritaria avere adeguati criteri per distinguere quando un certo servizio è prestato a titolo di cortesia o come attività imprenditoriale. Poiché questo non sembrerebbe l'obiettivo della norma, e poiché l'intera proposta tiene fuori dal suo raggio di applicazione ogni attività di carattere imprenditoriale (il ché renderebbe comunque fuori luogo l'uso del termine "consumatore" che in assenza di un soggetto "professionista" non sembrerebbe trovare giustificazione), si deve concludere che il secondo comma dell'art. 5 intenda rendere giustiziabili ogni tipo di rapporto mediato dall'utilizzo di una piattaforma digitale e risarcibile aquilianamente ogni eventuale danno ingiusto.
Anche il trattamento fiscale di cui all'art. 7 sembrerebbe riprendere quello della proposta della Camera. La norma individua una soglia di reddito pari a 10.000 euro al di sotto della quale si applica un'imposta del 10%. Nulla si dice nel caso si superi tale soglia.
Infine, dal punto di vista delle misure a sostegno dell'economia collaborativa, l'art. 8 impegna il Governo a rimuovere gli ostacoli alla diffusione e promozione della *sharing economy*.

5. Un'agenda europea per l'economia collaborativa

Un buon modo per valutare la portata di queste proposte potrebbe essere quello di verificare se e in che misura queste soddisfino i criteri che secondo l'Unione europea bisognerebbe tenere in considerazione per disciplinare la *sharing economy*.
Nel giugno del 2016 infatti, la Commissione europea ha elaborato una Comunicazione

[50] *Ibid.*, 3.

dal titolo *Un'agenda europea per l'economia collaborativa*, allo scopo di fornire orientamenti su come il diritto dell'UE dovrebbe essere applicato in questo settore, chiarendo le questioni essenziali affrontate sia dagli operatori del mercato che dalle autorità pubbliche[51].

La Comunicazione della Commissione, infatti, considera la *sharing economy* non solo come un'occasione per i consumatori – i quali potranno avere accesso a nuovi servizi, un'offerta più ampia e a prezzi più bassi – ma anche come il presupposto di nuove opportunità di occupazione, flessibilità e fonte di reddito.

Su questa linea, se da una parte intende sostenere e incoraggiare la condivisione e un uso più efficiente delle risorse, dall'altra è consapevole che l'economia collaborativa pone criticità dal punto di vista normativo. Ed infatti questa rende meno nette e in alcuni casi problematiche le distinzioni tra consumatore e professionista, lavoratore subordinato e autonomo, prestazione di servizi a titolo professionale e non professionale[52].

Gli ambiti sui quali la Comunicazione della Commissione invita a riflettere, al fine di rimuovere ambiguità e le criticità derivanti dall'applicazione di un quadro normativo obsoleto o lacunoso, sono quindi quelli dei: requisiti di accesso al mercato, responsabilità delle piattaforme digitali, applicazione del diritto a tutela dei consumatori, individuazione di rapporti di lavoro connessi all'attività delle piattaforme digitali, normativa fiscale applicabile.

5.1. Autorizzazioni e licenze

Il primo punto toccato dalla Commissione è quello relativo ai requisiti di accesso al mercato.

Autorizzazioni o licenze, infatti, dovrebbero essere previste solo se strettamente necessarie per la tutela di interessi generali. Dunque, le piattaforme dovrebbero essere soggette a autorizzazioni solo quando svolgono un ruolo attivo e non quando si limitano ad agire come intermediari.

La Commissione non dà indicazioni su quali sino gli interessi meritevoli di tutela. Ciononostante, ulteriori informazioni in merito si potrebbero ricavare dalla Direttiva 31/2000/UE, la c.d. "direttiva *e-commerce*" e dalla Direttiva 2006/123/UE, la c.d. "direttiva servizi".

Da una parte l'art. 4 della "direttiva *e-commerce*" stabilisce il principio dell'assenza di autorizzazione preventiva, dall'altra la "direttiva servizi" permette agli Stati membri di subordinare l'accesso ad un servizio e il suo esercizio ad un regime di autorizzazione soltanto se: a) il regime di autorizzazione non è discriminatorio nei confronti del prestatore; b) la sua necessità è giustificata da un motivo imperativo di interesse generale; c) l'obiettivo perseguito non può essere conseguito tramite una misura meno restritti-

[51] Commissione europea, *Un'agenda europea per l'economia collaborativa*, 2 giugno 2016, Bruxelles, consultabile al link: www.europa.eu/rapid/press-release_IP-16-2001_it.htm

[52] Comunicazione della Commissione al Parlamento Europeo al Consiglio al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *op. cit.*, 2.

va, un controllo a posteriori interverrebbe troppo tardi per avere reale efficacia (art. 9). Secondo la "direttiva servizi" inoltre, tra i motivi imperativi di interesse generale rientrerebbero: l'ordine pubblico; la sicurezza pubblica; l'incolumità pubblica; la sanità pubblica; il mantenimento dell'equilibrio finanziario del sistema di sicurezza sociale; la tutela dei consumatori, dei destinatari di servizi e dei lavoratori; l'equità delle transazioni commerciali; la lotta alla frode; la tutela dell'ambiente, incluso l'ambiente urbano; la salute degli animali; la proprietà intellettuale; la conservazione del patrimonio nazionale storico ed artistico; gli obiettivi di politica sociale e di politica culturale[53].
A tal riguardo si è visto che entrambe le proposte introducono un regime autorizzatorio in capo alle piattaforme. Per essere legittimo questo dovrebbe quindi tutelare uno degli interessi generali. La proposta della Camera, meglio di quella del Senato, potrebbe così integrare i riferimenti alla tutela dei consumati, dei destinatari dei servizi e dei lavoratori, l'equità della transazione commerciali e la lotta alle frodi.

5.2. Prestatori di servizi professionali, non professionali e responsabilità delle piattaforme

Dal punto di vista dei prestatori dei servizi, l'invito è quello di distinguere tra i privati cittadini e soggetti professionali, anche in considerazione del fatto che sempre più micro o piccole imprese fanno ricorso a questi modelli di scambio per i loro affari. A tal riguardo, solo la proposta della Camera sembrerebbe avvicinarsi a tale obiettivo. Tanto più se la proposta del Senato sembrerebbe esplicitamente escludere dal suo campo di applicazione ogni attività imprenditoriale, lasciando quindi fuori tutti quei soggetti professionali che fanno uso delle piattaforme di condivisione.
Per distinguere tra un prestatore di servizi professionale e non professionale, la commissione suggerisce l'adozione di soglie[54].
Dal punto di vista della responsabilità delle piattaforme, sull'esempio della responsabilità per gli ISP prevista dalla "direttiva *e-commerce*", la Commissione suggerisce che queste siano esenti da responsabilità se si limitino al ruolo di intermediario tecnico, automatico e passivo e, quindi, non esercitino alcun ruolo attivo o di controllo. Anche qui è prevista l'assenza di un obbligo generale di sorveglianza ma la piattaforma si deve prontamente attivare per cancellare o disabilitare l'accesso al contenuto illecito qualora ne venga a conoscenza[55].
Da ciò ne segue che la piattaforma non sarà responsabile per recensioni false, commenti negativi o altri fenomeni patologici legate all'utilizzo delle stesse, se si limiti a un mero servizio di *hosting*. Chiaramente, tale deroga non si estenderà oltre questo ruolo passivo e non coprirà altri servizi accessori offerti dalla piattaforma[56].
La Comunicazione individua alcuni elementi da cui si può desumere il ruolo più o

[53] Cfr. Considerando 40, Direttiva servizi (2006/123/UE).

[54] Comunicazione della Commissione al Parlamento Europeo al Consiglio al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *op. cit.*, 7.

[55] *Ibid.*, 8.

[56] *Ibid.*, 9.

meno passivo della piattaforma. A tal fine si potrà tener conto della possibilità per la piattaforma di influire sul prezzo del bene o servizio, stabilire i termini contrattuali nei rapporti tra prestatore e utente, se ha la disponibilità dei beni usati per il servizio, o se si limiti a fornire servizi della società dell'informazione o ulteriori servizi accessori all'utente[57]. Dovrà quindi condursi un'analisi caso per caso.
Su tali questioni, nessuna delle proposte presentate al Parlamento italiano ha preso posizione.

5.3. Applicazione delle normative a tutela di consumatori e utenti

Ancora, la Commissione rivendica l'applicazione della normativa consumeristica, così come quella delle pratiche commerciali, della concorrenza e in materia di protezione dei dati personali a ogni piattaforma e prestatore di servizi che rivesta un ruolo di professionista[58]. Anche qui dovrà condursi un'analisi caso per caso applicando i criteri distintivi del diritto UE tra professionista e consumatore.
A tal fine la Comunicazione individua ulteriori elementi da cui si può desumere la natura professionale del prestatore di servizi o della piattaforma: la frequenza con cui si offrono certi servizi di contro a attività meramente occasionali, l'individuazione di una finalità di lucro[59] o l'entità del fatturato[60].
Su tali punti, al di fuori di una presunzione di abuso di dipendenza economica da parte della piattaforma prevista dall'art. 10, c. 2, dalla proposta della Camera[61], nessuna delle due proposte disciplina il tema.

5.4. Rapporto di lavoro e fiscalità

Venendo al tema del rapporto di lavoro con le piattaforme, anche qui la Comunicazio-

[57] *Ibid.*,7 ss.

[58] *Ibid.*, 9 ss.

[59] «In linea di massima i prestatori che intendono scambiare beni o competenze (come nel caso di "scambi di case" o "banche del tempo") non si qualificheranno come professionisti. I prestatori che si limitano ad ottenere il rimborso dei costi di una transazione potrebbero non perseguire un lucro. Quei prestatori che invece ricevono una retribuzione al di là del rimborso dei costi probabilmente perseguono finalità di lucro», *ibid.*, 10.

[60] «Maggiore è il fatturato generato dal prestatore di servizi (che provenga da una o più piattaforme di collaborazione), maggiore è la probabilità che il prestatore si qualifichi come professionista. A questo proposito è importante valutare se tale fatturato sia il frutto della stessa attività (ad esempio *carpooling*) o di vari tipi di attività (*carpooling*, servizi di giardinaggio, ecc.). Nella seconda ipotesi un fatturato maggiore non implica necessariamente che il prestatore si qualifichi come professionista, in quanto tale fatturato può non avere alcun collegamento con la sua altra (principale) attività», *ibid.*, 10 ss.

[61] Secondo la norma contenuta nella proposta della Camera, in mancanza di prova contraria, l'Agcm sanziona la piattaforma che sfrutta abusivamente il suo potere sull'utente fornitore quando questo «si obblighi verso il gestore [della piattaforma] a un patto in forza del quale l'utente operatore stesso si trovi a dover ingiustificatamente rifiutare ai propri clienti, potenziali o abituali, proposte di fornitura di beni o servizi a condizioni migliorative rispetto a quelle assicurate al gestore stesso».

ne si pone il problema di distinguere tra prestazioni occasionali e attività che invece devono essere qualificate come rapporti di lavoro. Sarà quindi necessaria una valutazione caso per caso andando a valutare se: l'attività del prestatore è svolta sotto la direzione della piattaforma che ne determina l'attività, la retribuzione e le condizioni di lavoro; l'entità della prestazione, anche tramite il ricorso a soglie (salario, orario di lavoro), per distinguere attività modeste da quelle con un certo valore economico; infine la presenza e l'entità di una retribuzione[62].

Dunque, in materia di lavoro la Commissione suggerisce agli Stati membri di valutare l'adeguatezza della propria normativa sul lavoro con i nuovi modelli imprenditoriali al fine di estenderne l'applicazione[63].

Nonostante queste indicazioni, mentre la proposta della Camera sembrerebbe non prendere posizione, quella del Senato esclude dal suo raggio d'azione ogni attività che sia qualificabile come rapporto di lavoro.

Passando alla materia fiscale, la Commissione invita all'adozione di obblighi proporzionati e a condizione di parità, così come l'aumento della trasparenza e l'informazione verso gli utenti. Quindi anche i prestatori di servizi e le piattaforme dell'economia collaborativa sono tenuti a pagare le imposte pertinenti, tra cui le imposte sul reddito delle persone fisiche, delle società e l'imposta sul valore aggiunto, e le piattaforme dell'economia collaborativa dovrebbero cooperare con le autorità nazionali per la registrazione delle attività economiche e agevolare la riscossione delle imposte[64].

Su questo punto, entrambe le proposte sembrerebbero soddisfare i parametri europei nella misura in cui fanno ricorso a delle soglie, sebbene bisognerebbe poi valutare se in concreto un'unica soglia con le caratteristiche di una *flat tax* possa soddisfare criteri di proporzionalità e parità.

Infine, la Comunicazione incoraggia attività che possano favorire questi nuovi modelli di business, tramite la semplificazione e il monitoraggio delle attività e dei loro sviluppi[65].

Da questo punto di vista, la proposta della Camera sembrerebbe prevedere interventi e incentivi a favore dell'economia collaborativa maggiori rispetto alla proposta del Senato.

6. Conclusioni

In considerazione di quanto detto, risulterà chiaro come il settore da regolamentare sia complesso, vario e coinvolgente ambiti territoriali superiori al livello nazionale.

L'analisi delle due proposte italiane mostra un primo interesse alla materia, senza dubbio positivo, ancorché il paragone con i criteri individuati dalla Commissione europea lascia intendere che la strada da percorrere sia ancora lunga. Oltre a elementi di in-

[62] Comunicazione della Commissione al Parlamento Europeo al Consiglio al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *op. cit.*, 13 ss.

[63] *Ibid.*, 14.

[64] *Ibid.*, 15.

[65] *Ibid.*, 16 ss.

dubbio interesse, come le norme in materia di clausole contrattuali nei rapporti con le piattaforme digitali, risulta infatti ancora assente l'attenzione a tematiche sensibili dal punto di vista giuridico e sociale.

Ancora, proseguendo e portando a compimento l'analisi caso per caso suggerita dalla Commissione europea, una prima strada da seguire potrebbe essere quella di elaborare principi e clausole generali aperte e flessibili che, più che norme di dettaglio spesso vittima di una rapida obsolescenza, meglio si prestano a regolare il nuovo ambiente digitale senza soffocarne lo sviluppo[66].

Ciononostante non si può non registrare un certo interesse e la volontà di porre rimedio a alcune storture che si sono sviluppate nelle pieghe e lacune della normativa. Ciò è testimoniato sia a livello europeo dalla Comunicazione della Commissione che a livello nazionale dalle due proposte esaminate.

Proposte che ben potrebbero essere il primo *step* di una riflessione ancora in corso sul ruolo e le modalità di intervento normativo. Riflessione che ben potrebbe essere la base di nuove analisi e proposte normative durante l'appena iniziata XVIII legislatura.

La sfida a cui è chiamato il diritto è sicuramente complessa ma non può non essere accolta. Un quadro normativo chiaro, innovativo e *future proof*, possibilmente coordinato e armonizzato a livello sovrannazionale, è sicuramente un elemento di garanzia e tutela per tutti i soggetti coinvolti nell'economia collaborativa.

[66] S. Rodotà, *op. cit.*, 41 ss.

Note a Sentenza
Sezione Italia

La Corte Costituzionale ribadisce che le esternazioni di un parlamentare non sono *legibus solutae*

Claudio Martinelli, Jessica De Vivo

Corte Costituzionale, 23 marzo 2018, n. 59

Per il loro tenore testuale, le frasi per cui è in corso il procedimento penale non risultano ex se riconducibili a opinioni espresse nell'esercizio delle funzioni parlamentari.
La prerogativa parlamentare di cui all'art. 68, c. 1, Cost., infatti, non pù essere estesa sino a ricomprendere gli insulti – di cui è comunque discutibile la qualificazione come opinioni – solo perché collegati con le "battaglie" condotte da esponenti parlamentari.
Le frasi, inoltre, non hanno alcun contenuto sostanzialmente corrispondente a quello dei due atti di sindacato ispettivo cui si fa riferimento, così venendo a mancare una delle condizioni richieste dalla già richiamata giurisprudenza della Corte costituzionale affinché l'attività esterna del membro del Parlamento possa essere legittimamente ricompresa nelle funzioni parlamentare.

Keywords: Insindacabilità parlamentare, Diffamazione, Discriminazione razziale, Conflitto di attribuzione, Nesso funzionale.

La sentenza n. 59/2018 della Corte costituzionale ha rivitalizzato il tema dell'insindacabilità parlamentare, facendolo tornare agli onori delle cronache con un caso che ha suscitato molto scalpore da un duplice punto di vista. In primo luogo, per le cariche coinvolte, ossia un ex vice-Presidente del Senato e un ex ministro; in secondo luogo, per l'oggetto delle dichiarazioni in questione. È proprio sulla base di queste dichiarazioni, per le quali non è stata riconosciuta l'insindacabilità dal Giudice delle leggi, che il senatore Roberto Calderoli sarà processato dal Tribunale di Bergamo per il reato di cui all'art. 595, c. 3, c.p. con l'aggravante di cui all'art. 3 del d.l. 122/93.
La vicenda trae origine, appunto, da alcune affermazioni pronunciate dal senatore Calderoli nei confronti dell'allora ministro dell'integrazione Cécile Kashetu Kyenge nell'ambito di un comizio tenuto a Treviglio nel luglio 2013, poi diffuse da organi di stampa a livello nazionale. In particolare, il senatore aveva affermato che l'onorevole Kyenge «sarebbe un ottimo Ministro, […] ma dovrebbe esserlo in Congo non in Italia perché se c'è […] bisogno di un Ministro per le pari opportunità per l'integrazione, c'è bisogno là, perché […] se vedono passare un bianco là gli sparano». Lo stesso senatore aveva poi attribuito al ministro Kyenge «sembianze di un orango», tali da lasciarlo «sconvolto» nel vederla comparire sul sito del Governo italiano. Queste frasi, oltre ad integrare il reato di diffamazione di cui all'art. 595 c.p., presentavano due aggravanti: l'aver recato l'offesa «col mezzo della stampa o con qualsiasi altro mezzo di pubblicità,

ovvero in atto pubblico», *ex* c. 3, art. 595 c.p.; la finalità di discriminazione razziale, ai sensi dell'art. 3 del d.l.122/93.

Il Tribunale di Bergamo, competente a giudicare nel caso di specie, aveva disposto la trasmissione degli atti al Senato della Repubblica, affinché venisse accertato se il fatto oggetto del procedimento penale *de quo* rientrasse nell'alveo dell'art. 68, c. 1, Cost.

Il Senato procedeva, nella seduta del 16 settembre 2015, a votazione per parti separate, esprimendo voto favorevole all'insindacabilità del fatto ai sensi dell'art. 3 d.l. 122/93 e voto favorevole alla sindacabilità del fatto ai sensi dell'art. 595, c. 3, c.p.[1].

Con ordinanza del 29 gennaio 2016, il Tribunale ordinario di Bergamo promuoveva conflitto di attribuzione tra poteri dello Stato nei confronti del Senato della Repubblica, con riferimento alla suddetta deliberazione. Il ricorrente, in primo luogo, sosteneva che l'Assemblea della Camera Alta, esprimendosi con una doppia deliberazione, avrebbe invaso un settore riservato alla giurisdizione. In altre parole, secondo il Tribunale, l'Assemblea avrebbe apprezzato non un fatto naturalisticamente unitario, ma la sua qualificazione giuridica, con la conseguenza che il tribunale si troverebbe a giudicare su un fatto diversamente qualificato rispetto a quello contestato dal Pubblico Ministero. Sotto un secondo profilo, il ricorrente sosteneva che, in ogni caso, le dichiarazioni oggetto del procedimento penale non sarebbero state coperte dalla guarentigia del c. 1 dell'art. 68 Cost., non potendosi individuare un nesso funzionale tra le dichiarazioni rese dal senatore Calderoli *extra moenia* e la sua attività parlamentare, a differenza di quanto sostenuto nella relazione della Giunta delle Elezioni e delle Immunità parlamentari, secondo cui le parole di Calderoli rispecchiavano il contenuto di due atti di sindacato ispettivo, richiamati nella delibera della Giunta stessa.

Ciò posto, la Corte costituzionale, con ordinanza n. 139 del 2016, riconosceva l'ammissibilità del conflitto di attribuzione sollevato dal Tribunale di Bergamo. Il Senato della Repubblica, con atto dell'11 agosto del 2016, si costituiva in giudizio, eccependo unicamente l'improcedibilità del conflitto, a causa dell'inesistenza della notificazione degli atti introduttivi. Dopo la rinnovazione della notifica[2] e la nuova costituzione in giudizio, il Senato riteneva inammissibile il ricorso del Tribunale sotto entrambi i profili. Il resistente sosteneva, da un lato, il difetto di interesse a promuovere il conflitto da parte dei giudici di Bergamo e, dall'altro, che il Tribunale non avrebbe assolto l'onere di riportare in maniera esaustiva il contenuto delle dichiarazioni ritenute lesive, limitandosi solo a una pedissequa trascrizione del capo di imputazione

Nel merito, poi, il Senato insisteva sul rinvio agli atti tipici dell'attività parlamentare, già richiamati in sede di delibera della Giunta. In particolare, la parte resistente sosteneva che la verifica della sussistenza del nesso funzionale avrebbe dovuto incentrarsi bensì sulla valutazione di un possibile collegamento "sensato" all'esercizio delle funzioni parlamentari.

Dopo aver respinto entrambe le doglianze di inammissibilità mosse dal Senato, la Cor-

[1] La proposta della Giunta delle Elezioni e delle Immunità Parlamentari, invece, era quella di ritenere il fatto, ai sensi sia dell'art. 595, c. 3, c.p., sia dell'art. 3, d.l. 122/93, coperto dall'insindacabilità *ex* c. 1 dell'art. 68 Cost., perché «concerne opinioni espresse da un membro del Parlamento nell'esercizio delle sue funzioni» (Relazione della Giunta delle Elezioni e delle Immunità Parlamentari, Doc. IV *ter* n. 4 A).

[2] C. Cost., ord. 4 aprile 2017, n. 101.

te ritiene fondato, nel merito, il ricorso del Tribunale di Bergamo sotto entrambi i profili rilevati. Per quel che concerne il primo aspetto, ossia l'invasione da parte del Senato di un settore riservato alla giurisdizione, il Giudice delle leggi tiene a ribadire che le Camere «non sono chiamate a pronunciarsi sugli effetti che la singola autorità giudiziaria fa derivare dall'opinione espressa dal parlamentare, ma solo sulla correlazione tra quest'ultima e l'esercizio delle funzioni parlamentari»[3]. Compito dell'autorità giudiziaria, invece, è quello di «qualificare giuridicamente l'opinione espressa, ricollegando al fatto storico gli effetti giuridici previsti dalla legge». Il senato della Repubblica, affermando che il fatto per il quale il senatore Calderoli è sottoposto a procedimento penale è sindacabile solo con riferimento al reato di diffamazione aggravata dal mezzo di pubblicità, ma non in rapporto all'aggravante della finalità di discriminazione razziale, di fatto opera una valutazione più profonda, che va ben al di là delle sue competenze, fino a entrare direttamente nella qualificazione giuridica del fatto.

Per quel che concerne, poi, il secondo aspetto, la Corte torna a ribadire quanto già affermato in più occasioni, ossia che l'insindacabilità parlamentare è una guarentigia, la cui applicazione non può essere estesa «sino a ricomprendere gli insulti – di cui è comunque discutibile la qualificazione come opinioni – solo perché collegati con le "battaglie" condotte da esponenti parlamentari in favore delle loro tesi politiche»[4]. Inoltre, ad avviso della Corte, le dichiarazioni del senatore Calderoli non risultano corrispondenti sotto il profilo del contenuto ai due atti di sindacato ispettivo in materia di immigrazione richiamati dalla Giunta nella delibera.

Alla luce delle considerazioni poc'anzi prospettate, i giudici costituzionali concludono nel senso della lesività delle attribuzioni costituzionalmente garantite della delibera del Senato sotto entrambi i profili sollevati dal Tribunale di Bergamo e per il conseguente annullamento.

L'approdo della Corte risulta indubbiamente interessante da molteplici punti di vista. In primo luogo, è significativo notare come questa pronuncia arrivi esattamente trent'anni dopo la celebre sentenza n. 1150/1988 e vent'anni dopo la n. 289/1998. La prima rimane la pietra miliare sul percorso della giurisprudenza costituzionale in tema di insindacabilità parlamentare: è la Camera di appartenenza del parlamentare ad avere il potere di valutare il comportamento del proprio membro, verificando la riconducibilità alla prerogativa *ex* art. 68, c. 1, Cost.; tale potere, però, non è arbitrario, ma deve essere correttamente esercitato e apre al conflitto di attribuzioni, che si rende necessario «qualora si verifichi un contrasto tra Parlamento e Autorità giudiziaria circa l'applicazione nel caso concreto dell'art. 68, comma 1, Cost.»[5].

La seconda sentenza è estremamente significativa perché per la prima volta la Corte costituzionale provvedeva ad annullare una delibera di insindacabilità votata da una camera del Parlamento, accogliendo così il conflitto proposto contro di essa.

Anche in questa occasione, i giudici si sono premurati di riconfermare la tradizionale

[3] Punto 5.1. della sentenza in commento.

[4] C. Cost., 17 maggio 2001, n. 137; cfr. T.F. Giupponi, *Le immunità costituzionali*, in M. Angelini - M. Oliviero (a cura di), *Le immunità nel diritto interno e comparato,* Atti del convegno di Perugia 25-27 maggio 2006, Torino, 2014, 69.

[5] C. Martinelli, *L'insindacabilità parlamentare. Teoria e prassi di una prerogativa costituzionale*, Milano, 2002, 47.

impostazione per cui «il giudice costituzionale, che non è chiamato a riesaminare nel merito la valutazione compiuta dalla Camera, deve verificare se vi sia stato un corretto esercizio del potere […] di dichiarare l'insindacabilità del comportamento contestato al membro del Parlamento, anche sotto il profilo della sussistenza e della non arbitraria valutazione dei presupposti ai quali il primo comma dell'art. 68 condiziona l'operare della prerogativa dell'insindacabilità»[6].

Inoltre, si può aggiungere la curiosità che il protagonista di quel caso è lo stesso di quello in commento, ossia l'esponente leghista Roberto Calderoli: a riprova di una certa riottosità della classe politica ad adeguarsi agli indirizzi giurisprudenziali.

Il senso della continuità viene offerto dalla sentenza n. 59/2018 anche sotto il profilo della valutazione del nesso funzionale. Infatti, il ragionamento seguito dalla Corte si inserisce a pieno titolo nella consolidata visione di questo criterio di giudizio, inaugurata dalle sentenze nn. 10 e 11 del 2000[7], tale per cui le dichiarazioni, per poter essere coperte dalla guarentigia *de qua*, debbono essere sostanzialmente riproduttive di un'opinione espressa in sede parlamentare. È dunque necessario che «tra l'atto tipico della funzione parlamentare e la sua manifestazione esterna sia riscontrabile una identità sostanziale di contenuto»[8]. Tale identità non è appunto riscontrata dai giudici costituzionali nel caso di specie: le dichiarazioni del senatore nel comizio del 2013 hanno un contenuto sostanzialmente diverso rispetto a quello dei due sindacati ispettivi indicati dalla Giunta della Relazione e, pertanto, non vi può essere applicazione della prerogativa *ex* c. 1 dell'art. 68 Cost.

La Corte, però, si spinge ben oltre, ritenendo che il tenore stesso delle frasi pronunciate dal parlamentare sia di per sé sufficiente ad escludere l'applicazione della prerogativa. Ancora una volta, i giudici ribadiscono quanto stabilito in precedenti occasioni[9], arrivando ad affermare che le maglie dell'interpretazione della guarentigia dell'insindacabilità non possano essere estese fino a ricomprendere gli insulti – della cui qualificazione come opinioni la Corte dubita – solo perché in qualche modo collegati alle battaglie politiche di cui si fanno portatori i parlamentari.

Alla luce delle considerazioni poc'anzi proposte, è interessante notare come, nonostante la giurisprudenza costituzionale sia ormai consolidata e cristallizzata sul punto, le Camere continuino a servirsi di parametri totalmente esclusi dalla Corte per poter applicare la guarentigia *de qua* in maniera impropria. Un'interpretazione diversa da quella prospettata dalla Corte, e accolta invece dal Senato nel caso di specie, rischierebbe di dilatare «il perimetro costituzionalmente tracciato, generando un'immunità non più soltanto funzionale ma, di fatto, sostanzialmente "personale", a vantaggio di chi sia stato eletto membro del Parlamento»[10]. Significativo è anche il richiamo alla giurispru-

[6] Cons. dir. 5.1. C. Cost., 18 luglio 1998, n. 289.

[7] Sul punto la bibliografia è sterminata. *Ex multi*s si veda A. Pace, *Giurisdizione e insindacabilità parlamentare nei conflitti costituzionali*, in *Quaderni costituzionali*, 2, 2000, 289 ss.

[8] C. Martinelli, *L'insindacabilità parlamentare. Teoria e prassi di una prerogativa costituzionale*, cit., 177.

[9] Il riferimento è, in particolare, alle sentt. C. Cost. 17 maggio 2001, n. 137 e 20 giugno 2002, n. 257.

[10] Punto 3 cons. dir. C. Cost., 26 novembre 2014, n. 264.

denza europea[11] che, lungi dall'essere ultroneo, incide in maniera profonda sul tema, distinguendo nettamente le dichiarazioni rilasciate *intra moenia* e quelle rese al di fuori della sede tipica e affermando in più occasioni la necessità di una rigorosa interpretazione del requisito della ragionevole proporzionalità tra i mezzi impiegati e lo scopo perseguito.

Queste considerazioni e orientamenti giurisprudenziali in tema di insindacabilità, ormai ampiamente consolidati, non esauriscono necessariamente la loro portata nel campo del diritto parlamentare. Infatti, se lette nel quadro dell'intero impianto costituzionale, possono assumere una valenza molto più ampia che investe il concetto stesso di separazione dei poteri, inteso come doveroso e vicendevole bilanciamento volto ad evitare che la "naturale" propensione di ciascun potere ad esorbitare dalle proprie attribuzioni si traduca in una lesione dei diritti fondamentali dei cittadini, soprattutto quando per perpetrare queste lesioni ci si avvale del potente megafono della stampa, intesa nel più ampio significato del termine reso possibile dalle moderne tecnologie.

In tema di esternazioni del pensiero questa esigenza è speculare: vale per i parlamentari sull'insindacabilità e dovrebbe valere anche per i magistrati quando esprimono opinioni che non competono all'esercizio delle loro funzioni, anche se in questo secondo caso non è sempre possibile fare ricorso a strumenti efficaci come il conflitto di attribuzioni di fronte alla Corte costituzionale.

Comunque, questi trent'anni che ci separano dalla sentenza n. 1150/1988 non sono passati invano. La Corte ha spiegato più volte quale sia il perimetro della copertura di cui all'art. 68, c. 1, e che differenza passi tra una prerogativa e un privilegio. Il fatto che ancora troppo spesso le Camere fingano di non averlo capito non depone certo a favore della serietà istituzionale della nostra classe politica.

[11] *Ex multis* si veda C. Martinelli, *Le immunità costituzionali nell'ordinamento italiano e nel diritto comparato. Recenti sviluppi e nuove prospettive*, Milano, 2008, 81 ss.

Il *revirement* della Cassazione: la responsabilità per omesso controllo si applica al direttore della testata telematica*

Silvia Vimercati

Corte di Cassazione, sez. V, 11 dicembre 2017, n. 13398

Alle testate telematiche registrate si estendono non solo le garanzie costituzionali in tema di sequestro accordate agli stampati, ma anche le fattispecie incriminatrici previste per la carta stampata; sicché il direttore della testata online può essere chiamato a rispondere del reato previsto dall'art. 57 c.p.

Sommario

1. Premessa. – 2. Il caso concreto. – 3. Il precedente orientamento della giurisprudenza di legittimità: l'inapplicabilità dell'art. 57 c.p. al direttore del periodico online e, più in generale, della disciplina prevista per la stampa alla rete. – 4. La nuova interpretazione della nozione di "stampa" offerta dalle Sezioni Unite. – 5. La svolta della Cassazione: l'applicabilità dell'art. 57 c.p. al direttore del giornale online. – 6. Alcune considerazioni critiche sulla nuova interpretazione della nozione di "stampa" e sulle conseguenze della equiparazione giuridica tra testate telematiche e tradizionali.

Keywords: Direttore testata telematica, Responsabilità, Internet, Stampa, Omesso controllo

1. Premessa

La mancanza di una normativa *ad hoc* che individui e circoscriva la responsabilità per gli scritti divulgati in rete negli ultimi decenni ha indotto a interrogarsi costantemente sulla disciplina applicabile alle manifestazioni del pensiero nel web e, più precisamente,

* L'articolo è stato sottoposto, su determinazione della direzione, a referaggio anonimo.

sulla possibilità di estendere ad esse il regime previsto per la stampa[1].

Almeno per quanto riguarda lo "statuto penale" della stampa[2], superate le prime oscillazioni, la Corte di cassazione aveva escluso la sua estensione ai contenuti in rete in quanto, stante la non assimibilità di internet alla stampa, riconosceva nel divieto di analogia in *malam partem* un ostacolo non aggirabile per ogni operazione ermeneutica in tale direzione[3].

Con la sentenza che si annota, la quinta sezione penale della Corte di cassazione ha invece posto in essere un vero e proprio *revirement*, stabilendo che il direttore della testata telematica può essere chiamato a rispondere del reato di cui all'art. 57 c.p.[4]; norma che, come è noto, punisce a titolo di colpa per omesso controllo il direttore di un periodico cartaceo per i reati commessi per mezzo del giornale da lui diretto.

La premessa di tale radicale cambio di posizione è la nuova nozione di "stampa" offerta dalle Sezioni Unite nel 2015[5]. Il Supremo Collegio, decidendo della possibilità di

[1] Il primo a individuare in modo puntuale la questione è stato V. Zeno-Zencovich, *La pretesa estensione alla telematica del regime della stampa: note critiche*, in *Diritto dell'informazione e dell'informatica*, 1998, 15 ss., il quale già all'epoca sosteneva che «i tentativi di estendere alle comunicazioni telematiche la vigente normativa sulla stampa costituiscono maldestre operazioni di disciplina giuridica di realtà assai diverse e ben più complesse. Un sistema può ben vivere con delle lacune e l'horror vacui nasconde spesso una radicata vocazione dirigistica degli apparati statali cui nulla deve e può sfuggire». Affronta più di recente il medesimo tema, tra i molti, C. Melzi d'Eril, *La complessa individuazione dei limiti alla manifestazione del pensiero in internet*, in *Diritto dell'informazione e dell'informatica*, 2011, 571 ss.

[2] Ripercorre l'evoluzione della giurisprudenza in tema di estensione delle norme incriminatrici previste per la stampa alla rete, concentrando l'attenzione sui principi e sulle categorie costituzionali chiamati in causa, M. Bassini, *La disciplina penale della stampa alla prova di internet: avanzamenti e arresti nella dialettica giurisprudenziale da una prospettiva costituzionale*, in R. Flor - D. Falcinelli -S. Marcolini (a cura di), *La giustizia penale nella "rete"*, Milano, 2015, 15 ss.

[3] La giurisprudenza, fino alla pronuncia in commento, aveva saputo porre un solido argine agli indebiti tentativi di estensione alla rete di disposizioni incriminatrici esplicitamente dedicate alle sole condotte poste in essere mediante la carta stampata. Tale orientamento, come meglio si dirà, era stato inaugurato proprio dalla Corte di cassazione che aveva statuito l'inapplicabilità dell'art. 57 c.p. al direttore della testata giornalistica telematica. Il riferimento in particolare è al *leading case* Cass. pen., sez. V, 16 luglio 2010, n. 35511, in www.penalecontemporaneo.it, 17 novembre 2010, con nota di S. Turchetti, *L'art. 57 c.p. non è applicabile al direttore del periodico online*; in *Diritto dell'informazione e dell'informatica*, 2010, 899-907, con nota di C. Melzi d'Eril, Roma locuta*: la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica on-line*; in *Guida al diritto*, 44, 2010, 23 ss., con nota di I. Campolo, *Diffamazione: il direttore della testata telematica non è imputabile per reato di omesso controllo*; in *Cassazione penale*, 2011, 2982 ss., con nota di I. Salvadori, *La normativa penale della stampa non è applicabile,* de iure condito*, ai giornali telematici*; in *Quaderni costituzionali*, 2011, 415 ss. con nota di N. Lucchi, *Internet, libertà di informazione e responsabilità editoriale*; in *Rivista italiana di diritto e procedura penale*, 2012, 1611 ss. con nota di D. Petrini, *Il direttore della testata telematica, tra* horror vacui *e prospettive di riforma; sperando che nulla cambi*. Conferma l'esclusione della responsabilità per omesso controllo del direttore del periodico telematico Cass. pen., sez. V, 28 ottobre 2011, n. 44126, in www.penalecontemporaneo.it, 16 dicembre 2011, con nota di S. Turchetti, *Un secondo "alt" della Cassazione all'applicazione dell'art. 57 c.p. al direttore del periodico on line*; in *Diritto dell'informazione e dell'informatica*, 2011, 795-808, con nota di G. E. Vigevani, *La «sentenza figlia» sul direttore del giornale telematico: il caso Hamaui*; per ulteriori commenti alla sentenza si v. anche il commento di G. Corrias Lucente, *Al direttore responsabile di un periodico on line non si applica il reato previsto dall'art. 57 del codice penale*, in *Diritto dell'informazione e dell'informatica*, 2012, 82 ss.

[4] Per un primo commento di questa sentenza si v. P. Maciocchi, *Il direttore deve togliere il post diffamatorio*, in *Quotidiano del Diritto*, 23 marzo 2018.

[5] Cass.pen., sez. un., 29 gennaio 2015 (dep. 17 luglio 2015), n. 31022, in www.penalecontemporaneo.it, 9 marzo 2016, con nota di C. Melzi d'Eril, *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate on-line registrate.*

estendere l'applicazione della garanzia nei confronti del sequestro, prevista dall'art. 21 Cost., dalla stampa alla rete, ha fornito della prima una nozione "figurata", secondo la quale "stampa" corrisponderebbe all'informazione giornalistica professionale, sia se diffusa su carta stampata o attraverso il web.
Partendo da questo arresto, la Corte, una volta ricondotti i giornali telematici alla nuova nozione di "stampa", ha stabilito che ad essi «si estendono non solo le garanzie costituzionali a tutela della stampa e della libera manifestazione del pensiero previste dall'art. 21 Cost., ma anche le disposizioni volte ad impedire che con il mezzo della stampa si commettano reati, tra le quali particolare rilievo assume il disposto del citato art. 57 c.p.».

2. Il caso concreto

Anticipato il principio di diritto espresso e accennato al dibattito all'interno del quale si inserisce la decisione in commento, pare opportuno soffermarsi in breve sul caso concreto.
Su un periodico registrato era pubblicato un articolo anonimo dal contenuto, a dire della persona offesa, diffamatorio. Poiché l'autore dello scritto non veniva identificato, l'azione penale era esercitata soltanto nei confronti del direttore responsabile.
Dopo la sentenza di condanna emessa dal Tribunale nei confronti dell'imputato per il reato di cui all'art. 595, c. 1, 2 e 3, c.p., la Corte d'appello, dopo aver proceduto alla correzione del capo di imputazione aggiungendo la contestazione di cui all'art. 57 c.p., annullava tale decisione assolvendo l'imputato con la formula perché il fatto non è previsto dalla legge come reato.
Avverso la decisione di secondo grado, proponeva ricorso per cassazione la parte civile costituita, evidenziando *inter alia* che la Corte d'appello avrebbe erroneamente affermato l'inapplicabilità dell'art. 57 c.p. al direttore della testata online.
Più precisamente, i giudici di secondo grado, in linea con quello che all'epoca era l'orientamento univoco e consolidato di legittimità, avevano escluso la responsabilità dell'imputato sulla base del presupposto che, poiché la telematica non è assimilabile alla stampa - cui fa espresso riferimento la disposizione in esame - il divieto di analogia in *malam partem* precludeva una sua estensione al direttore di un periodico online.
Il ricorrente, invece, asseriva che tale procedimento logico fosse smentito dal principio di diritto espresso dalle Sezioni Unite nel 2015 (con la citata sentenza n. 31022) che avevano ricondotto la testata giornalistica telematica alla nozione di "stampa"; sicché i giudici di appello ben avrebbero potuto applicare l'art. 57 c.p., senza che potesse essere ravvisato una violazione del principio di legalità e tassatività.
La Corte di cassazione, in sostanza, segue la tesi della persona offesa, così sconfessando la posizione che essa stessa aveva assunto nel 2010 e mantenuto fino alla decisione *de qua*.

3. Il precedente orientamento della giurisprudenza di legittimità: l'inapplicabilità dell'art. 57 c.p. al direttore del periodico online e, più in generale, della disciplina prevista per la stampa alla rete

Per apprezzare la portata rivoluzionaria della sentenza in commento, non può non essere ricordato quello che era il precedente indirizzo, univoco e (almeno fino ad oggi) mai smentito, della giurisprudenza di legittimità: si riteneva che *de iure condito* al direttore di un giornale pubblicato in rete non fosse possibile estendere il dettato dell'art. 57 c.p, così come di tutte le altre disposizioni espressamente previste per la carta stampata.
Tale orientamento era stato inaugurato dalla prima storica sentenza in materia risalente al 2010[6], con argomenti convincenti.
In particolare, il primo consiste nel principio di tassatività in materia penale, corollario del principio costituzionale di stretta legalità di cui all'art. 25, c. 2, Cost., e quindi nel divieto di analogia in *malam partem*. La Corte prendeva le mosse dalla consapevolezza che «la telematica non è stampa»[7] e ciò perché si riteneva che il tenore letterale della definizione di stampa contenuta all'art. 1 della legge 47/1948, coincidente con «tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione», non fosse in alcun modo suscettibile di ricomprendere i fenomeni presenti in rete[8]. Tale norma, infatti, pone due requisiti indefettibili affinché una pubblicazione possa rientrare nella nozione di stampa, che non è dato rinvenire nelle comunicazioni in rete, vale a dire una riproduzione tipografica e la destinazione alla diffusione al pubblico della stessa. Nel web, manca una vera e propria "riproduzione" in quanto il contenuto è soltanto posto in rete e reso accessibile ai vari utenti mediante tecniche molto diverse rispetto a quelle tipografiche o a esse assimilabili. Data l'impossibilita di ricondurre la rete alla nozione di stampa, in forza del predetto principio costituzionale, la soluzione era obbligata: la norma che punisce l'omesso controllo del direttore della stampa periodica non poteva essere applicata al direttore di un sito diffuso solo online.
Il secondo argomento si basava sull'impossibilità di muovere un rimprovero per una condotta di controllo, imposta dalla citata fattispecie incriminatrice, materialmente inadempibile da parte del direttore sui contenuti pubblicati in rete a fronte della natura interattiva della stessa. In altri termini, si riteneva che l'intrinseca eterogeneità del web

[6] Il riferimento è a Cass. pen., sez. V, 16 luglio 2010, n. 35511, cit., il cui caso è molto noto, così come l'*iter* giudiziario: due politici avevano presentato querela per una lettera anonima ritenuta diffamatoria apparsa su un periodico telematico. Il giudice di primo grado condannava il direttore, imputato del reato di cui all'art. 57 c.p. e, in secondo grado, la Corte d'appello, pur dichiarando di non doversi procedere per intervenuta prescrizione, confermava le statuizioni civili. Avverso tale decisione, proponeva ricorso per cassazione l'imputato e la Corte, ritenendo che il fatto non fosse previsto dalla legge come reato, annullava senza rinvio.

[7] Espressione mutuata da V. Zeno Zencovich, *La pretesa estensione alla telematica del regime della stampa: note critiche*, cit., 27.

[8] Allo stesso modo, è stata altresì esclusa la possibilità di applicare la responsabilità di cui all'art. 57 c.p. al direttore della testata televisiva, proprio per la diversità tra i due mezzi di comunicazione (in questo caso, stampa e TV) e per l'impossibilità di operare una analogia in materia penale. In questo sento, *ex multis*, Cass. pen., sez. II, 23 aprile 2008, n. 34717.

avesse ricadute anche sul ruolo e sull'attività del direttore della testata telematica tali per cui un controllo, come quello posto in essere dal direttore di un giornale cartaceo, fosse in concreto inattuabile[9].

Dopo poco più di un anno dalla sentenza cd. "Brambilla", la Corte di cassazione, con la decisione n. 44126 del 2011 (definita non a caso «sentenza figlia»[10]) aveva modo di ribadire la non configurabilità del reato di omesso controllo nei confronti del direttore del periodico online[11].

A supporto di tale pronuncia, la Corte utilizzava argomentazioni quasi identiche a quelle indicate nella sentenza precedente. Infatti, dopo aver richiamato la decisione emessa dalla stessa sezione l'anno prima, riaffermava la strutturale diversità intercorrente tra giornali cartacei e telematici, nonché la necessità di un'applicazione rigorosa del divieto di analogia in materia penale. Dopodiché, sviluppando in maniera più profonda il secondo argomento[12], ribadiva l'inesigibilità del controllo da parte del direttore di rivista telematica sui contributi ivi pubblicati.

L'elemento di diversità di tale pronuncia rispetto alla decisione dell'anno prima consiste nell'aver cassato il tentativo dei giudici di merito di modificare la configurazione della condotta punita dalla norma incriminatrice. Invero, nel caso in questione, i giudici di Bologna avevano condannato l'imputata per il reato di cui all'art. 57 c.p. non per aver omesso il controllo richiesto da tale disposizione, ma per non aver provveduto a rimuovere lo scritto tempestivamente. Tale costruzione giuridica – che, come si vedrà, sarà in parte ripresa dalla decisione in commento – secondo la Corte comporta non solo un'analogia vietata in materia penale, ma altresì un vero e proprio stravolgimento della norma che sanziona il mancato impedimento della pubblicazione, non già l'omissione di un controllo successivo delle inserzioni già avvenute.

---

[9] Oltre ai commenti indicate alla nota 3, la sentenza n. 35511 del 2010 è stata analizzata, tra i molti, anche da C. Melzi d'Eril, *La complessa individuazione dei limiti alla manifestazione del pensiero in internet*, in *Diritto dell'informazione e dell'informatica*, 2011, 571 ss; A. Papa, *La disciplina della libertà di stampa alla luce delle nuove tecnologie,* in *Diritto dell'informazione e dell'informatica*, 2011, 490-493; A. Bevere-V. Zeno Zencovich, *La rete e il diritto sanzionatorio: una visione d'insieme*, in *Diritto dell'informazione e dell'informatica*, 2011, 380-382; M. Bassini, *La disciplina penale della stampa alla prova di internet: avanzamenti e arresti nella dialettica giurisprudenziale da una prospettiva costituzionale*, cit., 15-21.

[10] Espressione utilizzata da G. E. Vigevani, *La «sentenza figlia» sul direttore del giornale telematico: il caso Hamaui*, cit., 798.

[11] Cass. pen., sez. V, 28 ottobre 2011, n. 44126, cit. Questa la vicenda: dopo che i giudici di merito avevano condannato l'allora direttore della versione web de "L'Espresso" per omesso controllo a causa di un post di un lettore ritenuto diffamatorio, la Cassazione annullava senza rinvio la sentenza impugnata dall'imputata.

[12] Rileva come la Corte in tale pronuncia valorizzi maggiormente l'argomento della inesigibilità della condotta, sia pure accanto al divieto di analogia in campo penale, G. E. Vigevani, *La «sentenza figlia» sul direttore del giornale telematico: il caso Hamaui*, cit., 806 ss.; il passaggio cui si fa riferimento è quello in cui la Corte evidenzia che «non vi è solamente una diversità strutturale tra i due mezzi di comunicazione (carta stampata e Internet), ma altresì la impossibilità per il direttore della testata di impedire la pubblicazione di commenti diffamatori, il che rende evidente che la norma contenuta nell'art. 57 c.p. non è stata pensata per queste situazioni, perché costringerebbe il direttore ad una attività impossibile, ovvero lo punirebbe automaticamente ed oggettivamente, senza dargli la possibilità di tenere una condotta lecita».

In sintesi, questo era l'orientamento giurisprudenziale che si era cristallizzato[13]: escluse le ipotesi di concorso nel reato, il direttore di un giornale online non risponde della responsabilità di cui all'art. 57 c.p. per i contributi inseriti da soggetti terzi, siano essi semplici lettori o giornalisti facenti parte della redazione, anche se rimasti anonimi e a prescindere dal fatto che la testata telematica sia registrata o meno.
Di più, poiché secondo l'indirizzo che era emerso e si era assestato fino al 2015 alla nozione di "stampa" non potevano essere ricondotti i fenomeni che prendono corpo in rete, più in generale, tutte le norme previste per il mezzo tradizionale – sia quelle di favore[14] sia le disposizioni penali sfavorevoli[15] – non erano applicabili alla rete internet.

4. La nuova interpretazione della nozione di "stampa" offerta dalle Sezioni Unite

Come si è visto, l'argomentazione principale che aveva condotto a negare che l'attività del direttore della testata telematica potesse essere ricondotta nell'alveo della fattispecie di cui all'art. 57 c.p., ossia il divieto di analogia in materia penale, aveva quale presupposto indefettibile la riconosciuta intrinseca diversità tra stampa e internet.
Senonché, tutto è parso poter cambiare quando, ritenuto che vi fosse un contrasto giurisprudenziale *inter alia* sulla possibilità di applicare all'informazione online in via estensiva le guarentigie costituzionali previste dall'art. 21 Cost. per la stampa, è stata

[13] L'ultima decisione nello stesso verso risale soltanto a un mese prima di quella in commento. Si tratta di Cass. pen., sez. V, 19 febbraio 2018, n. 7885, con cui la Corte, seppur in *obiter dictum*, ha avuto occasione di riaffermare che all'informazione online non è applicabile l'art. 57 c.p.

[14] In merito alla applicabilità delle disposizioni di favore, nel 2014 la Corte di Cassazione aveva statuito che le garanzie costituzionali previste per gli stampati in tema di sequestro non potessero essere estese agli spazi comunicativi virtuali. Il riferimento è a due decisioni emesse entrambe dalla V sezione a distanza di pochi giorni: la prima, Cass. pen., sez. V, 5 novembre 2013 (dep. 5 marzo 2014), n. 10594, in www.penalecontemporaneo.it, 25 marzo 2014, con nota di C. Melzi d'Eril, *La Cassazione esclude l'estensione delle garanzie costituzionali previste per il sequestro degli stampati*; la seconda, Cass. pen., sez. V, 30 ottobre 2013 (dep. 12 marzo 2014), n. 11895, in www.medialaws.eu, con nota di F. Mazara Grimani, *Il sequestro preventivo di un blog: nuovi orientamenti alla luce della sentenza della Corte di Cassazione n. 11895/2014*. Per un puntuale commento critico di entrambe le decisioni, si v. C. Melzi d'Eril, *Il sequestro dei siti on-line: una proposta di applicazione analogica dell'art. 21 Cost. "a dispetto" della giurisprudenza*, in *Diritto dell'informazione e dell'informatica*, 2014, 153 ss.

[15] Per quanto riguarda le norme di sfavore, oltre al reato di cui all'art. 57 c.p., sempre in forza del divieto di analogia in *malam partem*, era stata esclusa l'applicabilità dell'aggravante prevista dall'art. 13 della legge stampa, nonché del reato di stampa clandestina di cui all'art. 16 della medesima legge. Sull'inestensibilità alla rete dell'art. 13 l. 47/48, tra le molte, si veda la recente Cass. pen., sez. V, 1 febbraio 2017, n. 4873 in *Quotidiano del Diritto,* 2 febbraio 2017, con nota di A. Galimberti, *Diffamazione "attenuata" se via Fb;* in www.penalecontemporaneo.it, 20 aprile 2017, E. Birritteri, *Diffamazione e Facebook: la Cassazione conferma il suo indirizzo ma apre a un'estensione analogica in malam partem delle norme sulla stampa*; in *Forum di Quaderni Costituzionali*, 14 aprile 2017, con nota di M. Tresca, *Il diritto di informazione nell'era digitale: la complessa equiparazione tra stampa tradizionale e media on line*; nonché, volendo C. Melzi d'Eril-S. Vimercati, *Diffamazione, Facebook non è stampa*, in *Il Sole 24 Ore online*, 8 febbraio 2017. Sull'inapplicabilità del reato di stampa clandestina di cui all'art. 16 della l. 47/1948 a un blog non registrato si veda Cass. pen., sez. III, 10 maggio 2012, n. 23230, in www.penalecontemporaneo.it, 8 ottobre 2012, con nota di F. Piccichè, *Giornali on line e reato di stampa clandestina*; in *Diritto dell'informazione e dell'informatica*, 2012, 1118, con nota di P. Di Fabio, *Blog, giornali on line e «obblighi facoltativi» di registrazione delle testate telematiche: tra confusione del legislatore e pericoli per la libera espressione del pensiero su internet*.

rimessa la questione alle Sezioni Unite[16], che hanno avuto modo di occuparsi più in generale della disciplina applicabile alle manifestazioni del pensiero in rete.

La Corte, nel risolvere i quesiti sottopostile, per quel che qui interessa, con sentenza n. 31022 del 2015[17], ha sancito che «la testata giornalistica telematica, in quanto assimilabile funzionalmente a quella tradizionale, rientra nel concetto ampio di 'stampa' e soggiace alla normativa, di rango costituzionale e di livello ordinario, che disciplina l'attività d'informazione professionale diretta al pubblico».

Per affermare tale principio di diritto, punto di partenza, da cui muove la Corte, è la situazione di tensione con il principio di uguaglianza determinata dall'irragionevole trattamento differenziato dell'informazione veicolata su carta stampata rispetto a quella diffusa in rete, in quanto soltanto la seconda, non beneficiando delle predette garanzie, sarebbe assoggettabile a sequestro preventivo. In altri termini, a detta della Cassazione, si correrebbe il rischio di porre in essere trattamenti differenziati a due fattispecie, giornali online e cartacei, sotto il profilo funzionale di diffusione dell'informazione professionale, assai simili.

E proprio allo scopo di scongiurare una simile tensione, la Corte offre una nuova definizione del termine "stampa" contenuta nell'art. 21 Cost. e nell'art. 1 della legge 47/1948. In particolare, secondo la Cassazione, in coerenza con il progresso tecnologico, è necessario attribuire alla nozione di stampa un differente significato: essa, intesa in senso "figurato", corrisponderebbe all'informazione giornalistica professionale, sia se diffusa su carta stampata o attraverso il web. In altri termini, la Corte sceglie di «discostarsi dall'esegesi letterale del dettato normativo e privilegiare una interpretazione estensiva dello stesso», ricomprendendo nel termine "stampa" anche le testate online registrate.

Da qui, una volta introdotto tale nuovo concetto di stampa, le Sezioni Unite hanno stabilito che, tra i vari strumenti di comunicazione telematici, solo i giornali online regi-

[16] Cass. pen., sez. I, ord. 3 ottobre 2014 (dep. 30 ottobre 2014), n. 45053, in www.penalecontemporaneo.it, 21 gennaio 2015, con nota di M. Mariotti, *Rimessa alle Sezioni Unite la questione sull'ammissibilità del sequestro preventivo, mediante oscuramento, di un sito web di una testata giornalistica.*

[17] Cass. pen., sez. un., 29 gennaio 2015 (dep. 17 luglio 2015), n. 31022, cit. Oltre al saggio indicato alla nota 5, per ulteriori commenti a tale decisioni si v. P. Caretti, *La Cassazione pone, meritoriamente, alcuni punti fermi in tema di regolazione dell'informazione via internet*, in *Quaderni costituzionali*, 2015, 1013 ss.; in *Processo penale e giustizia*, 2015, 78, con nota di A. Pulvirenti, *Sequestro e Internet: dalle Sezioni Unite una soluzione equilibrata ma "creativa"*; in *Cassazione penale*, 2015, 3454 ss., con nota di L. Paoloni, *Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa:* ubi commoda, ibi et incommoda*?*; in www.medialaws.eu, 17 maggio 2016, con nota di A. Regi, *Le Sezioni Unite si pronunciano sull'applicabilità delle garanzie costituzionali in tema di sequestro preventivo alle testate telematiche registrate*; in *Guida al diritto*, 2015, n. 38, 82 ss., con nota di C. Melzi d'Eril-G. E. Vigevani, *Il sequestro di una pagina web può essere disposto imponendo al service provider di renderla inaccessibile*; in *Diritto penale e processo*, 2015, 2002 ss., con nota di S. Lorusso, *Un'innovativa pronuncia in tema di sequestro preventivo di testata giornalistica on line*; in *Diritto dell'informazione e dell'informatica*, 2015, 1041 ss., con nota di G. Corrias Lucente, *Le testate telematiche registrate sono sottratte al sequestro preventivo. Qualche dubbio sulla "giurisprudenza legislativa".*

strati, in quanto coincidenti sotto i profili strutturale e funzionale a quelli tradizionali[18], sono soggetti alla normativa ordinaria e costituzionale specificatamente prevista per i secondi e beneficiano delle garanzie costituzionali in materia di sequestro preventivo.

5. La svolta della Cassazione: l'applicabilità dell'art. 57 c.p. al direttore del giornale online

Dato conto del precedente orientamento della giurisprudenza e dell'approdo delle Sezioni Unite sul concetto di stampa, passiamo ora all'analisi della sentenza in commento. Quale sia la portata rivoluzionaria di tale decisione lo si è già indicato: l'art. 57 c.p. può essere applicato al direttore responsabile della testata telematica registrata.
Vediamo allora il percorso motivazionale che la Corte ha seguito per giungere a tale conclusione e superare il proprio precedente indirizzo, considerato univoco e granitico.
La Cassazione, come si è anticipato, prende le mosse dalla sentenza delle Sezioni Unite del 2015 e dalla nuova nozione di "stampa" introdotta sulla base di una interpretazione asseritamente evolutiva. Richiamando espressamente tale arresto, ribadisce che il termine "stampa", in senso figurato, indicherebbe i giornali, siano essi cartacei o telematici. Pertanto, ogni giornale, anche se diffuso con strumenti differenti da quelli tipografici, sarebbe riconducibile alla nozione di stampa e soggetto allo statuto previsto per la stessa, purché contraddistinto da una testata, dotato di un direttore responsabile, registrato presso il tribunale e diffuso con periodicità regolare.
Da qui, poi, la Corte compie il salto: alle testate giornalistiche telematiche, in quanto strumenti informativi che rientrano nell'alveo della inedita definizione di stampa, si applicano non solo le garanzie costituzionali in materia di sequestro, ma l'intera disciplina di rango costituzionale e ordinario prevista per gli stampati, ivi comprese tutte le fattispecie incriminatrici, tra le quali appunto la responsabilità del direttore per l'omesso controllo prevista dall'art. 57 c.p.
E su un simile radicale ripensamento posto in essere con tale pronuncia i giudici di legittimità non danno spazio a dubbi di nessuna sorta, affermando esplicitamente che «risulta, pertanto, superato il contrario orientamento della giurisprudenza di legittimità, che escludeva la responsabilità del direttore di un periodico on-line per il reato di omesso controllo, *ex* art. 57 c.p.».
Ciò premesso, la Corte va oltre sostenendo che, benché l'articolo fosse stato pubblicato privo di firma, la sua collocazione nel corpo della testata doveva indurre a ritenere

[18] La Corte in tale decisione traccia uno spartiacque tra i fenomeni che prendono corpo in rete, precisando che l'interpretazione evolutiva del concetto di stampa riguarda solo ed esclusivamente le testate online registrate, mentre ne resta escluso il «vasto ed eterogeneo ambito della diffusione di notizie ed informazioni da parte di singoli soggetti in modo spontaneo», vale a dire blog, forum e social network. Seguendo pedissequamente quanto statuito dalle Sezioni Unite, l'anno successivo le sezioni semplici, con la sentenza Cass. pen., sez. V, 24 marzo 2016, n. 12536, hanno stabilito che, a differenza delle testate telematiche registrate, ai blog non si estendono le garanzie in tema di sequestro accordate agli stampati in quanto ritenuti non riconducibili alla nozione di "stampa". Per un commento a tale decisione, volendo, si v. S. Vimercati, *La Cassazione conferma l'inestensibilità ai blog delle garanzie costituzionali per gli stampati in tema di sequestro*, in www.penalecontemporaneo.it, 26 ottobre 2016. Nel medesimo senso, si veda anche la recentissima Cass. pen., sez. V, 15 maggio 2018, n. 21521 commentata da P. Maciocchi, *Diffamazione sì, al sequestro preventivo della pagina Facebook*, in www.ilsole24ore.com, 16 maggio 2018.

che non fosse stato inserito da un semplice utente, ma si trattasse di un contributo proveniente da un soggetto facente parte della redazione del giornale; il che, a suo dire, lasciava «presumere, infatti, la possibilità da parte del direttore responsabile di operare un controllo preventivo».
Da ultimo, la Cassazione prosegue osservando che, quand'anche si dovesse accertare che il direttore del periodico online non avesse avuto la concreta possibilità di controllare preventivamente il contenuto dell'articolo, ciò comunque non escluderebbe una sua responsabilità – che potrebbe «atteggiarsi, indifferentemente, a titolo di colpa, *ex* art. 57 c.p., o di concorso *ex* art. 110, nel reato di diffamazione» – per non aver rimosso il contenuto illecito. E ciò, a detta dei giudici di legittimità, senza che si possa sostenere nel primo caso che si stia ponendo in essere una modifica della fattispecie incriminatrice di cui all'art. 57 c.p., in quanto la condotta di controllo del direttore dovrebbe essere effettuata non solo al momento dell'inserimento in rete dei contributi, ma anche successivamente, durante la loro permanenza tra le colonne del giornale telematico.
Da qui, dunque, l'annullamento con rinvio della sentenza impugnata che invece aveva escluso la responsabilità del direttore della testata online.

6. Alcune considerazioni critiche sulla nuova interpretazione della nozione di "stampa" e sulle conseguenze della equiparazione giuridica tra testate telematiche e tradizionali

Conclusa l'analisi dell'orientamento giurisprudenziale precedente e reso noto il contenuto della motivazione della sentenza in commento, merita ora svolgere alcune riflessioni critiche sia sul presupposto logico della stessa, ossia l'interpretazione asseritamente evolutiva del concetto di stampa, sia sulle conseguenze tratte dalla Corte in ambito penale e in punto di applicabilità del delitto previsto dall'art. 57 c.p.
La prima attiene all'inedita nozione di stampa introdotta dalle Sezioni Unite tre anni orsono che, lo si è già precisato, in senso figurato abbraccerebbe non più soltanto le riproduzioni effettuate con mezzi tipografici, meccanici o fisico-chimici destinate alla pubblicazione – come vorrebbe la lettera dell'art. 1 della cd. legge stampa –, ma i giornali in generale, siano essi cartacei o telematici.
Una simile ricostruzione ermeneutica non appare convincente per almeno due ordini di ragioni. In primo luogo, non sembra essere corretto l'assunto di base, ossia che in origine la nozione di stampa coincidesse con i soli giornali cartacei[19]. Invero, tale definizione, benché comprenda certamente anche questi ultimi, si riferisce storicamente a qualsiasi altro stampato, come manifesti, volantini, libri e ciò a prescindere dall'attività

[19] Fra i primi a individuare tale errore interpretativo C. Melzi d'Eril, *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate online registrate*, cit., 11.

svolta o dal tipo di informazione veicolata[20]. In secondo luogo, appare errato ricondurre nella definizione di stampa l'informazione online attraverso una attività interpretativa che sembra forzare il dettato dell'art. 1 della legge stampa. Tale norma, invero, pone due requisiti imprescindibili affinché una pubblicazione possa essere considerata stampa, ovvero una riproduzione tipografica e la destinazione alla diffusione al pubblico della stessa; requisiti che – come rilevato anche dall'orientamento giurisprudenziale precedente – non si rinvengono nei contributi immessi in rete.

Non solo, anche i riferimenti normativi utilizzati dalle Sezioni Unite per avvalorare il tentativo di equiparazione dell'informazione online a quella cartacea appaiono non idonei: ne costituisce un esempio il preteso impatto che avrebbe avuto la legge n. 62/2001, che aveva introdotto la nozione di "prodotto editoriale"[21]. Invero superati i primi dubbi interpretativi[22], da tempo si era escluso che tale normativa comportasse l'estensione all'editoria online delle norme relative alle indicazioni obbligatorie sugli stampati e all'obbligo di registrazione delle testate giornalistiche e dei periodici. Suddetta disciplina, infatti, lungi dall'aver equiparato stampa e web, ha carattere settoriale ed è stata adottata al solo scopo di estendere ai contenuti virtuali le provvidenze previste per l'editoria. Peraltro, la bontà di questa interpretazione è stata avvalorata dallo stesso legislatore che, fornendo una sorta di interpretazione autentica della normativa del 2001, con il d. lgs. 70/2003, all'art. 7, c. 3 ha chiarito che non vi è alcun obbligo di registrazione per le testate telematiche, essendo al contrario un mero onere per poter usufruire dei benefici previsti per l'editoria tradizionale[23].

Ciò premesso, tale interpretazione evolutiva del concetto di stampa era stata introdotta

[20] Peraltro, ciò trova conferma nello stesso dettato dell'art. 21 della Costituzione che al c. 3 pone garanzie (quelle cioè di cui si discute) a tutela indistintamente di tutti gli stampati, siano essi comuni oppure periodici, mentre al c. 4 si riferisce espressamente alla sola stampa periodica. In particolare, quest'ultima disposizione, in deroga alla riserva di giurisdizione, attribuisce agli ufficiali di polizia giudiziaria il potere di disporre il sequestro della sola stampa periodica, che entro ventiquattro ore deve essere denunziato all'autorità giudiziaria e nelle successive ventiquattro ore deve essere da questa convalidato. In altri termini, dunque, la stampa periodica gode addirittura di una tutela più debole rispetto agli stampati comuni. Sul punto si v. A. Pace - M. Manetti, *Rapporti civili, La libertà di manifestazione del pensiero*, cit., 56 e 770.

[21] La l. 62/2001 all'art. 1, rubricato "definizione e disciplina del prodotto editoriale", al primo comma dispone: «Per 'prodotto editoriale', ai fini della presente legge, si intende il prodotto realizzato su supporto cartaceo, ivi compreso il libro, o su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico, o attraverso la radiodiffusione sonora o televisiva, con esclusione dei prodotti discografici o cinematografici». A suddetto articolo, con la l. 198/2016 all'art. 3, c. 4, lett. *c)*, è stato aggiunto il c. 3 *bis* ove oggi si rinviene la definizione di "quotidiano online", ovverosia «quella testata giornalistica: a) regolarmente registrata presso una cancelleria di tribunale; b) il cui direttore responsabile sia iscritto all'Ordine dei giornalisti, nell'elenco dei pubblicisti ovvero dei professionisti; c) che pubblichi i propri contenuti giornalistici prevalentemente on line; d) che non sia esclusivamente una mera trasposizione telematica di una testata cartacea; e) che produca principalmente informazione; f) che abbia una frequenza di aggiornamento almeno quotidiana; g) che non si configuri esclusivamente come aggregatore di notizie».

[22] Per una prima puntuale analisi di tale intervento normativo si veda V. Zeno-Zencovich, *I «prodotti editoriali» elettronici nella l. 7 marzo 2001 n. 62 e il preteso obbligo di registrazione*, in *Diritto dell'informazione e dell'informatica*, 2001, 153 ss.

[23] Sul punto, si veda A. Pace - M. Manetti, *Rapporti civili. La libertà di manifestazione del pensiero*, Bologna, 2006, 524 ss.; M. Cuniberti, *Disciplina della stampa e dell'attività giornalistica e informazione in rete*, in Id. (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Milano, 2008, 215 ss.; S. Seminara, *Internet (diritto penale)*, in *Enciclopedia del diritto*, *Annali*, vol. VII, Milano, 2014, 585 ss..

– o almeno così sembrava dedursi dalla lettura della sentenza delle Sezioni Unite – allo scopo di risolvere una intollerabile disparità di trattamento tra informazione cartacea e quella diffusa tramite giornali online e quindi di evitare una lesione del principio di uguaglianza. Tuttavia, se pure pare comprensibile la volontà di porre rimedio a un simile *vulnus* e in linea di massima apprezzabile l'estensione delle garanzie dell'art. 21, c. 3, Cost. dai giornali cartacei a quelli telematici, non erano esenti da critiche tanto il metodo esegetico utilizzato a tal fine dalle Sezioni Unite quanto il rischio che una equiparazione indiscriminata tra informazione stampata e online potesse aprire la strada all'applicazione della intera disciplina prevista per la prima alla seconda, e non dunque solo delle garanzie.

In questa prospettiva, non pochi autori avevano, infatti, rilevato come – benché la sovrapposizione tra giornali cartacei e online dovesse essere valutata in connessione con la specifica questione affrontata nella citata sentenza, ossia l'applicabilità anche ai secondi delle garanzie di cui all'art. 21, c. 3, Cost. – tra le righe della motivazione potesse annidarsi il rischio dell'estensione, oltre che delle disposizioni di favore, anche di quelle incriminatrici[24]. Ebbene, con la pronuncia in commento la Cassazione ha trasformato in realtà proprio quei timori espressi dai commentatori all'indomani della decisione delle Sezioni Unite, dimostrando che fossero tutt'altro che preoccupazioni peregrine.

Il punto di arrivo della decisione annotata lo si è già precisato: poiché il giornale telematico è riconducibile alla nuova nozione di stampa, al soggetto che lo dirige può essere attribuita la responsabilità per omesso controllo prevista dall'art. 57 c.p. per il direttore del periodico cartaceo.

Simile approdo è stato evidentemente reso possibile dall'impianto ermeneutico prescelto dalle Sezioni Unite nel 2015: la nozione attribuita al concetto di "stampa" è l'esito non già di un'operazione analogica, ma di una più volte dichiarata interpretazione estensiva ed evolutiva[25]. Sicché, prendendo per buona tale impostazione, l'applicazione all'informazione professionale in rete delle fattispecie incriminatrici stabilite per la stampa non violerebbe il divieto di analogia in *malam partem*, vale a dire quel principio sul quale fino ad oggi la giurisprudenza faceva leva per escludere ogni indebita estensione.

Ebbene, qui batte il cuore del problema: l'opzione esegetica posta in essere dal Su-

[24] Tra i primi a esprimere considerazioni particolarmente critiche rispetto alle conseguenze in ambito penale che sarebbero potute discendere dalla assimilazione giuridica delle testate telematiche a quelle tradizionali v. C. Melzi d'Eril, *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate online registrate*, cit., 9; nello stesso senso, L. Paoloni, *Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa:* ubi commoda, ibi et incommoda*?*, cit., 3472; cfr. G. Corrias Lucente, *Le testate telematiche registrate sono sottratte al sequestro preventivo. Qualche dubbio sulla "giurisprudenza legislativa"*, cit., 1051; volendo v. anche S. Vimercati, *La Cassazione conferma l'inestensibilità ai blog delle garanzie costituzionali per gli stampati in tema di sequestro*, cit., 11-12.

[25] Sul punto, Cass. pen., sez. un., 29 gennaio 2015 (dep. 17 luglio 2015), n. 31022, cit, osserva espressamente che «l'interpretazione estensiva, se coerente con la *mens legis* – nel senso che ne rispetta lo scopo oggettivamente inteso, senza porsi in conflitto con il sistema giuridico che regola il settore d'interesse – consente di discostarsi dalla definizioni legali, le quali sono semplici generalizzazioni destinate ad agevolare l'applicazione della legge in un determinato momento storico, e di accreditare al dato normativo un senso e una portata corrispondenti alla coscienza giuridica e alle necessità sociali del momento attuale».

premo consesso, a parere di chi scrive, parrebbe invece discendere non da un'interpretazione estensivo-evolutiva, bensì proprio da un'operazione analogica che ben può giustificare l'estensione di norme di favore (quali appunto le garanzie costituzionali in materia di sequestro degli stampati), ma non invece quella di disposizioni sfavorevoli, pena la violazione del divieto del divieto di analogia in campo penale. E tale convinzione discende dalla circostanza che il disposto dell'art. 1 della legge stampa è chiaro nell'esigere la tipografia quale modalità tecnica di riproduzione, che invece nell'informazione in rete è senza dubbio assente. Dunque, la riconduzione del giornalismo telematico al concetto penalmente rilevante di "stampa" è un'operazione che implica una forzatura della lettera della legge così profonda che non può ritenersi frutto di una semplice interpretazione estensiva, proprio perché sembra essere stato superato il significato proprio della norma.

Ora, per quanto l'impianto di fondo della motivazione delle Sezioni Unite e alcune ambiguità ivi contenute potessero condurre all'esito cui è giunta la quinta sezione con la sentenza qui annotata, residuano comunque alcune perplessità dovute all'automaticità che caratterizza l'*iter* argomentativo. Sembra infatti che l'approdo raggiunto dalla Corte sull'ambito di applicazione dell'art. 57 c.p. venga presentato come la piana conseguenza di quanto statuito dalle Sezioni Unite; in altri termini, sembra darsi per scontato che la nozione di stampa contenuta nell'art. 57 c.p. e quella di cui all'art. 1 l. 47/48 siano del tutto sovrapponibili. Di qui un interrogativo: una volta accolta una nuova interpretazione della definizione di stampa prevista dalla l. 47/1948, è così certo che si debba considerare automaticamente modificata anche la nozione di stampa periodica della fattispecie incriminatrice *de qua*? Il quesito offre, se non risposte chiare, almeno due spunti di riflessione.

Il primo riguarda la circostanza che il delitto in questione (seppur oggetto di una modifica successiva)[26] esisteva nel nostro ordinamento ben prima dell'approvazione della legge stampa, con l'evidente conseguenza che, se il ragionamento della Corte fosse corretto, dovremmo ritenere possibile che l'interpretazione di una disposizione successiva di rango ordinario (quale è l'art. 1 legge stampa) abbia la forza di modificare in modo automatico una preesistente di pari livello, senza che ciò sia espressamente stabilito dal legislatore e per di più estendendo l'area della punibilità.

Il secondo attiene all'ancoraggio costituzionale. Le Sezioni Unite erano state spinte a introdurre una nuova nozione di stampa per superare un possibile contrasto con il principio di uguaglianza e, considerata la sempre maggior diffusione dell'informazione in rete, per evitare il rischio che una garanzia costituzionale subisse una profonda contrazione laddove si fosse continuato ad applicarla alla sola informazione cartacea. Al contrario, la scelta operata con la sentenza in commento non trova giustificazione nell'esigenza di dare piena attuazione ad alcun presidio costituzionale in quanto non è previsto alcun obbligo in capo al legislatore di attribuire una responsabilità al direttore di un giornale.

E se ciò non bastasse, almeno per quanto riguarda il delitto di cui all'art. 57 c.p. permane comunque il problema della inesigibilità della condotta da parte del direttore del periodico online. Invero, resta ancora oggi pienamente condivisibile la considerazione

[26] La formulazione attuale dell'art. 57 c.p. è stata introdotta con l. 127/1958.

svolta dai giudici di legittimità nelle precedenti decisioni in merito alla inattuabilità di una condotta di controllo in rete come quella posta in essere da chi dirige un periodico cartaceo. Infatti, porre in capo al direttore di un giornale telematico il dovere di controllare tutto ciò che entra nel sito significa richiedere una prestazione inesigibile, se si considerano i continui aggiornamenti, l'interazione dei lettori e il fatto che, a differenza dei giornali cartacei non c'è un momento in cui il direttore ha davanti a sé l'intero giornale su cui poter svolgere il controllo richiesto per poi dare il via libera e mandarlo in stampa[27]. Di conseguenza l'imposizione anche per l'informazione online di tale controllo, che evidentemente era stato a suo tempo concepito in base alle caratteristiche dei periodici cartacei, porterebbe con sé il rischio di scivolare indebitamente verso una responsabilità di tipo oggettivo, trattandosi di una condotta materialmente impossibile. Suddetta questione, a ben vedere, non pare sfuggire alla Corte che, nel tentativo di attribuire una qualche forma di responsabilità penale al direttore del giornale telematico si spinge a delinearne una inedita, richiedendo che il controllo rispetto alla diffusione del contributo illecito avvenga non *ex ante*, ma *ex post*. La Cassazione, infatti, consapevole quantomeno delle difficoltà tecniche, giunge ad affermare che, qualora si accerti l'impossibilità di svolgere un controllo preventivo, il direttore potrebbe comunque essere chiamato a rispondere del reato di cui all'art. 57 c.p. per non averlo svolto successivamente all'inserimento dello scritto illecito provvedendo alla sua tempestiva rimozione. In altri termini, se il controllo imposto dalla legge risultasse impossibile prima della diffusione del contenuto illegale, esso andrebbe svolto in un momento successivo attraverso la sua eliminazione.

Una interpretazione esegetica di questo genere non è nuova; la Corte di cassazione, tuttavia, in passato aveva avuto modo di porre un solido argine ai tentativi di alcuni giudici di merito di determinare una sostanziale modifica della fattispecie normativa prevista dall'art. 57 c.p. che conduceva a sanzionare una condotta diversa da quella tipizzata dal legislatore[28].

L'impostazione accolta dalla decisione *de qua* (e invece stigmatizzata in precedenza) sembrerebbe distorcere la lettera e la *ratio* della disposizione incriminatrice che, lo si ribadisce, prevede un controllo che precede la diffusione dello stampato e non impone al contrario alcuna condotta successiva alla pubblicazione[29]. Non sarebbe invero pensabile un controllo sugli stampati collocato in un momento successivo alla loro diffusione, in quanto una volta mandati in stampa e immessi nel circuito informativo, certamente

[27] In questo senso le considerazioni di C. Melzi d'Eril, Roma locuta*: la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica on-line*, cit., 904 ss.

[28] Ci si riferisce alla già menzionata Cass. pen., sez. V, 28 ottobre 2011, n. 44126, cit. ove la Corte aveva censurato il tentativo dei giudici di primo e secondo grado di attribuire una responsabilità al direttore di un giornale telematico per l'omesso controllo successivo all'inserimento dello scritto ritenuto diffamatorio.

[29] A tal proposito, si segnala che in giurisprudenza di recente non sono mancati tentativi di attribuire una qualche forma di responsabilità al gestore di un sito web per la mancata rimozione di scritti illeciti creati e inseriti in rete da soggetti terzi. La Cassazione, infatti - in Cass. pen., sez. V, 14 luglio 2016, n. 54946 – ha confermato la condanna del titolare di un blog per concorso nel reato di diffamazione con l'autore del contributo a causa della mancata tempestiva cancellazione dello scritto ritenuto diffamatorio. Per un commento a tale decisione, che non è certo rimasta immune da critiche, si v. C. Melzi d'Eril, *Una pronuncia problematica in tema in tema di responsabilità del gestore del sito per i commenti dei lettori*, in questa *Rivista*, 1, 2017, 165 ss.

non potrebbero essere oggetto di alcuna forma di rimozione; il che, peraltro, dà ulteriore dimostrazione del fatto che solo per tale mezzo di comunicazione è pensata e configurata dal legislatore la responsabilità per omesso controllo del direttore.
A ciò si aggiunga che nel nostro ordinamento, *de iure condito*, nemmeno a mente di altre disposizioni può ritenersi sussistente un obbligo in capo al direttore responsabile di un giornale telematico di eliminare dal sito i contributi offensivi. Invero, non solo non è possibile ricavare tale dovere dall'art. 57 c.p., ma nemmeno è possibile riconoscere in capo allo stesso una posizione di garanzia ai sensi dell'art. 40, c. 2, c.p. E ciò perché la possibilità di fondare una responsabilità in virtù di tale ultimo articolo è esclusa dall'assenza di una specifica disposizione, impositiva dell'obbligo di impedire l'evento, che si combini con la clausola generale ivi contenuta.
In definitiva, se pure la soluzione accolta dalla decisione annotata muove dell'esigenza di evitare una tensione con il principio di uguaglianza applicando la medesima disciplina a due strumenti – giornali cartacei e telematici – sotto non pochi profili assai simili, essa sembra tuttavia porsi in insanabile contrasto con un altro principio costituzionale, vale a dire quello di tassatività e determinatezza di cui all'art. 25, c. 2, Cost.
Peraltro, una strada per non incorrere in una simile tensione e, al contempo, evitare di mandare esente da responsabilità il direttore della testata telematica a ben vedere esisteva. Si sarebbe infatti potuto indicare quale via percorribile quella di far rispondere l'imputato del reato di diffamazione, in concorso con l'autore dell'articolo rimasto anonimo, ai sensi degli artt. 110 e 595 c.p.[30], evitando così di dover ricorrere all'estensione della fattispecie di cui all'art. 57 c.p. Alla Corte, come anticipato, non sfugge tale ipotesi, ma pare cadere in errore laddove la indica come una alternativa *sic et sempliciter* alla responsabilità per omesso controllo[31], omettendo che diverso è l'elemento soggettivo (nel primo caso il dolo e nel secondo la colpa) nonché differente è la condotta punita (nel primo caso la compartecipazione alla commissione del reato di natura materiale o morale e nel secondo l'omesso controllo); tanto che, come è noto, diverso è altresì il trattamento sanzionatorio.
La sensazione, invece, è che la Corte, prediligendo una soluzione che si potrebbe definire di "giustizia sostanziale", abbia seguito un percorso logico-giuridico sganciato da quei criteri interpretativi rigorosi che presidiano l'applicazione delle disposizioni penali; in altri termini, tale pronuncia si espone alla critica di porsi al di là del ruolo nomofilattico riconosciuto alla Cassazione, proponendo un'interpretazione della disposizione incriminatrice talmente disancorato dal testo da scivolare verso la funzione legislativa.

[30] Ciò a patto che in concreto possano ritenersi sussistenti i presupposti per ipotizzare il concorso del direttore nel reato di diffamazione con l'autore dello scritto. A tal proposito la Cassazione, decidendo della responsabilità del direttore relativa a uno scritto pubblicato con uno pseudonimo, ha avuto modo di precisare che, quando manca la prova diretta del suo coinvolgimento nel reato, l'esistenza del concorso deve essere ancorata alla presenza di alcuni elementi, quali il contenuto dello scritto, la sua correlazione con il contesto sociale dal quale trae ispirazione, la forma dell'esposizione, l'evidenza e la collocazione tipografica ad esso assegnata nello stampato; il riferimento è a Cass. pen., sez. V, 26 settembre 2012, n. 41249 in www.penalecontemporaneo.it., 28 novembre 2012, con nota di C. Melzi d'Eril, *La condanna per diffamazione nei confronti di Sallusti: un paio di spunti, oltre le polemiche.*

[31] Nella sentenza annotata, la Corte espressamente si riferisce a una responsabilità del direttore della testata telematica che può «atteggiarsi, indifferentemente, a titolo di colpa, *ex* art. 57 c.p., o di concorso *ex* art. 110, c.p., nel reato di diffamazione».

Invero si ritiene che, allo stato, solo il legislatore, in quanto unico soggetto cui compete individuare l'area del punibile, cosicché ai cittadini sia garantita la prevedibilità dei precetti penali, potrebbe imporre una qualche forma di controllo al direttore online, assistita da una sanzione penale; tuttavia, in assenza di un simile intervento normativo che introduca disposizioni testuali concepite per la rete, e dunque adeguate alle sue caratteristiche e alle condotte che materialmente si possono chiedere agli operatori online, non dovrebbero poter trovare cittadinanza i tentativi di allargare l'area del penalmente rilevante a fenomeni che non sono riconducibili al dettato delle disposizioni incriminatrici.

La posta elettronica è sempre un "mezzo di pubblicità"?

Iolanda Campolo

Corte di Cassazione, sez. V penale, 20 settembre 2017, n. 311

Integra il reato di diffamazione aggravato ai sensi dell'art. 595, c. 3, c.p. (offese recate con la stampa o con qualsiasi altro mezzo di pubblicità), la diffusione di espressioni offensive attraverso un messaggio di posta elettronica indirizzato a una pluralità di destinatari.

Sommario

1. Il caso. – 2. L'aggravante di cui all'art. 595, c. 3, c.p. – 3. Dubbi interpretativi.

Keywords: Aggravante, Altro mezzo di pubblicità, Diffamazione, E-mail, Pluralità di destinatari

1. Il caso

Con la sentenza qui commentata la V sezione della Corte di Cassazione ha annullato una sentenza di condanna emessa dal Tribunale di Chieti (nella sua veste di giudice dell'impugnazione avverso una pronuncia del giudice di pace) per il delitto di diffamazione "semplice" ai danni di un titolare di un'autoscuola. Costui era stato fatto oggetto, presumibilmente da parte di un collega, di taluni giudizi offensivi veicolati in un messaggio di posta elettronica inviato a tutti gli appartenenti a un consorzio di autisti professionali; consorzio di cui facevano parte sia lo stesso imputato che la persona offesa. L'annullamento del Supremo Collegio, con conseguente trasmissione degli atti alla Procura della Repubblica competente, nasce dalla ritenuta incompetenza per materia del Giudice di pace, dovendo ritenersi il fatto di diffamazione in questione aggravato ai sensi del terzo comma dell'art. 595 c.p. (offese recate con la stampa o con qualsiasi altro mezzo di pubblicità) per essersi il reato consumato a mezzo di un messaggio di posta elettronica.

Uno strumento, quest'ultimo, «di pubblicità di notevolissima capacità diffusiva», per usare le parole della Corte di Cassazione.

La motivazione della sentenza è piuttosto scarna e si limita pressoché soltanto alla sopra citata affermazione di principio. Non è possibile, quindi, attraverso il solo testo della pronuncia ricostruire come si sia sviluppata l'istruttoria nelle fasi di merito e quali esiti abbia avuto.

Certo è che il principio di diritto espresso – forse un po' troppo stringatamente – nella

decisione qui commentata, sembra affermare che l'uso della posta elettronica integri di per sé sempre l'aggravante del mezzo di pubblicità. Tale conclusione, nella sua sinteticità che le conferisce una certa assolutezza, merita qualche ulteriore e più approfondita riflessione.

2. L'aggravante di cui all'art. 595, c. 3, c.p.

Il terzo comma dell'art. 595 c.p. prevede un'aggravante ad effetto speciale[1] per il caso in cui l'offesa venga recata «col mezzo della stampa o con qualsiasi altro mezzo di pubblicità».

Le ragioni che sono alla base dell'aumento di pena allorché la condotta diffamatoria venga perpetrata con il mezzo della stampa ovvero con altri mezzi di pubblicità, pur nella diversità oggettiva delle due ipotesi, risiedono nel maggior danno che si presume derivi al soggetto passivo a causa della peculiare capacità diffusiva del mezzo adoperato[2].

In particolare, il legislatore ritiene meritevoli di un inasprimento del trattamento sanzionatorio le offese recate con qualunque mezzo che sia suscettibile di determinare un'ampia e indiscriminata diffusione del messaggio diffamatorio tra un numero indeterminato di persone.

Tralasciando in questa sede ogni riflessione sui confini della nozione di "stampa" che non rileva nell'ambito della vicenda processuale commentata, il concetto di "altro mezzo di pubblicità", di per sé assai generico come spesso accade con le norme di chiusura, non ha una definizione normativa ed è intrinsecamente più ambiguo del primo.

Secondo l'interpretazione consolidata, costituisce "mezzo di pubblicità" qualunque strumento in grado di consentire una particolare e spiccata circolazione dell'offesa. In quanto tale, esso è suscettibile di provocare un più sensibile pregiudizio al soggetto passivo.

La giurisprudenza, sia di merito che di legittimità, ha evocato in passato tale aggravante con riferimento alle offese arrecate all'interno di un pubblico comizio o più in generale nei discorsi pubblici, le circolari dirette a numerose persone indeterminate, le rappresentazioni cinematografiche. Prima dell'intervento della l. 14 aprile 1975, n. 103 e successivamente della l. 6 agosto 1990, n. 223[3] – recanti la disciplina del sistema

[1] In casi siffatti la diffamazione viene punita con la pena della reclusione da sei mesi a tre anni o della multa non inferiore a € 516, con conseguente competenza per materia riservata al Tribunale.

[2] Cfr. Cass. pen., sez. I, 2 dicembre 2016, n. 50 in punto diffusione di un messaggio diffamatorio attraverso l'uso di Facebook: «…trattasi di una condotta potenzialmente capace di raggiungere un numero indeterminato o comunque qualitativamente apprezzabile di persone; l'aggravante dell'uso di un mezzo di pubblicità nel reato di diffamazione trova infatti la sua ratio nell'idoneità del mezzo utilizzato a coinvolgere e raggiungere una vasta platea di soggetti, ampliando – e aggravando – in tal modo la capacità diffusiva del messaggio lesivo della reputazione della persona offesa…secondo la logica e la funzione propria dello strumento di comunicazione e condivisione telematica».

[3] L'art. 30, c. 4, della l. 6 agosto 1990, n. 223 dispone che le sanzioni previste dall'art. 13 della l. 47/1948 si applicano al concessionario privato, alla concessionaria pubblica ovvero alla persona a loro delegata al controllo della trasmissione «nel caso di reati di diffamazione commessi attraverso trasmissioni consistenti nell'attribuzione di un fatto determinato».

radiotelevisivo pubblico e privato – la radio e la televisione venivano anch'esse ricondotte alla locuzione "altro mezzo di pubblicità" di cui al terzo comma dell'art. 595 c.p. Più di recente, la nozione di "altro mezzo di pubblicità" si è utilmente prestata a far rientrare nell'ambito di applicazione della norma incriminatrice anche le condotte realizzate in generale nell'ambito di internet, e in particolare attraverso l'uso dei social network.

La diffusione, in particolare, di un messaggio diffamatorio pubblicato su una bacheca di Facebook integra, secondo giurisprudenza oramai consolidata, una ipotesi di diffamazione aggravata ai sensi dell'art. 595, c. 3, c.p. Il livello di diffusività dell'offesa può variare in concreto a seconda delle impostazioni più o meno restrittive di privacy adottate dall'utente ma è certo che il mezzo utilizzato sia di per sé idoneo a determinare la circolazione – tendenzialmente anche incontrollabile – del messaggio tra un numero indeterminato di persone[4].

Più complessa, ad avviso di chi scrive, appare la riconducibilità *sic et simpliciter* alla nozione di "altro mezzo di pubblicità" di diversi strumenti di circolazione delle informazioni che non possiedono per loro natura la potenzialità diffusiva di un sito internet, di un blog o di un profilo pubblico, o anche solo parzialmente pubblico, su un social network.

Ci si riferisce, in particolare, a mezzi del tutto ordinari di comunicazione quali il fax e, per l'appunto, la posta elettronica.

La giurisprudenza sembra essersi assestata su una interpretazione estensiva e per lo più formale del concetto di "altro mezzo di pubblicità", affermandosi o negandosi l'aggravante a seconda della mera natura oggettiva del mezzo: più volte, ad esempio, è stato affermato che l'invio di un documento dal contenuto diffamatorio a mezzo fax integri di per sé gli estremi dell'aggravante.

Si è detto, a questo proposito, che – essendo la diffamazione un reato istantaneo che si consuma con l'adozione di mezzi che rendano accessibili a più persone le affermazioni offensive – ove un singolo apparecchio fax si trovi fisicamente in un ambiente a cui hanno accesso più persone, deve ritenersi presunta la conoscenza, o quanto meno la conoscibilità, del messaggio diffamatorio da parte di tutti coloro che possono avere accesso al dispositivo[5].

Del tutto analogamente, è stata ritenuta configurata la fattispecie aggravata della diffamazione nel caso di comunicazione pervenuta via fax al Consiglio di un ordine professionale contenente espressioni offensive nei confronti di uno degli iscritti; questo perché «le caratteristiche e la natura del mezzo prescelto implicano la conoscenza o la conoscibilità del contenuto della comunicazione da parte di un numero indeterminato di soggetti, ancorché qualificati da un titolo professionale»[6]. La "pubblicità" si sarebbe realizzata quindi non solo nei confronti dei componenti del Consiglio dell'ordine, effettivo destinatario in quel caso della comunicazione, ma di tutti gli iscritti all'ordine professionale.

---

[4] Cfr. oltre alla già citata Cass. pen., sez. I, 2 dicembre 2016, n. 50 anche, *ex multis*, Cass. pen., sez. V, 16 gennaio 2015, n. 6785; Cass. pen., sez. I, 22 gennaio 2014, n. 16712.

[5] Cfr. Cass. pen., sez. V, 9 dicembre 2015, n. 6081.

[6] Cfr. Cass. pen., sez. I, 26 aprile 2007, n. 18888.

Ecco che la ritenuta esistenza del requisito della "pubblicità" – evidentemente diverso da quello della "comunicazione con più persone" di cui al primo comma dell'art. 595 c.p. – sembra essere passato talvolta attraverso una certa forzatura delle specificità del caso concreto.

3. Dubbi interpretativi

Non meno problematica sul piano squisitamente concettuale, ad avviso di chi scrive, è la riconducibilità al concetto di "altro mezzo di pubblicità" della posta elettronica *tout court*.

La decisione qui commentata, come anticipato, nella sua sinteticità non compie alcun distinguo e si limita ad affermare che la posta elettronica deve ritenersi strumento «di pubblicità di notevolissima capacità diffusiva» sicché l'aggravante sembra quasi esistere *in re ipsa*.

Una pronuncia siffatta non è, per la verità, inedita nel panorama giurisprudenziale.

Già in passato la Corte di Cassazione, con una decisione del tutto identica nel suo contenuto a quella qui commentata e altrettanto stringata, aveva ritenuto integrato il reato di diffamazione aggravato ai sensi dell'art. 595, c. 3, c.p. nel caso di «diffusione delle espressioni offensive mediante il particolare e formidabile mezzo di pubblicità della posta elettronica». Ciò in virtù dello «strumento del "*forward*" a pluralità di destinatari»[7].

In altre parole, ad avviso della Corte, il fatto che ogni singola e-mail possa essere (non è detto che lo sia) inoltrata un numero illimitato di volte non solo dal mittente ma anche dai suoi destinatari renderebbe la posta elettronica di per sé un "mezzo di pubblicità". Questo anche nel caso, va da sé, in cui gli originari destinatari della comunicazioni siano un numero molto limitato di soggetti.

Il principio espresso dalla recente sentenza del Supremo Collegio non è dunque affatto "nuovo", affondando le sue radici in una impostazione che, come si è visto, da sempre identifica l'accertamento dell'aggravante con la valutazione della natura del mezzo utilizzato e la sua astratta potenzialità diffusiva.

Questo tipo di approccio – pur essendo senz'altro condivisibile in linea di principio perché coerente con la lettera della norma incriminatrice – richiederebbe però forse in alcuni casi un maggiore approfondimento e un più robusto sforzo argomentativo.

È ovvio che la valutazione sulla sussistenza dell'aggravante non può implicare l'accertamento ogni volta della concreta ed effettiva diffusione *ex post* del messaggio diffamatorio in base al numero di persone effettivamente raggiunte, non solo perché questo sarebbe irrealistico nella maggior parte dei casi ma anche per la evidente impossibilità di stabilire un limite quantitativo al di sotto del quale si dovrebbe escludere una "pubblicità" dell'offesa.

Se però la *ratio* dell'aumento di pena si fonda sull'esigenza di punire condotte in grado di arrecare un danno particolarmente pregnante alla persona offesa perché tali da estendere in modo esponenziale – per l'appunto a un numero indeterminato di soggetti – la conoscenza del messaggio diffamatorio, un qualche accertamento in concreto,

[7] Cfr. Cass. pen., sez. V, 6 aprile 2011, n. 29221.

caso per caso, delle modalità di utilizzo della posta elettronica appaiono imprescindibili. La mera comunicazione a più soggetti determinati di un'offesa, che è poi l'essenza della diffamazione, è fatto diverso da quello sotteso all'aggravante che impone un accertamento ulteriore ovvero la (effettiva) destinazione alla divulgazione a un numero potenzialmente illimitato di persone, che costituisce la ragione giustificativa dell'aumento di pena.

Il criterio distintivo tra fattispecie semplice e aggravata rimane sempre quello della determinatezza (o determinabilità) o meno dei destinatari della comunicazione. Accertamento, questo, che non dovrebbe appagarsi di clausole di stile ma dovrebbe essere compiuto ogni volta in concreto.

A seguire, infatti, fino alle estreme conseguenze il ragionamento espresso dalla Corte di Cassazione, l'aggravante di cui al terzo comma dell'art. 595 c.p. assumerebbe sempre e comunque una connotazione formale tale per cui l'uso di quel peculiare strumento, a prescindere dal numero degli effettivi destinatari del messaggio (che per la sussistenza del reato, come è noto, è sufficiente siano anche solo due), renderebbe sempre implicita la destinazione al pubblico e la sua diffusione a un numero indeterminato di soggetti. Conclusione, questa, che – a seconda dei casi – rischia di essere del tutto sproporzionata sul piano afflittivo rispetto all'uso concreto che può essere fatto della posta elettronica.

Per quanto dunque l'accertamento della effettiva estensione soggettiva della lesione all'onore sfugga alle maglie della lettera della norma, resta ferma sempre la necessità di un'analisi in concreto della reale potenzialità diffusiva del mezzo utilizzato.

La copia cartacea dello *screenshot* ha valore probatorio

Andrea Ranghino

Corte di Cassazione, sez. V penale, 16 gennaio 2018, n. 8736

La copia cartacea di una schermata telematica è soggetta alla libera valutazione del giudice e ha valore probatorio anche se è priva di attestazione ufficiale che ne confermi l'autenticità.

Sommario

1. Il caso. – 2. La nozione di "documento" di cui all'art. 234, c. 1, c.p.p. e le garanzie previste per l'acquisizione dei dati informatici.- 3. Conclusioni

Keywords: Prova, Documento, Copia, Indagini informatiche, Libero convincimento

1. Il caso

Su un quotidiano *online* venivano pubblicati alcuni articoli dal contenuto diffamatorio in danno del presidente di una Provincia. All'esito del primo grado di giudizio il Tribunale emetteva una sentenza di condanna per il reato di diffamazione: la prova decisiva della colpevolezza sembra essere stata desunta da una copia cartacea delle schermate telematiche del sito Internet (prodotta dalla parte civile), da cui risultava che l'imputato fosse l'autore degli articoli e il direttore responsabile del giornale *online*.

La condanna era successivamente annullata dalla Corte di Appello, che, al contrario, non riteneva attendibile tale prova documentale, non essendo vidimata da un notaio e in mancanza di dati ulteriori che ne confermassero la certezza e l'autenticità.

Con la sentenza in commento la V sezione della Corte di Cassazione ha annullato la sentenza di assoluzione, ritenendo, invece, utilizzabile e attendibile la copia delle schermate del sito Internet su cui erano stati pubblicati gli articoli dal contenuto diffamatorio.

A supporto della propria decisione il Giudice di legittimità ha osservato, anzitutto, che l'estrazione di dati archiviati su un supporto informatico non costituisce un accertamento tecnico irripetibile neppure in seguito all'entrata in vigore della l. 48/2008.

La Corte ha precisato, inoltre, che con tale legge si è introdotto solamente l'obbligo per la polizia giudiziaria di rispettare determinati protocolli di comportamento, senza prevedere alcuna sanzione processuale nel caso gli stessi non fossero attuati. La violazione della normativa, dunque, si rifletterebbe unicamente sul piano dell'attendibilità

della prova acquisita tramite l'accertamento.
Si è rilevato, poi, che i dati di carattere informatico contenuti nel computer rientrano tra le prove documentali, in quanto rappresentano cose e che per l'estrazione di tali dati non occorre alcuna particolare garanzia, trattandosi di un'operazione esclusivamente meccanica.
È richiamata, inoltre, una recente pronuncia in cui si sostiene che i fotogrammi scaricati dal sito Internet *Google Earth* costituiscono prove documentali pienamente utilizzabili ai sensi dell'art. 234, c. 1, c.p.p. e 189 c.p.p.[1]
La Corte di Cassazione ha concluso il proprio ragionamento ricordando che la possibilità di acquisire un documento e di porlo alla base della decisione non è limitata ai soli casi in cui il documento provenga da un pubblico ufficiale o sia autenticato. Ogni documento acquisito legittimamente, infatti, ha valore probatorio ed è soggetto alla libera valutazione del giudice sebbene sia privo di certificazione ufficiale di conformità e l'imputato ne disconosca il contenuto.
Dal momento che l'annullamento è stato disposto ai soli fini civili, la Corte di Cassazione ha trasmesso il procedimento al giudice civile competente per valore in grado di appello.

2. La nozione di "documento" di cui all'art. 234, c. 1, c.p.p. e le garanzie previste per l'acquisizione dei dati informatici.

Come rilevato in dottrina[2], il codice di procedura penale ha consapevolmente omesso di fornire una definizione di "documento", essendosi limitato a prevedere la possibilità di acquisire ogni supporto materiale che rappresenti fatti, persone o cose. Gli elementi costitutivi del documento sono, dunque: (i) il fatto rappresentato, ossia l'oggetto della prova; (ii) la rappresentazione, che è la creazione di un equivalente al fatto rappresentato; (iii) l'incorporamento, vale a dire la procedura con cui la rappresentazione è fissata sulla base materiale e (iv) la base materiale, che è il mezzo con cui si conserva e si riproduce la rappresentazione[3].
Ogni documento, inoltre, è formato con la medesima finalità di diffondere e condividere le informazioni.
La decisione di lasciare aperto il catalogo dei supporti idonei a riprodurre il documento ha certamente agevolato l'estensione della disciplina dettata dall'art. 234, c. 1, c.p.p. anche ai documenti informatici.
Tale possibilità, del resto, è stata ammessa pacificamente dalla giurisprudenza della Corte di Cassazione secondo cui:

«I dati contenuti nel computer […] costituiscono prova documentale ai sensi dell'art.

[1] Cass. pen., sez. III, 15 settembre 2017, n. 48178, *CED* 271313

[2] L. Kalb, *Il documento nel sistema probatorio*, Torino, 2000, 57.

[3] P. Tonini – C. Conti, *Le prove penali*, Milano, 2012, 383.

234 c.p.p., c. 1, trattandosi della rappresentazione di cose, termine cui deve attribuirsi la più ampia estensione, effettuata mediante mezzi diversi da quelli tradizionali, così come previsto dalla norma»[4].

Se non vi sono dubbi sulla possibilità di ricondurre il documento informatico alla categoria di documenti di cui al citato art. 234, più incerto è il rapporto tra il documento informatico e i documenti tradizionali. Infatti, se da un lato, il documento informatico potrebbe essere ritenuto una *species* di rappresentazione nuova e ulteriore rispetto a quelle codificate; dall'altro, si è correttamente osservato che uno scritto, una fotografia o un video possono indistintamente rivestire la tradizionale forma analogica oppure quella digitale, quando sono contenuti all'interno di un *file*.

Ciò che distingue un documento informatico da uno tradizionale, dunque, non è l'attitudine rappresentativa, ma la metodologia di incorporamento: all'interno dei *file* (la base materiale) vi è una serie ulteriore di dati che, pur non attenendo alla rappresentazione del fatto, sono rilevanti nel momento in cui la prova deve essere acquisita, ammessa e valutata. Si pensi alla dimensione del *file*, alla data di ultima modifica, all'autore del documento, alla data di ultimo accesso: sono tutte informazioni che, se alterate, potrebbero incidere irrimediabilmente sulla genuinità della rappresentazione.

Proprio in ragione della rilevanza di tali dati, la l. 48/2008, modificando alcune norme del codice procedura penale, ha imposto, in caso di accertamenti su materiale informatico, di adottare misure tecniche idonee ad assicurarne la conservazione e a impedirne l'alterazione, nonché di procedere, se possibile, alla immediata duplicazione dei dati mediante procedura che garantisca la conformità della copia all'originale e la sua immodificabilità.

Va rilevato, peraltro, come a differenza di quanto affermato nella sentenza in esame, in dottrina si è sostenuto che l'adozione di procedure scorrette, a tal punto da far sorgere dubbi in ordine alla conformità della copia all'originale, comporterebbe l'inutilizzabilità del dato digitale in quanto acquisito in violazione dell'art. 191 c.p.p[5].

Parimenti in dottrina non si condivide l'opinione secondo cui l'acquisizione di dati da un *hard disk* sia da considerare sempre alla stregua di un accertamento tecnico ripetibile, ai sensi dell'art. 354 c.p.p., dal momento che la semplice accensione del computer potrebbe portare alla modica di alcuni dati conservati nella memoria[6].

3. Conclusioni.

Il principio di diritto affermato nella sentenza in commento è chiaro: la copia cartacea di una schermata telematica è prova documentale anche se priva di attestazione ufficiale che ne confermi l'autenticità.

Stando alla prima parte delle motivazioni sembrerebbe che la Corte di Cassazione sia

[4] Cass. pen., sez. III, 12 luglio 2012, n. 37419, *CED* 253573.

[5] L. Luparia, *La ratifica della Convenzione* Cyber Crime *del Consiglio d'Europa. I profili processuali*, in *Diritto penale e processo*, 2008, 696 ss.

[6] P. Tonini, *Documenti informatici e giusto processo*, in *Diritto penale e processo*, 2011, 406 ss.

giunta a tale conclusione dopo aver qualificato la prova documentale acquisita nel caso concreto come un documento informatico riconducibile alla categoria dell'art. 234, c. 1, c.p.p. ed escluso la necessità di acquisire i dati tramite la procedura dell'accertamento tecnico irripetibile, essendo sufficiente un'operazione meccanica, inidonea a modificare il contenuto dei dati stessi. Parimenti irrilevante è stata ritenuta la mancata applicazione dei protocolli di comportamento di cui alla l. 48/2008.

Se la ripetibilità dell'operazione con cui è stata acquisita la copia delle schermate telematiche appare indiscutibile, invece, i brevi approfondimenti sulla nozione di documento informatico e sulla acquisizione di dati da un supporto informatico fanno sorgere dei dubbi in merito agli altri passaggi della motivazione.

In particolare, si può davvero ritenere che nel caso concreto la Corte abbia valutato un documento informatico e che vi sia stata l'acquisizione di dati conservati su un sistema informatico nel senso di cui alla l. 48/2008?

Dal tenore letterale delle motivazioni emerge, infatti, che la valutazione ha riguardato la copia cartacea delle schermate telematiche del sito Internet ove erano stati pubblicati gli articoli dal contenuto diffamatorio. La prova, dunque, sembrerebbe essere costituita da un documento analogico, simile a una fotografia, che riproduce ciò che era visualizzato sullo schermo del computer. Si tratterrebbe, in altri termini, di una stampa dello *screenshot*.

L'estrapolazione dei dati sottoposti alla valutazione del giudice, inoltre, sembra essere avvenuta solo "dall'esterno", ossia senza entrare nel sistema e senza acquisire il "vero" documento informatico.

Mancherebbe, quindi, la copia informatica, in senso stretto, dei dati conservati sul sito Internet, che avrebbe consentito al giudice di valutare elementi ulteriori, quali, per esempio, l'autore dei *file* di testo contenenti le espressioni diffamatorie, l'autore delle eventuali modifiche e il responsabile della pubblicazione dei *file* sulla pagina *web*.

Il giudice, diversamente, pare che abbia valutato una prova "tradizionale", costituita solo da ciò che era rappresentato all'interno del documento cartaceo.

I passaggi conclusivi della motivazione non chiariscono tali dubbi.

Nel precedente relativo ai fotogrammi scaricati dal sito *Google Earth*, infatti, non si fa mai riferimento alla nozione di "documento informatico", riconducendo, piuttosto, tali immagini alla categoria delle prove atipiche di cui all'art. 189 c.p.p.

Infine, nella fase conclusiva del ragionamento è richiamata una pronuncia in cui si afferma che le copie fotostatiche hanno efficacia probatoria anche in assenza di una certificazione ufficiale di conformità, in forza del principio della libertà della prova[7].

Qui il tema è radicalmente diverso: non si tratta più di capire quali garanzie devono essere rispettate per acquisire i dati informatici, ma si ragiona sulla possibilità di utilizzare una copia di un documento in luogo dell'originale, e sulla valenza probatoria che deve essere riconosciuta alla copia medesima.

In definitiva, nonostante le premesse, rimane il dubbio che la Corte di Cassazione abbia propeso per l'utilizzabilità del documento ritenendolo equivalente a una copia fotostatica dello schermo del computer, di cui si è ritenuta l'attendibilità in assenza di

[7] Cass. pen., sez. II, 21 novembre 2014, n. 52017, *CED* 261627.

elementi dimostrativi di una qualche alterazione.

Va rilevato, infine, come la decisione assunta nel caso in esame si allinei con quanto affermato in altra pronuncia di legittimità, pressoché coeva, in cui è stata ritenuta utilizzabile la stampa di una pagina *Facebook* sebbene non fossero state rispettate le procedure di cui alla l. 48/2008. Anche in tale caso la Corte ha rilevato che tale disciplina non avesse introdotto alcuna inutilizzabilità probatoria del dato acquisito (costituito, peraltro, da una mera stampa di una videata frutto di un'operazione informaticamente elementare) senza il rispetto delle suddette procedure, che il giudice potrà valutare secondo il principio del libero convincimento, al pari di qualsiasi altro documento»[8].

[8] Cass. pen., sez. V, 4 dicembre 2017, n. 5175.

Responsabilità del direttore per omesso controllo e del giornalista per diffamazione: autonomia delle fattispecie e ricadute sulle formule assolutorie

Laura Ninni

Corte di Cassazione, sez. V penale, 1° marzo 2018, n. 16763

Il delitto di diffamazione commesso dal giornalista con il mezzo della stampa rappresenta l'evento del reato colposo attribuibile al direttore responsabile ai sensi dell'art. 57 c.p. Ne consegue che, se il delitto di diffamazione di cui all'art. 595, c. 3, c.p., non risulta essere stato consumato per carenza dell'elemento psicologico, la fattispecie omissiva prevista a carico del direttore non può trovare applicazione, imponendo la pronuncia di assoluzione con formula "il fatto non sussiste".

Sommario

1. Il caso. – 2. Le questioni a monte. – 3. Conclusioni

Keywords: Diffamazione, Direttore responsabile, Diritto di cronaca, Formula assolutoria, Responsabilità penale

1. Il caso

Con la pronuncia in esame la Corte di Cassazione, con succinta motivazione, annulla l'impugnata sentenza di assoluzione pronunciata dalla Corte d'Appello di Milano nei confronti del direttore di un periodico imputato del delitto di cui all'art. 57 c.p., accogliendo il motivo di ricorso volto ad ottenere formula assolutoria più favorevole per quest'ultimo.

L'*iter* processuale. Il ricorrente, direttore responsabile di un periodico, assolto in primo grado dal reato di cui all'art. 57 c.p., in relazione agli artt. 595 c.p. e 13, l. 47/1948, con formula "perché il fatto non costituisce reato", impugna il provvedimento lamentando l'erroneità della formula assolutoria. Proposto appello, il giudice di seconde cure non accoglie la tesi della difesa. Secondo quest'ultima, l'assoluzione nei confronti dell'autore del delitto di diffamazione, in ragione della scriminante del diritto di critica, avrebbe imposto l'assoluzione del direttore non con la medesima formula adottata per il giornalista ("il fatto non costituisce reato"), ma con quella, più favorevole, "il fatto non sussiste". Di qui l'ulteriore grado di giudizio, con riproposizione della medesima

tesi difensiva.
L'accoglimento del ricorso da parte della Corte di Cassazione, pur concisamente motivato, merita qualche riflessione, dal momento che la questione in esame presuppone lo scioglimento di nodi interpretativi che tradizionalmente gravitano intorno all'art. 57 c.p.

2. Le questioni a monte

Il tema che occupa i giudici di legittimità nella sentenza in esame non è invero nuovo[1]. Come si anticipava, esso è solo l'ultimo (o l'estrema conseguenza) di quella che potremmo definire una catena di questioni che riguardano, tra i molti profili problematici relativi alla fattispecie di cui all'art. 57 c.p., il delicato rapporto tra la responsabilità dell'autore del reato a mezzo stampa e quella del direttore, con particolare riguardo al significato da attribuire all'espressione "reato commesso" di cui alla norma incriminatrice.
Sul punto è necessario ripercorrere brevemente gli snodi principali della questione, a partire dall'antica *querelle* tra chi individuava nel "reato commesso" dal giornalista una condizione obiettiva di punibilità e chi, invece, riteneva quest'ultimo evento del reato in senso tecnico[2], con tutte le conseguenze derivanti dall'accoglimento dell'una o dell'altra soluzione, prima tra tutte la qualificazione giuridica dell'art. 57 c.p. quale reato omissivo proprio o improprio. A tacer d'altro, infatti, il riconoscimento del reato commesso quale *evento* del delitto di cui all'art. 57 c.p. implica che quest'ultimo debba ritenersi fattispecie causalmente orientata e addebitabile all'agente al quale possa essere mosso un rimprovero di colpa per omesso impedimento dell'evento. Viceversa, inscrivere il reato commesso dal giornalista nell'alveo della mera condizione obiettiva di punibilità implica un totale scollamento tra il fatto del giornalista e quello del direttore: come noto, tratto caratteristico delle condizioni di cui all'art. 44 c.p. è l'essere svincolate dal nesso materiale e psicologico, le stesse non contribuendo a descrivere l'offesa al bene giuridico tutelato.
La questione può dirsi oggi del tutto superata, esistendo ormai, sin dalla pronuncia delle Sezioni Unite Clementi[3], un orientamento giurisprudenziale granitico che abbraccia la tesi dell'evento costitutivo e, dunque, sotto un diverso profilo, della qualificazione

[1] È la Corte stessa, nel motivare l'accoglimento del ricorso, che indica precedenti conformi alla propria decisione: Cass. pen., sez. V, 4 marzo 2005, n. 15001, in *DeJure*; Cass. pen., sez. V, 26 febbraio 2003, n. 19827, in *Riv. pen*., 2003, 845 ss.; Cass. pen., sez. V, 17 novembre 1999, n. 1062, in *DeJure*.

[2] In tema A. Mino, *La disciplina sanzionatoria dell'attività giornalistica: dalla responsabilità penale del direttore alla responsabilità da reato dell'ente*, Milano, 2012, *passim*; M. Fumo, *La diffamazione mediatica*, Torino, 2012, 161 ss., V. Pezzella, *La diffamazione. Responsabilità penale e civile*, Torino, 2009, 216 ss.; G. Corrias Lucente, *Il diritto penale dei mezzi di comunicazione di massa*, Padova, 2000, 207; G. Delitala, *Titolo e struttura della responsabilità penale del direttore responsabile per i reati commessi sulla stampa periodica*, in *Riv. it. dir. proc. pen*., 1959, 548.

[3] Cass. pen., sez. un., 18 novembre 1958, n. 28, in *Riv. it. dir. proc. pen*., 1959, 543 ss.; Cass. pen., sez. V, 13 novembre 1981, n. 10252, in *DeJure*; Cass. pen., sez. V, 12 giugno 1992, in *Giur. it*., 1994, 2, 45 ss; Cass. pen., sez. VI, 10 marzo 1994, in *Cass. pen.,* 1995, 3076 ss.; Cass. pen., sez. V, 31 marzo 2000, in *Riv. pen*., 2000, 1026 ss.; Cass. pen., sez. V, 30 aprile 2003, n. 19827, in *Riv. pen*., 2003, 845 ss.

della fattispecie di cui all'art. 57 c.p. come reato omissivo improprio.
Ulteriore tema che ha impegnato l'interprete era il seguente: il reato presupposto, evento del delitto *de quo*, deve essere completo di tutti i suoi elementi - ossia deve trattarsi di un fatto tipico, antigiuridico, colpevole nonché punibile - oppure il riferimento al reato commesso è da intendersi nella sua mera oggettività, bastando il fatto tipico?
La questione è stata affrontata e variamente risolta. Secondo un'interpretazione[4], la soluzione più rispondente alla *ratio* della norma di cui all'art. 57 c.p. sarebbe quella di non limitare la responsabilità del direttore ai casi in cui il reato sia completo di tutti gli elementi essenziali ma, al contrario, di ritenerla fondata allorché sia integrato un fatto tipico e antigiuridico da parte del giornalista.
La dottrina maggioritaria, tuttavia, adotta un criterio interpretativo più rigoroso e ritiene necessario che il reato sia completo di tutti i suoi elementi, compreso quello soggettivo[5], fondando tale soluzione sul rispetto del principio di offensività e sul criterio letterale (la norma infatti recita "reato commesso")[6].
La giurisprudenza ha aderito alla dottrina maggioritaria[7], richiedendo che il reato presupposto sia perfezionato in tutti i suoi elementi, senza esigere che il controllo da parte del direttore si spinga a ricomprendere un'indagine sull'atteggiamento psicologico dell'autore dello scritto[8].
Ecco il tema centrale per la questione sottoposta alla Corte nella sentenza in commento: l'autonomia tra il reato la cui commissione deve essere impedita dal direttore ed il reato ascrivibile al direttore stesso, con le relative conseguenze in termini di costruzione della fattispecie.
A mente dell'art. 57 c.p., infatti, il direttore risponde dell'omesso, dovuto controllo, secondo il modello del c.d. *culpa in vigilando*, sui contenuti del periodico. Tale responsa-

[4] Cass. pen., sez. V, 4 marzo 1982, in *Cass. pen*., 1983, 2012 ss., con nota di L. Vignale, *La nozione di reato commesso nella fattispecie dell'art. 57 c.p.* La pronuncia aderisce per vero all'interpretazione della dottrina maggioritaria, che ritiene necessario un fatto non solo tipico, ma anche antigiuridico e colpevole; l'autore in commento si discosta viceversa da tale soluzione, ritenendo non necessario l'elemento psicologico della colpevolezza per l'integrazione del "reato commesso".

[5] *Ex pluris* in dottrina G. Corrias Lucente, *op. cit*., 207; F. Mantovani, *Diritto penale, parte generale*, Padova, 1979, 374.

[6] Tale soluzione sembra, a parere di chi scrive, corretta nell'esito ma non nelle premesse. Il principio di offensività è criterio di orientamento che concerne l'elemento materiale del reato: la lesione al bene giuridico è infatti parte del fatto tipico, nulla avendo a che fare con l'elemento psicologico. Quanto al criterio letterale, oltre a non apparire in generale dirimente, se seguito porterebbe ad opposta soluzione, considerata la lettera degli artt. 110 e 116 c.p. La soluzione, pertanto, dovrebbe essere la medesima ma fondata sul rapporto intercorrente tra il delitto ascrivibile al direttore e quello che lo stesso ha l'obbligo di impedire.

[7] Cass. pen., sez. V, 22 febbraio 2012, n. 15004, in *Guida dir.,* 22, 2012, 31 ss., con nota di C. Melzi d'Eril - G.E. Vigevani, *Lo scarso rilievo e la poca visibilità dello scritto dovrebbero ridurre i doveri di controllo del vertice*; Cass. pen., sez. V, 8 aprile 2003, n. 22869, in *Leggi d'Italia*; Cass. pen., sez. V, 4 marzo 1982, in *Cass. pen*., 1983, 2012 ss., con nota di L. Vignale, *La nozione di reato commesso nella fattispecie dell'art. 57 c.p.*

[8] Come correttamente nota E. Musco, *Stampa (dir. pen.)*(voce), in *Enc. Dir.*, XLIII, Milano, 1990, 641.

bilità, come si è visto, si differenzia da quella dell'autore dello scritto[9]: il reato presupposto e quello ascrivibile al direttore godono di reciproca autonomia in termini di costruzione della fattispecie salvo, chiaramente, quanto si è detto poc'anzi relativamente all'evento del reato in esame.

3. Conclusioni

Date tutte queste premesse e ricordando che il "reato commesso", completo di ogni elemento oggettivo e soggettivo, è evento costitutivo del delitto di cui all'art. 57 c.p., deve poi giungersi all'obbligato corollario che *in assenza* di detto evento, il reato (omissivo, improprio) non si compie.

A tale conclusione era già giunta parte della giurisprudenza[10] ma, evidentemente, non sempre traendone le dovute conclusioni.

Come dimostra, infatti, la sentenza appellata, a fronte dell'assoluzione dell'autore del reato presupposto in ragione della scriminante del diritto di critica e, dunque, con la formula assolutoria "perché il fatto non costituisce reato", viene utilizzata la *medesima formula assolutoria* anche per il direttore del periodico.

Una tale assimilazione implica il riconoscimento della causa di giustificazione – nel caso di specie, dell'esercizio del diritto di critica – sia nei confronti del giornalista, nell'ambito del delitto di diffamazione sia, per estensione, nei confronti del direttore del periodico.

Estendere la formula assolutoria del giornalista al direttore del periodico sarebbe possibile e corretto laddove fosse applicabile la disciplina generale delle cause di giustificazione nell'ambito del concorso di persone. Come noto, infatti, di regola le scriminanti operano ai sensi dell'art. 119, c. 2, c.p. sia nei confronti dell'autore del fatto di reato, sia nei confronti di chi sia concorso – con contributo atipico, si intende – nel fatto di questi. Tuttavia, come si è tentato di evidenziare, dall'interpretazione dell'art. 57 c.p. di cui si è dato brevemente conto in commento, emerge l'autonomia della fattispecie rispetto al reato presupposto e, pertanto, l'esclusione della disciplina del concorso di persone allorché sia contestato il reato di omesso controllo.

Correttamente dunque la sentenza in esame si inserisce nel filone giurisprudenziale che, oltre ad aderire alla piena autonomia del delitto di cui si tratta, ne fa discendere le corrette conseguenze in termini sostanziali nonché processuali, adottando una formula

[9] Tuttavia, è ben possibile che il direttore concorra nel fatto dell'autore dello scritto: ciò accade quando egli – con condotta attiva o anche omissiva – apporti un contributo atipico nel reato presupposto medesimo, secondo i crismi del concorso di persone, sorretto dalla rappresentazione e volizione di tutti gli elementi significativi della fattispecie dello specifico reato. Nel caso di concorso *ex* art. 110 c.p. nel reato presupposto, pertanto, dovrà dimostrarsi che il direttore ha inteso pubblicare l'articolo esattamente nella sua connotazione, nella consapevolezza e volontà di divulgarlo con *quei* contenuti, con ciò venendo a caratterizzare l'elemento soggettivo – nonché oggettivo - in modo del tutto differente rispetto a quello che integra la responsabilità di cui all'art. 57 c.p. per l'omesso controllo. Sul punto v. più diffusamente M. Fumo, *op. cit.,* 161 ss.

[10] Cass. pen., sez. V, 4 marzo 2005, n. 15001, in *DeJure*; Cass. pen., sez. V, 30 aprile 2003, n. 19827, cit.; Cass. pen., sez. V, 17 novembre 1999, n. 1062, in *DeJure*.

assolutoria – "il fatto non sussiste"[11] – che si differenzia da quella propria del giornalista, autore del reato presupposto, il cui fatto, sì, è scriminato dall'esercizio del diritto di critica.

[11] Più favorevole per l'imputato quanto a rimborso delle spese e risarcimento del danno: cfr. artt. 427, c. 2 e 3, e 652, c. 1, c.p.p.

Le testate telematiche e la tutela costituzionale*

Sabrina Peron

Tribunale di Milano, sez. I civile, ord. 25 gennaio 2018

È possibile ricondurre alla nozione di "stampa" anche i giornali telematici sulla base del riscontro dell'esercizio di un'attività professionale di divulgazione e commento di notizie ed informazione, esercitata secondo regole preliminarmente elaborate di responsabilità o doveri o rispetto di limiti - ed in prevalenza autoamministrate per l'organizzazione in albi di natura pubblicistica - da parte di soggetti particolarmente qualificati, in regime di trasparenza anche quanto a fonti di finanziamento e sostanzialmente di riferimento. Ne segue che le forme o limitazioni di tutela di cui all'art. 21 Cost. possono predicarsi riservate a quelle specifiche forme di manifestazioni di pensiero, come appunto la diffusione ed il commento professionali di notizie od informazioni, indispensabili per la formazione della pubblica opinione in una moderna società democratica, quali giustificazione stessa o contrappeso della particolare responsabilità loro richiesta ed imposta.

Fermo restando l'onere di valutare separatamente i contenuti propri od esclusivi delle testate telematiche, ad essi non potrà allora immediatamente estendersi la conclusione della applicazione de plano della normativa di tutela, di rango tanto costituzionale che sovranazionale ed ordinario, ma dovrà essere ricercata di volta in volta in base ai parametri rilevanti propri della singola fattispecie, eventualmente diversi, a tutto concedere riferiti al solo art. 21 c. 1 Cost. ed al più intenso bilanciamento con gli altri diritti fondamentali della prima parte della Carta fondamentale. Ragion per cui, nel caso di testate telematiche – alla luce della tutela attenuata garantita dalla pronta pubblicazione della rettifica, nelle modalità sopra indicate – non possano trovare accoglimento provvedimenti di inibitoria che porterebbero all'adozione di un provvedimento assimilabile ad una censura, con effetti sostanzialmente simili a quelli di un provvedimento di sequestro, emesso all'esito di un accertamento solo sommario dei fatti – in violazione del diritto alla libera manifestazione del pensiero, tutelata nei limiti di cui all'art. 21 Cost.

Sommario

1. Il caso - 2. La libertà di espressione e il sequestro della stampa – 3. I rimedi atipici offerti dall'art. 700 c.p.c. - 4. L'art. 21 Cost. e l'informazione *online*

Keywords: Stampa, Testata telematica, Sequestro preventivo, Diritto di cronaca, Art. 21

* L'articolo è stato sottoposto, su determinazione della direzione, a referaggio anonimo.

1. Il caso

Con ricorso d'urgenza *ex* art. 700 c.p.c. veniva adito il Tribunale di Milano per ottenere l'inibizione all'ulteriore diffusione di un articolo pubblicato *online* da una testata giornalistica e ritenuto lesivo dell'immagine e della reputazione professionale dei ricorrenti che ne lamentavano la falsità dei contenuti.
Con ordinanza del 22 dicembre 2017 (comunicata il 27 dicembre 2017), il giudice della cautela dichiarava inammissibile il ricorso, richiamandosi ai principi recentemente espressi dalle sezioni unite civili[1].
I ricorrenti proponevano dunque reclamo, deciso con l'ordinanza collegiale qui in commento, che lo rigettava per motivi parzialmente difformi.

2. La libertà di espressione e il sequestro della stampa

Accanto alla libertà personale, la libertà di espressione rappresenta il "cuore" dei diritti di libertà, dal quale possono farsi discendere tutti gli altri diritti. La libertà di espressione a livello nazionale trova riconoscimento e tutela nell'art. 21 Cost., che recita: «tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione», mentre a livello sovranazionale nell'art. 10 CEDU secondo cui: «Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera»[2].
È noto che l'art. 21, c. 3, Cost. sancisce il principio che la stampa non può essere soggetta ad autorizzazioni o censure e che «si può procedere a sequestro soltanto per atto motivato dell'autorità giudiziaria nel caso di delitti, per i quali la legge sulla stampa espressamente lo autorizzi, o nel caso di violazione delle norme che la legge stessa prescriva per l'indicazione dei responsabili»[3]. Inoltre, come ricordano anche le sezioni unite, «l'assemblea costituente, in attuazione della XVII disposizione transitoria della Carta fondamentale, varò anche la L. 8 febbraio 1948 n. 47, intitolata "disposizioni sulla stampa" e ritenuta integrante il disposto dell'art. 21 Cost., il cui art. 1 precisa che sono da considerarsi stampe o stampati "tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubbli-

[1] Cass. civ., sez. un., 18 dicembre 2016, n. 23469.

[2] Il comma successivo così precisa: «L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario».

[3] I casi nei quali le leggi vigenti consentono il sequestro preventivo sono: a) violazione delle norme sulla registrazione delle pubblicazioni periodiche e sull'indicazione dei responsabili (l. 8 febbraio 1948, n. 47 artt. 3 e 16); b) stampati osceni o offensivi della pubblica decenza ovvero divulganti mezzi atti a procurare l'aborto (r.d.lgs. 31 maggio 1946, n. 561: dichiarato incostituzionale con sentenza C. cost. 16 marzo 1971, n. 49); c) stampa periodica che faccia apologia del fascismo (l. 20 giugno 1952, n. 645, art. 8); d) violazione delle norme a protezione del diritto d'autore (l. 22 aprile 1941, n. 633, art. 161).

cazione"»[4].

A sua volta, il r.d.lgs. del 31 maggio 1946, n. 562 (norme sul sequestro dei giornali e delle altre pubblicazioni), all'art. 1 stabilisce che «non si può procedere al sequestro della edizione dei giornali o di qualsiasi altra pubblicazione o stampato […] se non in virtù di una sentenza irrevocabile dell'autorità giudiziaria». La Costituzione, disciplina quindi l'istituto del sequestro in stretta correlazione col divieto di autorizzazione o censura, preventiva o successiva, sottoponendolo alla duplice garanzia della riserva di legge e di giurisdizione[5].

Come osservato dalla Corte Costituzionale (opportunamente richiamata dal Tribunale di Milano, nell'ordinanza che qui si pubblica), per accertare la sfera di applicazione dell'art. 21 Cost., occorre partire dalla non controvertibile constatazione che la «rigorosa disciplina disposta dalla Costituzione a proposito della stampa e la tassativa delimitazione degli interventi consentiti al legislatore ordinario ed alle pubbliche autorità sono preordinate, in un settore di particolare rilevanza, a garanzia del diritto di libera manifestazione del pensiero». Ne segue che, per garantire la diffusione della stampa, la quale potrebbe venire «compromessa o addirittura definitivamente pregiudicata da provvedimenti che, ancorché adottati dall'autorità giudiziaria, si basano su una cognizione sommaria e possono poi risultare ingiustificati in sede di accertamento definitivo, la Costituzione, tenendo conto della importanza del ruolo della stampa in un regime democratico, ha disciplinato il conflitto fra l'interesse al sequestro e l'interesse alla circolazione della stampa: la norma costituzionale di raffronto, mentre consente al legislatore ordinario di dar prevalenza al primo (purché attraverso un'espressa previsione) nel caso di delitti, direttamente stabilisce la prevalenza del secondo in ogni altra ipotesi»[6].

Tale previsione costituzionale «copre l'intera area del sequestro, qualunque sia il contrapposto interesse col quale la stampa entra in collisione»[7], e «mira ad assicurare, contro ogni forma di censura, sia successiva che preventiva, la libera circolazione dell'attività di pensiero»[8]. In definitiva, nel regolare il conflitto tra interesse al sequestro e interesse alla circolazione della stampa, si ritiene che l'art. 21, c. 3, Cost. accordi una «indefettibile prevalenza al secondo, così ponendo un divieto a qualsiasi provvedimento, ivi compresi quelli del giudice civile a tutela dei diritti di sfruttamento di opera dell'ingegno, che comporti il sequestro dello stampato se non nei casi in cui la legge espressamente lo autorizzi e sempre che a mezzo dello stampato sia stato commesso

[4] Cass. civ., sez. un., 18 novembre 2016, n. 23469, in *Foro it.*, 2016, I, 3753 ss., con note di richiamo di A. Palmieri.

[5] *Ibidem*. La sentenza, a sua volta, richiama C. Cost., 19 gennaio 1972, n. 4 e C. Cost. 25 marzo 1976, n. 60: «il sequestro della stampa generalmente intesa cioè, senza specificazioni, sia essa periodica o comune - può essere disposto, con atto motivato dell'autorità giudiziaria, soltanto nel caso di delitti per i quali la legge sulla stampa espressamente lo autorizzi o nel caso di stampa clandestina; quello della stampa periodica è soggetto ad ulteriori garanzie procedurali; in ogni caso, il riferimento alla legge sulla stampa non introduce una riserva qualificata di legge, ma è indicativo del complesso delle norme riguardanti la materia».

[6] Come notazione storica si evidenzia che tale decreto fu uno degli ultimi firmati da Umberto II e venne pubblicato sulla Gazzetta Ufficiale di luglio quando l'Italia era già una Repubblica.

[7] C. Cost., 9 luglio 1970, n. 122, in *Foro it.*, 1970, I, 2294 ss.

[8] Trib. Napoli, 15 dicembre 1997, in *Dir. inf.*, 1998, 608 ss.; Trib. Roma, 6 dicembre 1993, in *Dir. inf.*, 1994, 334 ss.

un delitto»[9]. Inoltre, il limite del sequestro a tre esemplari previsto dall'art. 1, c. 1, r.d.l-gs. 561/1946, «riguarda, invece, il solo sequestro probatorio, sia per ragioni storiche sia perché la previsione di un sequestro preventivo limitato a tre sole copie sarebbe contraria alle finalità tipiche dell'istituto, preordinato ad impedire l'aggravamento e il protrarsi delle conseguenze della ipotizzata condotta criminosa; con riguardo al sequestro preventivo, il legislatore - salvo che per talune fattispecie (stampa clandestina ovvero pubblicazioni o stampati osceni ed offensivi) - non ha dato, infatti, attuazione alla riserva di legge, sicché l'adozione del sequestro preventivo, al di là dei casi espressamente previsti, è illegittima»[10].

3. I rimedi atipici offerti dall'art. 700 c.p.c.

È altrettanto noto che i procedimenti d'urgenza *ex* art. 700 c.p.c., sono tesi ad ottenere provvedimenti cautelari atipici, ossia tutti quei provvedimenti che appaiono, secondo le circostanze, più idonei ad assicurare provvisoriamente gli effetti della decisione sul merito. Per tale ragione vengono richiesti dalla parte che – durante il tempo occorrente per far valere il suo diritto in via ordinaria – ha fondato motivo di temere che esso sia minacciato da un pregiudizio grave ed irreparabile. Correlativamente, il giudice ha ampia discrezionalità nell'individuare il contenuto del provvedimento più idoneo a preservare un diritto, quando vi è il fondato motivo che durante il tempo occorrente per farlo valere, questo sia minacciato da un pregiudizio imminente ed irreparabile.
Ciò posto, al di fuori dei casi di «stampa oscena, apologetica del fascismo o integrante violazione del diritto d'autore costituente delitto, non è ammissibile il sequestro cautelare o provvedimenti ad esso equivalenti, *ex* art. 700 c.p.c., delle pubblicazioni a mezzo stampa, ancorché lesive dei diritti all'onore, alla riservatezza o all'identità personale della persona; né può ritenersi in contrasto con l'art. 2 Cost. la mancata previsione, nel codice della protezione dei dati personali, di una norma che consenta l'adozione di provvedimenti anticipatori assimilabili al sequestro»[11].
In questa linea giurisprudenziale consolidata si pone anche il Tribunale di Milano, il quale osserva come «sebbene l'art. 700 c.p.c. possa consentire l'emanazione di provvedimenti cautelari atipici intesi a far cessare temporaneamente o a limitare il pregiudizio

[9] Trib. Milano, 26 settembre 1994, in *AIDA*, 1995, 556 ss.

[10] Cass. pen., sez. V, 12 giugno 2008, n. 27996. Si veda anche Trib. Milano, 23 ottobre 2002, in *Foro ambrosiano*, 2003, 471: «È da ritenersi tuttora in vigore il disposto dell'art. 1 r.d.leg. 561/1946, ai sensi del quale, nel caso di diffamazione a mezzo stampa, è previsto il sequestro di un massimo di tre esemplari dell'opera incriminata, qualora non sia stata pronunciata sentenza irrevocabile di condanna e non si verta in materia di pubblicazioni oscene, di stampa clandestina o di diritto d'autore».

[11] Trib. Roma, 14 febbraio 2008, in *Dir. inf.*, 2008, 177 ss. In senso contrario: Trib. Napoli, 18 febbraio 2015, n. 1184, in *Dir. inf.,* 2015, 336 ss. (con nota di P. Sammarco, *Stampa on-line: compatibilità dello strumento cautelare di cui all'art. 700 c.p.c. per la rimozione di articoli diffamatori e brevi annotazioni sui profili risarcitori*), secondo il quale «lo strumento cautelare di cui all'art. 700 c.p.c. attivato per la rimozione di articoli di stampa pubblicati su internet all'interno di testate telematiche non è soggetto alle limitazioni riportate dall'art. 21 Cost. e dalle disposizioni della legge sulla stampa (art. 1 del r.d.lg. n. 561 del 1946) perché non vi è equiparazione di tale provvedimento cautelare richiesto al giudice civile al sequestro preventivo proprio del processo penale e contemplato dall'art. 321 c.p.p.».

che deriva a terzi da una pubblicazione, tale strumento non può, tuttavia, costituire la fonte di un potere di concedere un provvedimento sostanzialmente di sequestro della stampa, vietato da altra norma dell'ordinamento e, in particolare, dall'art. 21 Cost., che lo consente solo con l'osservanza di limiti molto rigorosi».
Fermo restando, in ogni caso, che tutti i diritti fondamentali tutelati dalla Costituzione sono tra loro in un «rapporto di integrazione reciproca e non è possibile pertanto individuare uno di essi che abbia la prevalenza assoluta sugli altri», altrimenti si «verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe "*tiranno*" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette, che costituiscono, nel loro insieme, espressione della dignità della persona»[12]. Difatti la «Costituzione italiana, come le altre Costituzioni democratiche e pluraliste contemporanee, richiede un continuo e vicendevole bilanciamento tra princìpi e diritti fondamentali, senza pretese di assolutezza per nessuno di essi. La qualificazione come "primari" dei valori dell'ambiente e della salute significa pertanto che gli stessi non possono essere sacrificati ad altri interessi, ancorché costituzionalmente tutelati, non già che gli stessi siano posti alla sommità di un ordine gerarchico assoluto. Il punto di equilibrio, proprio perché dinamico e non prefissato in anticipo, deve essere valutato - dal legislatore nella statuizione delle norme e dal giudice delle leggi in sede di controllo - secondo criteri di proporzionalità e di ragionevolezza, tali da non consentire un sacrificio del loro nucleo essenziale»[13].

4. L'art. 21 Cost. e l'informazione *online*

Nelle moderne società liberal-democratiche, il ruolo svolto dai *mass media*, nella formazione di una pubblica opinione[14] è sicuramente di primaria importanza (tanto da essere descritto come un ruolo di "cane da guardia", secondo la definizione nota definizione della Corte EDU[15]), poiché in tal modo i «cittadini possono esercitare i diritti costituzionalmente sanciti per la loro democratica partecipazione alla vita politica, economica e sociale del paese»[16]: del resto, «è grazie alle discussioni tra giornali di partiti diversi, onesti o disonesti, partigiani o indipendenti, che in una democrazia un barlume di luce qualche volta filtra tra la gente. Sopprimete queste discussioni e il cittadino che sotto una democrazia è miope, sotto una dittatura diventa completamente cieco»[17].

[12] C. Cost., 24 gennaio 2017, n. 20 e C. Cost., 11 febbraio 2015, n. 10.

[13] C. Cost., 9 maggio 2013, n. 85 (espressamente richiamata nell'ordinanza in commento).

[14] Tanto che i *mass media* vengono intesi come intesi come «luogo di raccolta, di produzione e di archiviazione della parola pubblica», così, J. Derrida, *Breve storia della menzogna*, Roma, 2006, 61.

[15] La Corte EDU ha più volte ribadito il ruolo di "cane da guardia" svolto dall'informazione all'interno delle democrazie europee: CEDU, *Colombani c. Francia*, ric. 51279/99 (2002), in *Riv. internaz. dir. dell'uomo*, 2003, 216 ss.; CEDU, *Perna c. Italia*, ric. 48898/99 (2003), in *Cass. pen.*, 11, 3566 ss. (con nota di A. Tamietti, *Libertà di espressione della stampa e diritto all'onore delle persone diffamate nella giurisprudenza della Corte europea dei Diritti dell'Uomo*). Concetto questo ripreso anche dalla giurisprudenza nazionale, si veda ad esempio: Cass. pen., sez. V, 2 luglio 2007, n. 25138, in *Resp. civ. prev.*, 2007, 2550 ss.

[16] Cass. pen., sez. V, 3 giugno 1983, in *Giustizia penale*, 1984, 69 ss.

[17] G. Salvemini, *Sulla democrazia*, Torino, 2007, 37.

Tuttavia, a partire dal c.d. secolo breve[18], la rapida e costante evoluzione dei mezzi con i quali si diffondono le informazioni, ha rivoluzionato i *mass media* ed il loro rapporto con le persone e la società: tant'è che oggi è stato palesato il rischio che i *mass media* più che una forma di rappresentazione della realtà, vengano percepiti come la realtà stessa[19].

Alla categoria dei mezzi di comunicazione di massa, non vi è dubbio alcuno che vi appartenga anche internet, rispetto al quale è stato rimarcato come «grazie alla facilità di accesso, all'interattività e alla copertura mondiale», internet ben «possa dare concreta attuazione al diritto sancito dall'art. 21 Cost., nel duplice senso di esprimere liberamente il proprio pensiero, diffonderlo e di assicurare la pluralità delle fonti informative»[20].

L'altra faccia della medaglia è che internet si presti facilmente a diventare una cassa di risonanza (che, a volte, assume i connotati di una gogna mediatica) pressoché inesauribile: una qualunque informazione che cade nella rete viene ripresa e riciclata, circolando in maniera istantanea e cumulativa (teoricamente all'infinito sia nel tempo che nello spazio virtuale[21]) da un sito all'altro, navigando all'interno di *blog*, transitando nei vari *social network*, arricchendosi di commenti etc., tanto che, in qualche caso, si arriva a smarrire il significato originario dell'informazione o, in altri casi, talune false informazioni vengono create e fatte circolare ad arte per le finalità più disparate[22]. Può dunque accadere che tramite la rete internet si possano commettere reati di manifestazione del pensiero (anzi secondo la Cassazione è «addirittura intuitivo»[23]), quali, esemplificativamente, ingiurie, diffamazioni, vilipendi, diffusioni di scritti immagini o disegni osceni, istigazioni ed apologie di reati, etc. Per tale ragione è pacifico che anche l'informazione *online*, soggiace ai ben noti limiti, rappresentati dalla tutela della persona umana (e parimenti tutelati dalla Costituzione agli artt. 2 e 3), i quali si concretizzano nella tutela del diritto all'immagine, al nome, all'onore, alla reputazione, alla riservatezza.

Ciò posto, anzitutto, pare utile ricordare che giurisprudenza consolidata ha general-

[18] È il felice titolo del saggio dello storico inglese E. Hobsbawm: *Il secolo breve,* Milano, 2007.

[19] J. Braudillard, *Il virtuale ha assorbito il reale*: «i media si frappongono in maniera tale fra la realtà e il soggetto, che, mi pare, non ci sono più interpretazioni possibili in quanto l'informazione rende l'accadimento incomprensibile. L'evento storico non si sa più cosa sia quando passa attraverso i media, in breve si ha una transustanziazione di questo tipo in tutto ciò che i media fanno, così che ne risulta quel che io chiamerei una simulazione, un simulacro, e perciò non esiste più né il vero né il falso: non si sa più quale sia il principio della verità. Questo è certamente un dato importante; ma infine, c'è davvero bisogno della verità? In fin dei conti, l'obiettivo dei media non è stato forse di eliminare effettivamente il principio morale e filosofico della verità, per installare al suo posto una realtà completamente ingiudicabile».

[20] C. Di Lello, *Internet e costituzione: garanzia del mezzo ed i suoi limiti*, in *Dir. inf.*, 2007, 907 ss., il quale sottolinea come internet, sue «caratteristiche di poliedricità ed interattività, si rende mezzo potenzialmente idoneo a fungere contemporaneamente da mezzo di informazione e di comunicazione e dà luogo virtuale nel quale possono realizzarsi innumerevoli altri rapporti».

[21] Ma con possibilità di concretizzarsi anche in quello reale, dato se sempre più spesso accade che un'informazione nata nella rete, venga poi ripresa e diffusa dai *mass media* tradizionali.

[22] In tema di *fake news* si rinvia a M. Bassini – G.E. Vigevani, *Primi appunti su fake news e dintorni*, in *Rivista di diritto dei media*, 2017, 11 ss.; G. Ghidini – A. Massolo, *Fake news: responsabilità, non censura*, in *Diritto industriale*, 2017, 352 ss.; E. Bertolini, *Selfie con Merkel? Diffamazione, hate speech, fake news e responsabilità dei social networks: un difficile bilanciamento*, in www.dpce.it, 2017, 149; F. Pizzetti, *Fake news e allarme sociale: responsabilità, non censura*, in www.astrid-online.it, 2017.

[23] Cass. pen., sez. V, 17 novembre 2000, n. 4741, in *Resp. civ. prev.*, 2001, 309 ss.

mente escluso l'estensione dell'obbligo di registrazione per il giornale *online*[24] e, conseguentemente, l'applicabilità ad internet del regime penalistico previsto dalla Legge sulla stampa (l. 47/1948) o dalla legge sul sistema radiotelevisivo (l. 223/1990), aderendo agli insegnamenti della dottrina secondo la quale la nozione di stampa non può estendersi sino a ricomprendervi anche quella telematica. Vi osterebbe, difatti, il tenore letterale dell'art. 1, l. 47/1948, il quale richiede una riproduzione con mezzi meccanici o fisico-chimici[25], ai quali il messaggio diffuso per via telematica non può essere assimilato[26].

Su questo tema la Cassazione, aveva avuto modo di precisare che, affinché possa «parlarsi di stampa in senso giuridico (ai sensi della ricordata l. 47/948, art. 1), occorrono due condizioni che certamente il nuovo medium non realizza: a) che vi sia una riproduzione tipografica *(prius),* b) che il prodotto di tale attività (quella tipografica) sia destinato alla pubblicazione e, quindi, debba essere effettivamente distribuito tra il pubblico *(posterius)*». Peraltro, il «fatto che il messaggio internet (e, dunque, anche la pagina del giornale telematico) si possa stampare non appare circostanza determinante, in ragione della mera eventualità, sia oggettiva, che soggettiva. Sotto il primo aspetto, si osserva che non tutti i messaggi trasmessi via internet sono "stampabili": si pensi ai video, magari corredati di audio; sotto il secondo, basta riflettere sulla circostanza che, in realtà, è il destinatario colui che, selettivamente ed eventualmente, decide di riprodurre a stampa la "schermata"»[27].

Seguendo questa linea interpretativa, la Dottrina ha escluso l'estensibilità alla telematica della legge che disciplina il sistema radiotelevisivo (l. 223/1990), sul presupposto che la nozione legislativa di «*trasmissione*» non possa comprendere servizi di comunicazione che operano su richiesta individuale, con la conseguenza che si potrebbe ammettere l'assoggettabilità al «regime della L. 223/1990 solo quelle trasmissioni radiofoniche o televisive che vengono diffuse attraverso una rete telematica con modalità analoghe e

[24] Cass. pen., sez. V, 10 maggio 2012, n. 23230, in *Dir. inf.*, 2012, 1120 ss. (con nota di P. Di Fabio, *Blog, giornali on line e «obblighi facoltativi» di registrazione delle testate telematiche: tra confusione del legislatore e pericoli per la libera espressione del pensiero su Internet*): «l'omessa registrazione, preventiva alla diffusione, di un giornale telematico non integra il reato previsto dagli artt. 5 e 16 della legge 8 febbraio 1948, n. 47 atteso che tale adempimento è riservato solo alle testate editoriali per le quali i prestatori di servizio intendano avvalersi delle provvidenze economiche per l'editoria e che la sua estensione costituirebbe interpretazione analogica in "*malam partem*"».

[25] Ai sensi dell'art. 1, l. 47/1948, «sono considerati stampa o stampati […] tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinati alla pubblicazione».

[26] Così, testualmente, V. Zeno-Zencovich, *La pretesa estensione alla telematica del regime della stampa: note critiche*, in *Dir. inf.*, 1998, 15, il quale osserva che il messaggio diffuso per via telematica, viene «sì riprodotto, ma non con mezzi tipografici e similari. E quando si materializza attraverso tali mezzi non vi è più una pubblicazione, ma un uso privato».

[27] Cass. pen., sez. V, 16 luglio 2010, n. 35211, in *Resp. civ. prev.*, 2011, 82 ss., con nota di S. Peron*, Internet, regime applicabile per i casi di diffamazione e responsabilità del direttore*. In senso conforme anche: Cass. pen., sez. V, 11 giugno 2010, n. 30065, secondo la quale «appare errato (oltre che, ancora una volta, superfluo) il richiamo - contenuto nel capo di imputazione- alla L. n. 47 del 1948, art. 13 relativo alla diffamazione a mezzo stampa, atteso che un quotidiano telematico, pur essendo certamente un giornale, non di meno non può essere ricondotto al concetto di stampato. Ne consegue la differenza di trattamento sanzionatorio (che, per il ricordato art. 13, in presenza di fatto determinato, comporta reclusione da uno a sei anni); ne consegue ancora, ad es., la inapplicabilità del disposto di cui all'art. 57 c.p.».

quelle della diffusione via etere e cioè con una programmazione continua determinata dall'emittente e non alterabile dal ricevente nel suo contenuto e nella sua disposizione cronologica»[28].

Dalla non riconducibilità dell'informazione *online* alla nozione di stampa (quanto meno sotto il profilo dell'interpretazione analogica in *malam partem*), discende che per tutte le ipotesi di dichiarazioni diffamatorie contenute in un sito *internet* non potrebbero applicabili né l'art. 13, l. 47/1948, che punisce la diffamazione a mezzo stampa, né l'art. 30, c. 4, l. 223/1990, che sanziona la diffamazione commessa tramite trasmissioni radiofoniche e televisive. Al riguardo si ritiene che essendo *internet* un mezzo di informazione del tutto peculiare, non può essere estesa in via analogica (stante il divieto di estensione analogica in *malam partem*[29], fondamentale estrinsecazione del principio del *nullum crimen sine lege,* enunciato dall'art. 25, c. 2, Cost.), la disciplina dettata per la stampa. In questo contesto non trovano inoltre applicazione gli art. 57 (responsabilità

[28] V. Zeno-Zencovich, *La pretesa estensione alla telematica del regime della stampa: note critiche*, cit., 19. In senso conforme anche: G. Corrias Lucente, *Il diritto penale dei mezzi di comunicazione di massa*, cit., 262, secondo il quale «alla nozione di televisione non sono, comunque, riconducibili i servizi di comunicazione che operano su richiesta individuale accessibili per internet».

[29] Difatti, si ricorda che ai sensi dell'art. 14 delle disposizioni sulla legge in generale «le leggi penali e quelle che fanno eccezione a regole generali o ad altre leggi non si applicano oltre i casi e i tempi in esse considerati». In questo senso tra le corti di merito si vedano: Trib. Lecco, 3 ottobre 2014, «È inapplicabile al settore dell'informazione diffusa via internet la disciplina delle disposizioni incriminatrici dettate in materia di carta stampata, su tutte quella di cui all'art. 57 c.p., con ogni conseguenza anche di ordine civile che ne possa derivare»; Trib. Bologna, 18 febbraio 2010, n. 508: «all'ipotesi di diffamazione a mezzo internet non è applicabile la normativa prevista in ordine alla diffamazione a mezzo stampa, atteso che diversamente verrebbe violato il principio generale del divieto di interpretazione analogica "*in malam partem*" che vige in materia penale»; Trib. Oristano, 25 maggio 2000, in *Foro it*., 2000, II, 663 ss., con nota di C. Russo, *Internet, libertà di espressione e regole penali: spunti di riflessione a margine di una pronuncia in tema di diffamazione*: «nell'ipotesi di dichiarazioni diffamatorie contenute in un sito web non si applica né l'art. 13 l. 47/48, che punisce la diffamazione a mezzo stampa, né l'art. 30, 4° comma, l. 223/90, che sanziona la diffamazione commessa tramite trasmissioni radiofoniche e televisive, ma può configurarsi il delitto di diffamazione aggravata ai sensi dell'art. 595, 2° e 3° comma, c.p., consistente nell'attribuzione di fatti determinati mediante «altri mezzi di pubblicità» (nella specie, il reato è stato escluso perché i fatti in questione sono stati ritenuti privi di concreta attitudine diffamatoria nei confronti del querelante)». La sentenza è stata pubblicata anche con nota di P. Costanzo, *Ancora a proposito dei rapporti tra diffusione in Internet e pubblicazione a mezzo stampa*, in *Dir. inf*., 2000, 659 ss.

del direttore responsabile)[30], 57-*bis* (responsabilità dell'editore), 58 (responsabilità dello stampatore) c.p.

Tanto premesso in via generale, la Corte di Cassazione, nel precisare che i *forum online* «non possono essere qualificati come un prodotto editoriale, o come un giornale "*on line"*, o come una testata giornalistica informatica», trattandosi di una semplice *area di discussione* non soggetta alle regole e agli obblighi cui è soggetta la stampa (ad es. indicare un direttore responsabile; registrare la testata, giovarsi delle guarentigie in tema di sequestro che la Costituzione riserva solo alla stampa)»[31], apriva la strada ad un'interpretazione evolutiva laddove lasciava intendere che sarebbe stato possibile giungere a conclusioni diverse per i «*forum* strutturalmente inseriti in una testata giornalistica diffusa per via telematica, di cui costituisca un elemento e su cui il direttore responsa-

[30] Rileva G. Buonomo, *La responsabilità penale*, in E. Tosi (a cura di), *I problemi giuridici di internet*, Milano, 2003, 604: «l'articolo 57 del codice penale, se applicato anche nel caso di diffamazione per via telematica, comporterebbe la responsabilità (penale) per il direttore o il vice-direttore responsabile (...). È evidente il fine cui tendono i sostenitori della tesi della responsabilità diretta del "gestore-direttore": per la persona offesa è certamente più facile ottenere giudiziale tutela nei confronti del (certamente noto) fornitore di servizi, piuttosto che nei confronti del (non sempre noto autore del fatto). A questo punto basterebbe ricordare che il divieto di analogia nell'interpretazione della legge penale (art. 14 della disposizione sulla legge in generale) esclude l'applicazione degli articoli citati al di là dei casi espressamente considerati dalla norma incriminatrice (direttore del periodico a stampa) per chiudere la discussione». Per la giurisprudenza, in questo senso si veda: Cass. pen., sez. V, 5 novembre 2013, n. 10594, in *Cass. pen.*, 3, 2015, 1202 ss., in cui «il direttore di un periodico on-line non è responsabile per il reato di omesso controllo, ex art. 57 c.p., sia per l'impossibilità di ricomprendere detta attività online nel concetto di stampa periodica, sia per l'impossibilità per il direttore della testata on line di impedire le pubblicazioni di contenuti diffamatori "postati" direttamente dall'utenza»; Cass. pen., sez. V, 16 luglio 2010, n. 35511, in *Dir. inf.*, 2010, 895 ss., (con nota di C. Melzi D'Eril, Roma locuta*: la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica on-line*) secondo cui «il direttore di periodico "on line" non risponde del delitto di omesso controllo ex art. 57 c.p. in relazione ai reati ivi commessi (nella specie diffamazione a mezzo di lettera ivi inserita), non rientrando le comunicazioni telematiche nel concetto di "stampa"»; App. Roma, 11 gennaio 2001, in *Dir. inf.*, 2001, 31: «l'art. 2 l. 47/1948 prevede l'obbligo di un direttore responsabile solo per i giornali a stampa, il quale assume i relativi doveri a seguito della prescritta registrazione; alla edizione telematica dello stesso giornale, non costituendo stampato e non essendo assoggettato a registrazione, non sono estendibili in *malam partem* le responsabilità previste dalla legge penale per il direttore responsabile dell'edizione a stampa».

[31] Cass. pen., sez. III, 11 dicembre 2008, n. 10535, in *Foro it.*, II, 2010, 95 ss. (con nota di M. Chiarolla, *Riflessioni intorno al concetto di prodotto editoriale digitale*), continua la Corte, gli «interventi dei partecipanti al forum in questione, invero, non possono essere fatti rientrare nell'ambito della nozione di stampa, neppure nel significato più esteso ricavabile dalla L. 7 marzo 2001, n. 62, art. 1, che ha esteso l'applicabilità delle disposizioni di cui alla L. 8 febbraio 1948, n. 47, art. 2 (legge sulla stampa) al "prodotto editoriale", stabilendo che per tale, ai fini della legge stessa, deve intendersi anche il «prodotto realizzato... su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico». Il semplice fatto che i messaggi e gli interventi siano visionabili da chiunque, o almeno da coloro che si siano registrati nel forum, non fa sì che il forum stesso, che è assimilabile ad un gruppo di discussione, possa essere qualificato come un prodotto editoriale, o come un giornale on-line, o come una testata giornalistica informatica. Si tratta quindi di una semplice area di discussione, dove qualsiasi utente o gli utenti registrati sono liberi di esprimere il proprio pensiero, rendendolo visionabile a tutti gli altri soggetti autorizzati ad accedere al forum, ma non per questo il forum resta sottoposto alle regole ed agli obblighi cui è soggetta la stampa (quale quello di indicazione di un direttore responsabile o di registrazione) o può giovarsi delle guarentigie in tema di sequestro che l'art. 21 Cost., comma 3, riserva soltanto alla stampa, sia pure latamente intesa, ma non genericamente a qualsiasi mezzo e strumento con cui è possibile manifestare il proprio pensiero. D'altra parte, nel caso in esame, neppure si tratta di un forum strutturalmente inserito in una testata giornalistica diffusa per via telematica, di cui costituisca un elemento e su cui il direttore responsabile abbia la possibilità di esercitare il controllo (così come su ogni altra rubrica della testata)».

bile abbia la possibilità di esercitare il controllo (così come su ogni altra rubrica della testata)»[32].

Tale tendenza evolutiva è stata inizialmente intercettata nelle decisioni di alcuni Tribunali[33] e, recentemente, è stata ulteriormente delineata, dapprima, dalle sezioni unite penali[34] e poi dalle sezioni unite civili[35], le quali hanno indicato, tra i compiti del giurista, quello di «interpretare il sistema giuridico esistente per verificarne la tenuta ed adattare alla nuova realtà, benché in magmatica evoluzione, gli istituti e le discipline esistenti in coerenza quanto meno coi principi generali o fondamentali che si ritengano di persistente validità».

In particolare tali ultimi due recenti arresti giurisprudenziali hanno precisato:

- che il «dato informatico in sé, in quanto normativamente equiparato a una "cosa", può essere oggetto di sequestro, da eseguirsi, avuto riguardo al caso concreto, secondo determinate modalità espressamente previste dal legislatore e nel rispetto

[32] In questa linea evolutiva si veda anche Cass. pen., sez. V, 25 febbraio 2016, n. 12536, in *Foro it.*, II, 2016, c. 359: « È legittimo il sequestro preventivo di un sito, qualificato blog anche dal suo gestore, che sia stato utilizzato per commettere il reato di diffamazione e manchi degli elementi necessari a individuare una testata giornalistica telematica (nella specie, era stata dal giudice di merito valorizzata l'assenza del carattere della periodicità regolare delle pubblicazioni, della testata e della registrazione), non rilevando in senso contrario la natura dell'attività informativa svolta dal sito medesimo, né la circostanza che il gestore fosse iscritto all'ordine dei giornalisti».

[33] Trib. Milano, 21 giugno 2010, in *Guida dir.*, 44, 28 ss., con nota di J.A. Dudan - C. Melzi d'Eril, *In assenza dei presupposti previsti dalla norma inapplicabili le garanzie sulla non sequestrabilità*; Trib. Padova (ord.), 1 ottobre 2009, in *Foro it.*, I, 2009, 3225. Nonché, in anticipo su tutti, sempre Trib. Milano, 16 maggio 2002, n. 6127, in *Resp. civ. prev.*, 2004, 214 ss., con nota di S. Peron, *Sull'applicabilità della normativa del sequestro di stampati alle testate telematiche.*

[34] Cass. pen., sez. un., 29 gennaio 2015, n. 31022, pubblicata e annotata in numerose Riviste, quali: *Riv. pen.*, 2015, 831 ss., con nota di V. Vartolo, *In tema di sequestro preventivo della pagina web di testata giornalistica on line; Processo penale e giustizia*; *Giur. it.*, 2015, 2002 ss., con nota di S. Lorusso, *Un'innovativa pronuncia in tema di sequestro preventivo di testata giornalistica on line*; *Cass. pen.*, 2015, 3437 ss., con nota di L. Paoloni, *Le sezioni unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa: «ubi commoda, ibi et incommoda»?*; *Dir. inf.*, 2015, 468 ss., con nota di G. Corrias Lucente, *Le testate telematiche registrate sono sottratte al sequestro preventivo - Qualche dubbio sulla «giurisprudenza legislativa»*; *Giur. costit.*, 2015, 1055 ss., con nota di L. Diotallevi, *La Corte di cassazione sancisce l'«equiparazione» tra giornali cartacei e telematici ai fini dell'applicazione della disciplina in materia di sequestro preventivo: un nuovo caso di «scivolamento» dalla «nomofilachia» alla «nomopoiesi»?*; *Processo penale e giustizia*, 6, 2015, 62 ss., con nota di A. Pulvirenti, *Sequestro e Internet: dalle sezioni unite una soluzione equilibrata ma «creativa»*; *Dir. pen. e proc.*, 2016, 201 ss., con nota di B. Piattoli, *Il sequestro preventivo di una pagina web: il funzionalismo della rete e le sue intersezioni nelle dinamiche processuali*. Nonché anche in: *Foro it.*, I, 2016, c. 3753, con nota di A. Palmieri; *Guida Dir.*, 2015, 33, 64, n. Amato; *Guida Dir.*, 2015, 38, 82 (m), con nota di C. Melzi D'Eril – G.E. Vigevani.

[35] Cass. civ., sez. un., 18 novembre 2016, n. 23469.

del principio di proporzionalità»[36];

- che nel contesto della realtà digitale della rete, il sequestro preventivo - tenuto conto della peculiare realtà nella quale va ad incidere - consiste in una «inibitoria rivolta al fornitore di connettività, che deve impedire agli utenti l'accesso al sito o alla singola pagina *web* incriminati ovvero rimuovere il *file* che viene in rilievo, con l'effetto di arrestare l'attività criminosa in atto o scongiurare la commissione di ulteriori condotte illecite»;
- che, ove «ricorrano i presupposti del *fumus commissi delicti* e del *periculum in mora*, è ammissibile, nel rispetto del principio di proporzionalità, il sequestro preventivo *ex* articolo 321 c.p.p. di un sito *web*, o di una singola pagina telematica, anche imponendo al fornitore dei relativi servizi di attivarsi per rendere inaccessibile il sito o la specifica risorsa telematica incriminata»[37];
- che alla nozione di stampa possono ricondursi sia i giornali tradizionali che quelli telematici, laddove anche quest'ultimi siano caratterizzati: «da una testata, dalla diffusione regolare, dall'organizzazione in una struttura con un direttore responsabile che sia giornalista professionista o pubblicista, una redazione ed un editore registrato presso il registro degli operatori della comunicazione, dalla finalizzazione all'attività professionale di informazione diretta al pubblico, per tale intendendosi quella di raccolta e commento di notizie di attualità e di informazioni da parte di soggetti professionalmente qualificati»[38];
- che, dunque, anche la «testata giornalistica telematica, funzionalmente assimilabile a quella tradizionale in formato cartaceo, rientra nella nozione di "stampa" di cui alla l. 8 febbraio 1948, n. 47, art. 1 e, pertanto, non può essere oggetto di seque-

[36] Cass. pen., sez. un., 29 gennaio 2015, n. 31022,: «a seguito dell'entrata in vigore della L. 18 marzo 2008, n. 48, di ratifica della Convenzione del Consiglio d'Europa, fatta a Budapest il 23 novembre 2001, sulla criminalità informatica (*cybercrime*) e di adeguamento del nostro ordinamento agli impegni assunti con la medesima Convenzione, il dato informatico è esplicitamente equiparato al concetto di "cosa", che, se pertinente al reato, può essere oggetto di sequestro. La Convenzione, infatti, dopo avere definito all'articolo 1 il concetto di "dato informatico", disciplina nel successivo articolo 19 "Perquisizione e sequestro di dati informatici immagazzinati", stabilendo che "Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di sequestrare o acquisire in modo simile i dati informatici per i quali si è proceduto all'accesso (...). Tali misure devono includere il potere di: a) sequestrare o acquisire in modo simile un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici; b) fare e trattenere una copia di quei dati informatici; c) mantenere l'integrità dei relativi dati informatici immagazzinati; d) rendere inaccessibile o rimuovere quei dati dal sistema informatico analizzato". Al termine "sequestrare" è affiancata l'espressione "acquisire in modo simile", indicativa, come si legge nella relazione esplicativa del Comitato dei ministri del Consiglio d'Europa, degli altri modi con i quali i dati intangibili possono essere resi indisponibili (renderli cioè inaccessibili o rimuoverli dal sistema). Le modifiche apportate, in esecuzione di tale Convenzione, dalla L. n. 48 del 2008 al codice penale e a quello di procedura penale confermano l'assimilazione del dato informatico alle "cose"».

[37] Si veda anche Cass. pen., sez. V, 25 febbraio 2016, n. 12536, in *Foro it.*, II, 2016, 359 ss., secondo cui «è legittimo il sequestro preventivo di un sito, qualificato blog anche dal suo gestore, che sia stato utilizzato per commettere il reato di diffamazione e manchi degli elementi necessari a individuare una testata giornalistica telematica (nella specie, era stata dal giudice di merito valorizzata l'assenza del carattere della periodicità regolare delle pubblicazioni, della testata e della registrazione), non rilevando in senso contrario la natura dell'attività informativa svolta dal sito medesimo, né la circostanza che il gestore fosse iscritto all'ordine dei giornalisti».

[38] Cass. civ., sez. un., 18 novembre 2016, n. 23469.

stro preventivo in caso di commissione del reato di diffamazione a mezzo stampa, in quanto si tratta di prodotto editoriale sottoposto alla normativa di rango costituzionale e di livello ordinario, che disciplina l'attività di informazione professionale diretta al pubblico»[39].

A tale ultimo riguardo le sezioni unite civili hanno precisato che soltanto la stampa che presenti caratteristiche, in «teoria idonee ad offrire una divulgazione di informazione responsabile e professionale, possono meritare anche, da un lato, un sovvenzionamento pubblico e, dall'altro, la tutela preventiva dal sequestro». Ragion per cui, laddove questi «connotati strutturali e funzionali siano posseduti dal giornale pubblicato, non importa se in tutto o in parte, col mezzo telematico, a prescindere anche dall'equipollenza dei metodi impiegati […], si giustifica allora la riconduzione di tale giornale nel concetto di "*stampa*" rilevante ai fini dell'art. 21, 3° comma, Cost. e quindi ai fini dell'esclusione del sequestro od altra forma di controllo preventivo»[40]. Per contro invece, non vengono fatti rientrare nel concetto di stampa i nuovi mezzi di manifestazione del pensiero destinati a essere trasmessi in via telematica, quali *forum, blog*, *newsletter, newsgroup, mailing list*, e *social network*[41].

Il Tribunale di Milano, ha fatto applicazione di questi insegnamenti laddove, dapprima, ha accertato che la testata telematica in questione possedesse tutte quelle «caratteristiche, in teoria idonee ad offrire una divulgazione di informazione responsabile e professionale, e possa, di conseguenza, meritare la tutela preventiva dal sequestro». Dopodiché, ha valutato se le misure richieste in via cautelare dalla parte (o concedibili dal giudice) mirassero ad impedire la «persistenza nella Rete o l'ulteriore circolazione o diffusione dell'articolo - o equipollente - di giornale telematico ritenuto diffamatorio o comportino un effetto ad esso equivalente».

A tale ultimo riguardo il Tribunale, in un'ottica di bilanciamento tra i diritti costituzionali in gioco ed osservato che la natura pervasiva e diffusiva dell'informazione *online* non può portare ad un giudizio di inammissibilità nei confronti di qualunque tutela cautelare atipica, ha colto l'occasione per aggiungere un ulteriore tassello chiarificatore

[39] Cass. pen., sez. un. 29 gennaio 2015, n. 31022.

[40] Cass. civ., sez. un., 18 novembre 2016, n. 23469, la quale precisa che la «periodicità, talvolta richiesta dalla normativa in esame ed in ogni caso imposta per la qualificazione di una pubblicazione come giornale o periodico, sta nella non occasionalità o nella non episodicità o nella non unicità dell'edizione o pubblicazione: cosa che può riscontrarsi in una regolarità di pubblicazione di nuove edizioni (o numeri), unificate dall'identità o perlomeno dalla costanza degli altri elementi sopra descritti; e che, nella stampa telematica periodica, strutturalmente articolata su di un sito tendenzialmente permanente, può risolversi — ai fini che qui interessano e sempre con la vista premessa di grande approssimazione, funzionale all'applicazione di concetti originariamente modellati su realtà fattuali non ancora evolute — anche nel consueto «aggiornamento» delle relative pagine: ciò che, per mantenere un parallelismo meramente descrittivo con la stampa tradizionale, può equipararsi alla lontana ad una «edizione» di un certo giorno o di una certa ora».

[41] Cass. pen., sez. V, 25 febbraio 2016, n. 12536, in *Guida dir.*, 2016, 19, 94 ss.

alla materia[42].

In particolare il Tribunale, da un lato, ha ritenuto di non poter eludere l'esigenza di prevalenza che – in fase cautelare - la Costituzione accorda alla libertà di stampa, sull'onore e la reputazione, ragion per cui sono inammissibili tutti quei provvedimenti che avrebbero l'effetto di comprimere o limitare la predetta libertà; dall'altro lato, ha però giudicato ammissibili tutti quei rimedi i quali, pur «senza giungere ad un risultato pratico equivalente al sequestro e, dunque, senza limitare la formazione dell'opinione pubblica, consentano di informare il fruitore di notizie on line dell'esistenza di "voci contrarie", della "verità soggettiva" del soggetto oggetto della notizia, del potenziale aggiornamento delle informazioni (ad esempio in ragione di sviluppi di indagine o di successive rivelazioni da parte di altre fonti) o, ancora, dell'esistenza di un procedimento giurisdizionale volto all'accertamento della veridicità – anche solo putativa – delle informazioni contenute nell'articolo».

In tal modo, il Tribunale di Milano ha concretamente bilanciato il diritto all'onore e reputazione con libertà di stampa, in modo da non privare di ogni rimedio il titolare del diritto, al quale invece viene lasciata la scelta delle modalità di attuazione della tutela, considerato che, appaiono sicuramente ammissibili, «rimedi di tipo integrativo e correttivo che, peraltro, svolgono un ruolo di promozione del pluralismo *ex* art. 21 Cost.».

Esclusa quindi l'adozione di provvedimenti volti a impedire la diffusione e la permanenza della pubblicazione contenente le notizie ritenute diffamatorie, posto che avrebbero effetti corrispondente a quelli del sequestro, a diverse conclusioni si perviene con l'adozione di provvedimenti che mirano ad un "aggiornamento" della notizia, contenente le precisazioni e le contestazioni dei diritti interessati[43]. Provvedimenti che nel caso di specie il Giudice ambrosiano ha ritenuto di non dover adottare «atteso che […] nello stesso corpo dell'articolo è stato prontamente inserito un link contenente le lettere di precisazioni e spiegazioni inviate per e-mail alla redazione dagli odierni reclamanti».

Da ultimo, per completezza di esposizione si noti che tale rimedio, ad avviso del Collegio giudicante, può assimilarsi all'esercizio del «diritto di rettifica rispetto al quale, è comunque indubbio, che si differenzi per presupposti e disciplina - ed appare compatibile con l'attenuata tutela cautelare di cui godono l'onore e la reputazione rispetto

[42] Scrive il Tribunale che «carattere pervasivo e diffusivo del mezzo di comunicazione telematico e l'idoneità dello stesso a causare danni potenzialmente irreparabili (un'irreparabilità dovuta dagli effetti ormai irreversibili provocati dalla permanenza, on line, di informazioni dal contenuto ancora non verificato per molto tempo) – caratteristiche espressamente richiamate proprio dalle Sezioni Unite – precludano la possibilità di qualificare come inammissibile qualunque tutela cautelare atipica. In tal modo, infatti, verrebbe preclusa la possibilità di una tutela effettiva – nei limiti compatibili in sede cautelare – di un diritto fondamentale, rinviando ad una fase (quella di merito) i cui effetti dannosi dell'illecito (eventualmente accertato) sarebbero ormai irreversibilmente consolidati».

[43] Secondo Cass. civ., sez. III, 5 aprile 2012, n. 5525, in *Resp. civ. prev.*, 2012, 1155 ss. (con nota di G. Citarella, *Aggiornamento degli archivi online, tra diritto all'oblio e rettifica «atipica»*): «così come la rettifica è finalizzata a restaurare l'ordine del sistema informativo alterato dalla notizia non vera (che non produce nessuna nuova informazione), del pari l'integrazione e l'aggiornamento sono invero volti a ripristinare l'ordine del sistema alterato dalla notizia (storicamente o altrimenti) parziale. L'aggiornamento ha in particolare riguardo all'inserimento di notizie successive o nuove rispetto a quelle esistenti al momento iniziale del trattamento, ed è volto a ripristinare la completezza e pertanto la verità della notizia, non più tale in ragione dell'evoluzione nel tempo della vicenda».

alla stampa». La rettifica[44], difatti, trova fondamento nel «più ampio diritto all'identità personale, la cui lesione legittima il titolare all'esercizio dei rimedi speciali apprestati dal citato articolo 8 della legge sulla stampa e di quelli ordinari generalmente consentiti dall'ordinamento, tra cui anche il rimedio risarcitorio»[45]. Essa dunque non è diretta a realizzare la verità oggettiva dell'informazione, ma è diretta ad arricchire la divulgazione di una notizia con una verità soggettiva, costituita dall'interpretazione dei fatti della persona che si ritiene lesa.

[44] Si ricorda che ai sensi dell'art. 8, l. 8 febbraio 1948, n. 47, il direttore o il responsabile è tenuto a fare inserire nel quotidiano o nel periodico o nell'agenzia di stampa le dichiarazioni o le rettifiche dei soggetti di cui siano state pubblicate immagini od ai quali siano stati attribuiti atti o pensieri o affermazioni da essi ritenuti lesivi della loro dignità o contrari a verità, purché le dichiarazioni o le rettifiche non abbiano contenuto suscettibile di incriminazione penale. La norma esclude ogni discrezionalità in capo al direttore responsabile il quale è gravato da un vero e proprio obbligo, cui corrisponde una posizione di diritto soggettivo dell'interessato, che trova limite esclusivamente nell'ipotesi di rilevanza penale delle dichiarazioni o delle rettifiche (cfr. *ex multis* Cass. civ., sez. III, 24 novembre 2010, n. 23835, in *Dir. inf.*, 2011, 231 ss., con nota di M. Dimattia, *Funzione della rettifica e aggravamento del danno da reputazione*).

[45] Cass. civ., sez. III, 24 aprile 2008, n. 10690, in *Resp. civ. prev.*, 2009, 148 ss., con nota di S. Peron, *Sul corretto esercizio del diritto di rettifica*.

Tra diritto all'oblio e libertà di informazione: la sussistenza dell'interesse pubblico alla diffusione di una notizia*

Francesca Paruzzo

Corte di Cassazione, sez. I civile, 20 marzo 2018, n. 6919

Il diritto all'oblio può subire una compressione a favore del diritto di cronaca solo qualora quest'ultimo sia esercitato in presenza di specifici e determinati presupposti che vanno, così, ad aggiungersi, per il suo lecito esplicarsi, alle condizioni previste dal decalogo del giornalista: il contributo arrecato dalla diffusione dell'immagine o della notizia ad un dibattito di interesse pubblico; l'interesse effettivo ed attuale alla diffusione dell'immagine o della notizia (per ragioni di giustizia, di polizia o di tutela dei diritti e delle libertà altrui, ovvero per scopi scientifici, didattici o culturali), da reputarsi mancante in caso di prevalenza di un interesse divulgativo o, peggio, meramente economico o commerciale del soggetto che diffonde la notizia o l'immagine; l'elevato grado di notorietà del soggetto rappresentato, per la peculiare posizione rivestita nella vita pubblica e, segnatamente, nella realtà economica o politica del Paese.

Sommario

1. Premessa. Il caso. - 2. Il contesto. Cenni. - 3. La rilevanza del caso pratico nel bilanciamento tra oblio e libertà di informazione. Tra giurisprudenza civile e penale. - 3.1. Notorietà delle persone coinvolte e sussistenza di un interesse pubblico alla divulgazione. - 3.2. Tra giurisprudenza civile e penale. Diverse prospettive di bilanciamento.

Keywords: Diritto all'oblio, Diritto di cronaca, Interesse pubblico, Caso concreto, Riservatezza.

1. Premessa. Il caso.

Quali sono i casi in cui un soggetto può pretendere che una notizia, per quanto in passato legittimamente diffusa, non resti indeterminatamente esposta alla possibilità di nuova divulgazione? In che termini può ritenersi sussistente l'interesse pubblico a che vicende proprie di una persona siano oggetto di (ri)pubblicazione, comprimendo, così, il diritto all'oblio del singolo in favore dell'esercizio della libertà di manifestazione del

* L'articolo è stato sottoposto, su determinazione della direzione, a referaggio anonimo.

pensiero e del diritto di cronaca e critica?
Sono questi i temi al centro dell'ordinanza della Corte di Cassazione, sez. I civile, 6 dicembre 2017[1], n. 6919 riguardante la nuova diffusione, a distanza di cinque anni dalla prima, di un servizio televisivo in cui veniva mostrata la reazione di un noto cantante che, raggiunto dalla troupe di un programma Rai fuori da un ristorante, rifiutava in modo secco e perentorio di rilasciare un'intervista. Tale episodio veniva così riproposto all'attenzione del pubblico – all'insaputa dell'artista - al solo fine di collocarlo all'interno di una classifica dei «personaggi più antipatici e scorbutici del mondo dello spettacolo».
Nel caso in esame, la Corte ritiene che un episodio del genere costituisca «un fatto del tutto inidoneo ad aprire un dibattito di pubblico interesse e – men che mai – rispond[a] quelle ragioni di giustizia, di sicurezza pubblica o di interesse scientifico o didattico, che sole possono giustificare una nuova diffusione della vicenda da parte di una trasmissione televisiva. […] Il pregiudizio all'identità personale dell'artista, scaturente dalla violazione del diritto all'oblio, risulta pertanto del tutto evidente».
L'ordinanza in commento sembra così confermare un tendenza che vede la giurisprudenza civile e quella penale, pur partendo imprescindibilmente entrambe dall'analisi del caso concreto e della sua rilevanza pubblica, bilanciare in modo differente i diversi principi in gioco: libertà di manifestazione del pensiero, un lato, diritto all'oblio e diritti della personalità alla cui tutela il primo è funzionalmente volto, dall'altro.

2. La definizione del contesto. Cenni.

Il diritto all'oblio[2], quale «giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni arrecati dalla reiterata pubblicazione di una notizia, pur legittimamente divulgata in passato»[3], sorge e si affina nell'ambito di un rapporto di reciproca limitazione tra i diritti della personalità[4] - e, tra questi, quello all'identità per-

[1] Pubblicata in data 20 marzo 2018.

[2] In dottrina, sul diritto all'oblio si vedano *ex multiis* E. Gabrielli (a cura di), *Il diritto all'oblio*. Atti del Convegno di Studi del 17 maggio 1997, Napoli, 1999; T.A.Auletta, *Diritto alla riservatezza e "droit à l'oubli*", in G. Alpa - M. Bessone - L. Boneschi - G. Caiazza (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, 127 ss.; A. Masaracchia, *Diritto alla riservatezza e "droit à l'oublii",* in *Giurisprudenza costituzionale,* 1997, 3018 ss.; G. Ferri, *Diritto all'informazione e diritto all'oblio*, in *Rivista di diritto civile*, 1990, 801 ss.; M. R. Morelli, *Oblio (diritto all'),* in *Enciclopedia del diritto., Agg.,* VI, Milano, 2002; M. Mezzanotte, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009; A. Mantelero, *Il diritto all'oblio dalla carte stampata a Internet in* F. Pizzetti (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, 145 ss.; in giurisprudenza si segnalano: Cass. civ., sez. I, 18 ottobre 1984, n. 5259, in *Giurisprudenza italiana,* 1985, 762 ss.; Cass. civ., sez. III, 9 aprile 1998, n. 3679, in *Foro italiano*, 1998, 123 ss. e nel merito Trib. Roma 27 novembre 1996, in *Giustizia Civile*, 1997, 1979 ss. e Trib. Roma, ord. 27 novembre 1996, in *Diritto d'autore*, 1997, 372 ss.

[3] Cass. civ., sez. III, 9 aprile 1998, n. 3679.

[4] . Cfr *ex multiis* A. De Cupis, *I diritti della personalità,* Milano, 1959; D. Messinetti, *Personalità (diritti della),* in *Enciclopedia del diritto,* Milano, Vol. XXXIII, 1983, 355; P. Rescigno, *Personalità (diritti della),* in *Enciclopedia Giuridica,* Roma, Vol. XIII, 1990; F. Gazzoni, *Manuale di diritto privato*, Napoli, 1997; M. Ricca Barberis, *Diritti della personalità e loro estensione,* Modena, 1956; E. Capizzano, *I diritti tipici della personalità,* Napoli, 1972; P. Perlingieri, *Informazione, libertà di stampa e dignità della persona,* in *Rassegna di Diritto Civile*, 1986, 624 ss.

sonale[5], all'onore, alla reputazione[6] e alla riservatezza, sempre più intesa quale specificazione del diritto all'autodeterminazione informativa[7] - e la libertà di manifestazione del pensiero[8].

Quest'ultima, per il tema che qui interessa, viene in considerazione nella sua declinazione di cronaca[9] e critica[10] giornalistica, le quali, come noto, perché possano lecitamente esplicarsi devono rispettare tre condizioni: 1) la verità dei fatti narrati; 2) la forma civile dell'esposizione degli stessi e della loro valutazione; 3) la sussistenza di un pubblico interesse alla conoscenza della notizia[11].

Sono requisiti, quelli indicati, strettamente connessi[12] e in composizione variabile a seconda che si eserciti un diritto di cronaca o di critica. Se nel primo caso è la verità dei fatti ad assumere carattere determinante, nella critica, invece, i limiti scriminanti si rinvengono primariamente nella rilevanza sociale dell'argomento trattato e nella cor-

---

[5] Formula sintetica per contraddistinguere il «soggetto da un punto di vista globale nella molteplicità delle sue specifiche caratteristiche e manifestazioni […] e per esprimere la concreta ed effettiva personalità individuale [dello stesso] quale si è venuta solidificando […] nella vita di relazione». Cass. civ., sez. I, 22 giugno 1985, n. 3769.

[6] V. Zeno-Zencovich, *Onore e reputazione nel sistema del diritto civile*, Napoli, 1985, 343. Cfr. anche V. Zeno-Zencovich, *Onore, reputazione e identità personale,* in G. Alpa - M. Bessone (a cura di), *La responsabilità civile,* Torino, 1987; G. Santini, *Onore* (*diritto civile*), in *Novissimo Digesto italiano,* Torino, 1965, XI, 685 ss.

[7] F. Pizzetti, *Il prisma del diritto all'oblio,* cit. 30. Il diritto alla riservatezza inizia ad essere declinato anche in termini di potere di controllo sui propri dati personali che devono rispecchiare esattamente l'identità attuale dell'interessato (c.d. autodeterminazione informativa). Precursore di qualsiasi disciplina nazionale è l'art. 8, par. 1, della CEDU. Cfr., *Gaskin c. Regno Unito*, ric. 10454/83 (1989); *Z. c. Finlandia*, ric. 22009/9325 (1997); *Sidabras c. Lithuania,* ric. 59330/00 (2004).

[8] Nei suoi collegamenti con i diritti della personalità, *ex multiis* e senza alcuna pretesa di esaustività. C. Chiola, *Manifestazione del pensiero (libertà di)*, in *Enciclopedia giuridica*, Roma, XIX, 1990; P. Perlingieri, *Informazione, libertà di stampa e dignità della persona*, in *Rassegna di diritto civile,* 3, 1986, 624 ss.; L. Rossi Carleo, *Il diritto all'informazione nei suoi aspetti privatistici*, in *Rassegna di diritto civile,* 2, 1984, 129 ss.; A. Pace - M. Manetti, *Art. 21: la libertà di manifestazione del proprio pensiero*, in G. Branca - A. Pizzorusso, *Commentario alla Costituzione,* Bologna-Roma, 2006; P. Barile - S. Grassi, *Informazione (libertà di)*, in *Novissimo Digesto Italiano*, Torino, Appendice, IV, 1983, 196 ss.; P. Barile , *Libertà di manifestazione del pensiero*, in *Enciclopedia del diritto*, Milano, XXIV, 1974, 424 ss.; A. Loiodice, *Informazione (diritto alla)*, in *Enciclopedia del diritto*, Milano XXI, 1971, 472 ss.; P. Ceretti, *Pensiero (libertà di)*, in *Novissimo Digesto italiano*, Torino, XXII, 1965, 865 ss.; V. Crisafulli, *Problematica della libertà di informazione*, in *Il Politico*, 1964, 285 ss.*;* S. Fois*, Principi costituzionali e libera manifestazione del pensiero,* Milano, 1957; F. Carnelutti*, Diritto alla vita privata. Contributo alla teoria della libertà di stampa*, in *Rivista trimestrale di diritto e procedura civile*, 1953, 3 ss.

[9] Il diritto di cronaca ha trovato un primo riscontro giurisprudenziale nei primi anni Sessanta come causa di giustificazione *ex* art. 51 c.p. dei reati contro l'onore e la reputazione. Cfr. Cass. pen., sez. V, 5 marzo 1960, n. 103, in *Giustizia Penale*, 1961, II, 103 ss. e, in dottrina, A. Pace - F. Petrangeli*, Cronaca e critica (diritto di),* in *Enciclopedia del diritto,* Milano, 1991, 306 ss.

[10] Cfr. A. Pace - F. Petrangeli , *Cronaca e critica (diritto di),* cit., 303 ss.; M. Pelissero, *Diritto di critica e verità dei fatti*, in *Rivista italiana di diritto penale*, 1992, 1227 ss.; E. Vincenti , *Esercizio del diritto di critica e diffamazione a mezzo stampa*, in *Giurisprudenza di merito*, 1990, II, 120 ss.; A. Nappi, *Ingiuria e diffamazione*, in *Enciclopedia giuridica*, Roma, 1989, XVII, 8; cfr. anche Cass. pen., sez. V, 18 febbraio 2004, n. 11920 e Cass. pen., sez. un., 30 maggio 2001, n. 37140, Cass. pen., sez. V, 6 novembre 2001, n. 13685; Cass. pen., sez. V, 8 febbraio 2000, n. 3477.

[11] Cass. civ., sez. I, 18 ottobre 1984, n. 5259. In dottrina, cfr. S. Pugliatti, *Conoscenza e diritto*, in *Enciclopedia del diritto*, Milano, IX, 1961, 45 ss.; A. Falzea, *I fatti di conoscenza*, in Aa.Vv., *Scritti in onore di Salvatore Pugliatti*, Milano, 1978, I, 533 ss.; G. Catalisano, *Il ruolo del diritto di cronaca e di critica nell'attività giornalistica: profili di diritto dell'informazione,* Milano 2013, 18.

[12] Cass. civ., sez. III, 4 febbraio 2005, n. 2271 e Cass. civ., sez. III, 15 dicembre 2004, n. 23366; cfr., inoltre, Cass. civ., sez. III, 29 agosto 1990, n. 8963.

rettezza delle espressioni adoperate: tale diritto, infatti, si differenzia essenzialmente da quello di cronaca in quanto si concretizza «nell'espressione di un giudizio e, più in generale, di un'opinione che, come tale, non può pretendersi rigorosamente obiettiva»[13] e asettica, ma che ha, per sua natura, carattere congetturale[14]. Pertanto, purché il nucleo e il profilo dei fatti pubblicati non sia strumentalmente travisato e manipolato[15], la critica, per non presentare profili di illiceità, deve limitarsi a non trascendere in attacchi e aggressioni personali diretti a colpire sul piano morale la figura del soggetto interessato[16]; la continenza dell'espressione, in questo senso, è valutata con riferimento alla forma e alle modalità comunicative utilizzate. Mai in relazione al contenuto: essa, pertanto, «non può essere evocata come strumento oggettivo di selezione degli argomenti sui quali fondare la comunicazione dell'opinione, selezione che, invece, spetta esclusivamente al titolare del diritto di critica»[17].

Rispetto alle tre condizioni così individuate, è sulla pertinenza che incide il diritto all'oblio: la ripubblicazione di una notizia, invero, non deve solo rispondere a un'esigenza di pubblico interesse, ma altresì a una sua (nuova o persistente) attualità[18].

Appare evidente, dal quadro così sinteticamente delineato, che non sia possibile astrarre una regola che consenta di definire, una volta per tutte, le situazioni in cui la libertà di manifestazione del pensiero o il diritto all'oblio siano destinati a prevalere. Tutti i diritti in gioco, infatti, mostrano una struttura dinamica e flessibile, adattabile a realtà diverse e destinata a mutare a seconda della notorietà del personaggio, delle caratteristiche dei fatti in relazione ai quali quest'ultimo invoca di essere dimenticato e del modo di intendere la loro rilevanza pubblica[19]. Nulla toglie, però, che, guardando alle pronunce susseguitesi in questi ambiti, siano riscontrabili alcune tendenze, tutte confermate dall'ordinanza in commento.

---

[13] Cass. pen., sez. V, 2 luglio 2004, n. 2247. Cfr. anche Cass. pen., sez. V, 16 dicembre 1998, n. 935 Cass. pen., sez. V, 14 aprile 2000, n. 7499; Cass. pen., sez. V, 26 settembre 2016, n. 25518.

[14] Cass. pen., sez. V, 28 ottobre 2010, n. 4938.

[15] Cass. pen., sez. V, 6 febbraio 2007, n. 11662.

[16] Cass. pen., sez. V, 6 novembre 2001, n. 13685. Cfr. anche G. Ballarini, *Profili giuridici dell'informazione. Cronaca, critica e satira*, in *Giustizia Civile*, Milano, 2007, 422.

[17] Cass. pen., sez. V, 9 marzo 2015, n. 18170; Cass. pen., sez. V, 15 luglio 2010, n. 36602.

[18] Cass. civ., sez. I, 9 aprile 1998, n. 3679. Quanto a tale ultimo aspetto, pur nelle differenze riscontrabili, in relazione all'esito del bilanciamento tra i principi in gioco fra giurisprudenza civile e penale, risulta particolarmente chiara una pronuncia della Cass. pen., sez. V, 24 novembre 2009, n. 45051, che sottolinea come attualità della notizia e attualità dell'interesse pubblico costituiscano risvolti diversi «di una delle condizioni alle quali è subordinato l'esercizio del diritto di cronaca o di critica» e che, sostanziando il presidio costituzionale della libertà di manifestazione del pensiero, possono giustificare il sacrificio dei diritti della personalità: se, però, il decorso del tempo incide sul carattere attuale del fatto storicamente determinato, non necessariamente influenza anche la rilevanza pubblica della notizia che, al contrario, può persistere o, venuta meno per un certo periodo, può riattualizzarsi, imponendo un contemperamento con il diritto all'oblio nel frattempo maturato.

[19] Cass. pen., sez. un., 30 maggio 2001, n. 37140. G. Ballarini, *Profili giuridici dell'informazione. Cronaca, critica e satira*, cit., 417.

3. La rilevanza del caso pratico nel bilanciamento tra oblio e libertà di informazione. Tra giurisprudenza civile e penale

La Corte di Cassazione, dopo aver ricostruito il quadro normativo e giurisprudenziale di riferimento osserva che, affinché possa valutarsi una compressione del diritto all'oblio in favore di quello di cronaca, il contributo arrecato dalla diffusione dell'immagine o della notizia a un dibattito di pubblico interesse può inferirsi solo dalla necessità di garantire - anche a distanza di molto tempo - «ragioni di giustizia, di polizia o di tutela dei diritti e delle libertà altrui». In tali casi, invero, l'interesse della collettività a conoscere «questi fatti è immanente nella preminente rilevanza del personaggio e/o degli accadimenti che lo riguardano, e come tale si protrae nel tempo, o si riaccende quando un evento […] rende di viva attualità quelle vicende risalenti».
Il diritto all'informazione, al contrario, non può prevalere se, come nel caso da cui l'ordinanza trae origine, la diffusione di una notizia risponde solo a un mero interesse divulgativo, economico e commerciale del soggetto che ne dispone la pubblicazione.
Dall'iter argomentativo seguito dalla Corte sembrano così emergere due aspetti: in primo luogo, come detto, si ribadisce che sono solo le peculiarità del singolo caso concreto e lo scopo informativo che si propone chi rivendica il diritto di diffondere una notizia a definire la sussistenza di un pubblico interesse alla sua pubblicazione; in secondo luogo, poi, si conferma una tendenza che vede nella giurisprudenza civile una maggiore attenzione a forme di tutela del diritto all'oblio rispetto a quella penale, più orientata a garantire effettività ai diritti di cronaca e di critica.

3.1 Notorietà delle persone coinvolte e sussistenza di un interesse pubblico alla divulgazione

In un'epoca in cui la legge generale e astratta non trova più giustificazione integralmente in se stessa e non è più in grado di risolvere le tensioni e le imperfezioni che si riscontrano in ogni società attraverso un sistema di garanzie stabili e definitive[20], la tutela degli interessi coinvolti è rimessa all'interpretazione giuridica che, nel suo essere mossa da finalità essenzialmente pratiche, è chiamata a una regolamentazione delle diverse fattispecie il più adeguata possibile alle aspettative che la dinamica dei diversi rapporti sociali richiede[21].
È solo a partire dal singolo caso, pertanto, che è possibile definire quando possa configurarsi un effettivo interesse pubblico alla conoscenza di certe notizie[22], quando esso

[20] P. Prodi, *Una storia della giustizia. Dal pluralismo dei fori al moderno dualismo tra coscienza e diritto,* Bologna, 2000, 12.

[21] G. Zagrebelsky, *La legge e la sua giustizia,* Bologna, 2009, 189.

[22] Cass. civ., sez. I, 27 maggio 1975, n. 2129. Era già stata la pretura di Roma, con sentenza del 25 gennaio 1979 in *Il Foro italiano,* 1975, 1155 ss., a individuare i criteri applicati dalla giurisprudenza nell'ammettere la legittimità di molte rievocazioni storiche: notorietà e attenzione della collettività per le vicende nel periodo in cui queste sono accadute, interesse storico a esse correlato, attualità dell'interesse generale al riesame dei fatti.

possa essere considerato attuale e in che termini, sulla sua sussistenza, possa incidere la notorietà[23] di chi invoca la tutela del proprio diritto all'oblio: invero, quanto a quest'ultimo aspetto, più la vita di una persona è strettamente connessa a quella del contesto sociale di appartenenza, più l'interesse a che la notizia che la riguarda possa far parte della memoria collettiva[24] diventa rilevante, fino a prevalere rispetto alla protezione della riservatezza[25].

Nell'ordinanza in commento la Corte di Cassazione esclude che nella fattispecie in esame possa prevalere la libertà di informazione rispetto all'oblio, proprio perché la riproposizione in televisione, a distanza di cinque anni, del rifiuto di rilasciare un'intervista da parte del cantante, in alcun modo può costituire un rilevante interesse per la collettività.

Si segna, in questo modo, una netta distanza tra la vicenda sottoposta all'attenzione della Corte e altri episodi, alla base di pronunce da quest'ultima richiamate, fondati su fatti criminali, connessi a interessi economici o politici preminenti o volti alla «salvaguardia dell'ordine pubblico o della sicurezza delle persone»; rispetto a essi, afferma la Corte, l'interesse pubblico a conoscerli – anche a distanza di molto tempo – è immanente.

Se scopo informativo, contenuto della notizia e notorietà dei personaggi coinvolti sono i fattori che devono orientare l'opera dei giudici, a partire dall'ordinanza in commento emerge – e si conferma – l'individuazione di alcune condizioni la cui sussistenza consente di indirizzare l'esito ermeneutico nel senso, a seconda dei casi, della prevalenza della libertà di informazione o del diritto all'oblio.

Interessanti spunti, utili per definire il quadro entro cui l'ordinanza si muove, sono offerti dalle Linee guida relative alla corretta applicazione della sentenza Google Spain, adottate il 26 novembre 2014 dal Gruppo di lavoro Articolo 29. In tale documento si stabilisce, infatti, che il diritto all'oblio non è invocabile qualora le notizie di cui non si vuole una nuova divulgazione riguardino persone caratterizzate da un ruolo pubblico e si riferiscano «ai reati più gravi»[26].

Pronunce successive, tanto interne quanto provenienti da organi di giurisdizione internazionali, avallano questa impostazione (talvolta estendendone la portata anche oltre il presupposto della gravità del fatto criminoso): ad esempio, è negato il diritto all'o-

---

[23] Afferma la Corte, in Cass. pen., sez. V, 6 ottobre 2015, n. 6911, che la trasmissione, da parte di un giornalista che abbia assunto la posizione di terzo osservatore, di dichiarazioni, espresse da un personaggio noto, lesive della reputazione di un'altra persona nota, è lecita proprio in considerazione della notorietà degli individui coinvolti; ancora, Cass. pen., sez. V, 26 settembre 2014, n. 48712, Cfr. anche CEDU, *Mengi c. Turchia*, ric. 13471/05 (2013). Importanti, poi, sono le Linee Guida adottate il 26 novembre 2014 relative all'attuazione della sentenza della Corte di giustizia dell'Unione europea *Google Spain c. Google* in tema di diritto all'oblio che sanciscono la «prevalenza dell'interesse generale del pubblico ad avere accesso alle informazioni quando l'interessato esercita un ruolo pubblico, anche per effetto della professione svolta e dell'albo professionale a cui è iscritto».

[24] A. Mantelero, *Il diritto all'oblio dalla carta stampata a Internet,* in F. Pizzetti (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, 150.

[25] A. Pace - M. Manetti, *Art. 21. La libertà di manifestazione del proprio pensiero. Onore e reputazione*, cit. 280 ss.; P. Nuvolone, *Cronaca (libertà di),* in *Enciclopedia del diritto*, Roma, IV, 424 ss.; in giurisprudenza, cfr. Cass. pen., sez. V, 26 giugno 2003, n. 27778; Cass. pen., sez. V, 2 aprile 2004, n. 15595.

[26] «*As a rule, DPAs are more likely to consider the de-listing of search results relating to relatively minor offences that happened a long time ago, whilst being less likely to consider the de-listing of results relating to more serious ones that happened more recently. However, these issues call for careful consideration and will be handled on a case-by-case basis*».

blio rispetto a fatti collegati a episodi di terrorismo, risalenti al 1975 e riconducibili a soggetti che nell'attualità, lungi dall'adottare un profilo di riservatezza, scelgono consapevolmente di svolgere attività pubblica in ambito politico-sociale[27] o in relazione a vicende che, pur risalenti al 1997, riguardano la commissione di reati gravi e rispondono all'esigenza, da considerarsi preminente, di descrivere in modo analitico le origini del fenomeno mafioso[28]; ancora, il diritto di cronaca è ritenuto prevalente anche nel caso in cui il nominativo di una persona che sia tornata a ricoprire incarichi pubblici o di rilevante interesse economico dopo essere stata coinvolta in procedimenti penali, compaia nuovamente, anche non necessariamente in veste di indagato, nell'ambito di inchieste giudiziarie relative a reati analoghi[29].

Coerente, in tal senso, è, poi, la sentenza pronunciata dalla Corte europea dei diritti dell'uomo nel caso Fuschsmann c. Germania[30]. Si conferma, in questo caso, che il mantenimento nel tempo o la riproposizione di una notizia che associ un soggetto a un contesto criminale costituisce, nei limiti del rispetto di alcuni criteri precisamente individuati[31], un legittimo esercizio della libertà di espressione.

Questi stessi principi, in ultimo, sono fatti propri anche dal Garante della Privacy che, proprio nella connessione tra rilevanza penale dei fatti rispetto ai quali si invoca l'oblio e ruolo pubblico rivestito dalle persone coinvolte, individua l'impossibilità di tutelare il diritto degli interessati a essere dimenticati[32].

Nulla di tutto ciò riguarda la vicenda da cui trae origine l'ordinanza in commento: pertanto, nell'interpretare il contenuto della notizia e nel considerare lo scopo meramente

[27] Trib. Milano, 18 giugno 2015, n. 7610.

[28] Trib. Torino, 14 luglio 2015, n. 4977.

[29] Trib. Milano, 19 agosto 2014, n. 10258. Si veda, in ultimo, anche Cass. civ., sez. I, 3 agosto 2017, n. 38747.

[30] CEDU, *Fuchsmann c. Germania,* ric. 71233/2013 (2017). La vicenda trae origine dal caso di un uomo d'affari ucraino, Boris Fuchsmann, residente in Germania, amministratore di società televisive, su cui il New York Times, nel 2001, aveva pubblicato un articolo riguardante il suo coinvolgimento in attività di corruzione finalizzate proprio a ottenere licenze televisive in Ucraina. Con sentenza emessa nell'ottobre scorso, la Quinta Sezione della Corte Europea dei Diritti dell'Uomo rigetta il ricorso di un cittadino tedesco, proposto sulla base dell'art. 8 CEDU; l'uomo sosteneva che il rifiuto di oscurare un articolo online lesivo della sua reputazione violasse il suo diritto al rispetto per la vita privata.

[31] La Corte richiama espressamente i criteri sanciti in recenti decisioni: CEDU, *Couderc e altri c. Francia*, ric. 40457/2007 (2015); *Axel Springer AG c. Germania*, ric. 39954/2008 (2012); *Von Hannover c. Germania*, ric. 40660/2008 (2012).

[32] Provvedimento del 6 ottobre 2016 [doc. web: 5690378] in cui si afferma che nonostante i fatti oggetto di cronaca risalgano al 2006, sussiste il preponderante interesse pubblico al reperimento di notizie relative a reati particolarmente gravi, quali quelli commessi dal ricorrente a danno della sanità regionale, atteso anche l'attuale interesse dei mezzi di comunicazione di massa e dell'opinione pubblica verso tutti i reati contro la pubblica amministrazione; provvedimento del Garante Privacy n. 4988654 del 31 marzo 2016 in cui si è negato il diritto all'oblio per un ex- terrorista: «nonostante il decorso del tempo dall'accadimento dei fatti, sussiste il preponderante interesse pubblico al reperimento di notizie relative ad una delle pagine più buie della storia italiana, i c.d. "anni di piombo", nella quale il ricorrente è entrato a far parte a pieno titolo macchiandosi di reati di matrice terroristica eversiva dell'ordine democratico». Provvedimento del 24 marzo 2016 [doc. web: 5242797] sotto il profilo del ruolo rivestito dall'interessato nella vita pubblica, «la professione di avvocato esercitata dal ricorrente deve essere considerata "un ruolo pubblico" […] e che le notizie […] su presunte condotte certamente immorali oltre che illegali, quali la circonvenzione di incapace, hanno una indiscutibile rilevanza pubblica, quantomeno al fine di tutela del pubblico rispetto a comportamenti pubblici o professionali impropri».

divulgativo e di intrattenimento della sua diffusione, la Corte esclude la sua rilevanza pubblica e garantisce tutela al diritto all'oblio del personaggio coinvolto.

3.2. Tra giurisprudenza civile e penale. Diverse prospettive di bilanciamento

Nell'accordare tutela al diritto a essere dimenticato – e quindi all'identità personale e alla riservatezza - del cantante interessato dalla vicenda, la Cassazione conferma, altresì, come la giurisprudenza civile e quella penale, con riferimento a questi temi, sembrino aver trovato punti di equilibrio differenti.

La prima, infatti, nel suo essere la sede nel cui ambito il diritto all'oblio ha trovato le prime forme di riconoscimento, tende a valorizzare maggiormente i diritti del singolo alla riservatezza, al controllo sui propri dati e all'identità personale.

Interpretando gli artt. 7 e 11 del d.lgs 196/2003, invero, essa è andata progressivamente a orientare le proprie pronunce partendo da un assunto preliminare: ciascuno può pretendere che le informazioni che lo riguardano siano trattate in modo conforme ai criteri di proporzionalità, necessità, pertinenza allo scopo, esattezza e coerenza con la propria attuale ed effettiva identità personale o morale [33]. Sono criteri, quelli indicati, espressione di principi generali di «solidarietà sociale» dalla cui violazione conseguono profili di responsabilità[34]. In tal senso, pur in presenza di un interesse pubblico alla conoscenza dei fatti divulgati, della loro corrispondenza al vero e di una forma civile di esposizione degli stessi, dal momento che «al soggetto cui i dati pertengono è correlativamente attribuito il diritto all'oblio», non può determinarsi un'automatica compressione di quest'ultimo per il sol fatto della sussistenza di condizioni che renderebbero legittimo l'esercizio dei diritti di cronaca e critica: anche in questi casi è, invero, necessario effettuare una valutazione di proporzionalità, da compiersi in relazione al concreto atteggiarsi dei diritti in contrapposizione[35], tra la libertà di informazione e la lesione che il diritto ad essere dimenticati subirebbe dal lecito esercizio della prima.

L'attenzione che si può rinvenire in sede civile nei confronti dei diritti della personalità – se pur diversamente orientata in funzione del caso concreto e delle sue caratteristiche -, appare molto più lieve se si guarda alle sentenze pronunciate in sede penale: la giurisprudenza penale, invero, nel ribadire che la libertà di espressione deve essere la regola e la sua limitazione una circoscritta eccezione[36], tende generalmente a far sì che, valutata la sussistenza dei requisiti[37] che consentono di configurare le esimenti della cronaca e della critica e appurata l'esistenza di un interesse pubblico - persistente o

[33] Cass. civ., sez. III, 5 aprile 2012, n. 5525; Cass. civ., sez. III, 25 maggio 2000, n. 6877; Cass. civ., sez. III, 24 aprile 2008, n. 10690.

[34] cfr. Cass. civ., sez. III, 20 febbraio 2006, n. 3651; Cass. civ., sez. III, 27 ottobre 2006, n. 23273; Cass. civ., sez. III, 15 febbraio 2007, n. 3462; Cass. civ., sez. III, 27 aprile 2011, n. 9404.

[35] Cass. civ., sez. III, 26 giugno 2013, n. 16111; Cass. civ., sez. III, 9 giugno 1998, n. 5658.

[36] Cass. pen., sez. V, 9 marzo 2015, n. 18170.

[37] Cfr. Cass. pen., sez. V, 19 gennaio 2011, n. 1454; Cass. pen., sez. V, 4 marzo 2005, n. 15986.

rivitalizzato[38] - alla conoscenza della notizia, possa ritenersi «giustificata la violazione di quell'aspetto della dignità - riservatezza che è definito diritto all'oblio»[39]. Una notizia dotata di utilità sociale, quindi, perde rilevanza penale, ancorchè sia capace di ledere l'altrui reputazione, e rende legittimo l'esercizio della libertà di informazione.
Il diritto a essere dimenticati, in conclusione, sembra ribadire la Corte di Cassazione, si muove sul sottile filo che lega la tutela dei diritti della personalità, il diritto di cronaca e la memoria collettiva, all'interno di un panorama informativo che risulta influenzato da continue trasformazioni; trovare il giusto bilanciamento tra queste diverse esigenze è un compito particolarmente complesso che incide sul modo di intendere la democratica evoluzione delle moderne società che, da un lato, fanno del pluralismo delle informazioni e della conoscenza critica il loro pilastro fondamentale e, dall'altro, non possono prescindere dalla tutela della personalità del singolo nelle sue diverse espressioni.

[38] Cass. pen., sez. V, 24 novembre 2009, n. 45051.

[39] Cass. pen., sez. I, 2 aprile 2015, n. 13941.

Responsabilità ISP: chi decide se un contenuto è diffamatorio?

Marco Bellezza

Corte di Appello di Roma, sez. I civile, 19 febbraio 2018, n. 1065

La responsabilità dell'Internet Service Provider deve ritenersi sussistente per le informazioni oggetto di hosting (memorizzazione durevole) soltanto allorquando il provider sia effettivamente venuto a conoscenza del fatto che l'informazione è illecita e non si sia attivato per impedire l'ulteriore diffusione della stessa. In relazione a contenuti potenzialmente diffamatori è ipotizzabile un concorso nell'illecito commesso dagli utenti da parte del provider soltanto al cospetto di un ordine dell'autorità giudiziaria, ovvero dell'utilizzazione di espressioni univocamente lesive dei diritti della persona (ad esempio epiteti insultanti), ma giammai può configurarsi un obbligo di rimozione al cospetto di contenuti informativi di per sé non insultanti e addirittura corredati della indicazione delle relative fonti, comprensive di sentenze passate in giudicato.

Sommario

1. Il caso. – 2. La responsabilità dell'*hosting provider* nell'ipotesi di contenuti potenzialmente diffamatori pubblicati dagli utenti del servizio. – 3. Verso una nuova stagione della giurisprudenza italiana sulla responsabilità dei *provider*?

Keywords: ISP, Responsabilità, Diffamazione, Take down, Decreto E-commerce

1. Il caso.

La vicenda dalla quale ha avuto origine la decisione che si commenta ha riguardato il noto legale ed ex ministro Cesare Previti che innanzi al Tribunale di Roma qualche anno orsono, avviava un giudizio ai sensi dell'art. 702-*bis* c.p.c. al fine di ottenere la condanna della Wikimedia Foundation - fondazione che gestisce la più celebre enciclopedia online - alla rimozione di contenuti presuntivamente diffamatori sui propri servizi, oltre che al risarcimento del danno patrimoniale e non patrimoniale subito dall'attore, in conseguenza della pubblicazione di informazioni presuntivamente diffamatorie sulla biografia che riguardava quest'ultimo presente su Wikipedia.
Nel primo giudizio le domande attoree venivano integralmente rigettate. In quell'occasione il Tribunale osservava, in via preliminare, come non fosse applicabile al caso di specie la disciplina introdotta dal d.lgs. 70/2003, che ha recepito in Italia la Direttiva 2000/31/CE relativa ai servizi della società dell'informazione nel mercato interno, essendo la società convenuta stabilita negli Stati Uniti. Il Tribunale rilevava, in con-

seguenza, che per risolvere la controversia bisognava considerare la disciplina interna partendo dal presupposto che la società convenuta operava quale *hosting provider*, vale a dire in qualità di fornitrice di un servizio consistente nella memorizzazione permanente di informazioni da parte degli utenti dello stesso. Circostanza questa non scalfita, secondo i giudici capitolini, dalle argomentazioni difensive proposte dall'attore.
Nella direzione indicata il giudice di prime cure riconosceva, anzitutto, come non fosse sostenibile l'equiparazione tra *hosting provider* ed editore, escludendo per tal via l'applicabilità dell'art. 11 della l. 47/1948 sui reati commessi con il mezzo della stampa. Il Tribunale passava, quindi, ad analizzare la questione alla luce della disciplina sulla responsabilità per attività pericolose di cui all'art. 2050 c.c. Sotto questo profilo il primo giudice escludeva l'applicabilità della rigorosa disciplina codicistica in quanto sulla piattaforma gestita dalla società convenuta era presente un *disclaimer* generale idoneo ad informare gli utilizzatori della circostanza che la Wikimedia Foundation non garantiva in alcun modo la veridicità delle informazioni pubblicate sulla piattaforma. Infine, e con riferimento ad una una potenziale posizione di garanzia del *provider* in relazione alle informazioni pubblicate dagli utenti del servizio fornito, il Tribunale riconosceva l'insussistenza della stessa alla luce della libertà riconosciuta agli utenti di compilare le voci dell'enciclopedia online e modificare le stesse seguendo le regole della piattaforma. Nel rigettare integralmente le domande attoree il Tribunale rilevava, in conclusione, come, in ogni caso, l'attore non avesse seguito le procedure online predisposte dalla Wikimedia Foundation per richiedere la modifica o la cancellazione di contenuti ritenuti inveritieri presenti sulla piattaforma.
L'attore proponeva appello avverso la decisione del Tribunale affidando il proprio gravame ad un motivo centrale relativo al ruolo e alla conseguente responsabilità della Wikimedia Foundation nella gestione della piattaforma Wikipedia.
Nell'articolato motivo di appello l'attore, nel richiedere l'integrale riforma della decisione, deduceva come il Tribunale avesse errato nel ritenere la Wikimedia Foundation come un mero fornitore di servizi di *hosting,* in quanto la stessa eserciterebbe un controllo sui contenuti pubblicati dagli utenti della piattaforma, tanto da assicurarne l'affidabilità nella *home page* del sito. Inoltre, l'attore valorizzava, tra gli altri elementi evidenziati, come il Tribunale non avesse dato rilievo alla diffida stragiudiziale trasmessa alla convenuta nella quale venivano indicate le false notizie delle quali si chiedeva la rimozione, oltre che non avesse tenuto nel minimo conto l'istanza di mediazione presentata dall'attore, procedura alla quale la convenuta non aveva preso parte.

2. La responsabilità dell'*hosting provider* nell'ipotesi di contenuti potenzialmente diffamatori pubblicati dagli utenti del servizio

La Corte di Appello di Roma con la sentenza in analisi ha rigettato integralmente il gravame presentato dall'attore rilevando la totale infondatezza dei motivi di appello proposti. In particolare, con riferimento al merito della controversia, e dunque all'inquadramento del ruolo e della conseguente responsabilità della Wikimedia Foundation

nella gestione di Wikipedia, la Corte capitolina, nel solco tracciato da una parte della giurisprudenza nazionale intervenuta sul tema[1], si è soffermata sull'ampiezza degli obblighi posti a carico degli ISP nell'ipotesi di contenuti presuntivamente diffamatori caricati sulle piattaforme gestite.

La Corte nell'articolata decisione rileva anzitutto come il Tribunale abbia correttamente qualificato la convenuta come una fornitrice di un servizio di *hosting*. Infatti, nella gestione dell'enciclopedia online la Wikimedia Foundation offre agli utenti uno spazio virtuale sul quale questi ultimi possono pubblicare i propri contenuti nel rispetto delle regole del servizio e senza che la convenuta eserciti un controllo preventivo, o di natura editoriale, sui suddetti contenuti. In questa direzione, evidenzia il Collegio, le affermazioni contenute nella *home page* della piattaforma, contrariamente a quanto sostenuto dall'attore, non rivestono alcun carattere confessorio ma debbono, al contrario, considerarsi enunciazioni generiche volte a illustrare il funzionamento di Wikipedia. Quando si riferisce ai controlli, continuano i giudici, Wikimedia fa riferimento al sistema per la correzione dei contenuti presente sulla piattaforma che l'attore non ha utilizzato con riferimento alla biografia che lo riguardava.

Venendo ai contenuti della diffida trasmessa dall'attore in fase stragiudiziale, la Corte d'Appello evidenzia come la stessa fosse generica e si limitasse ad una indimostrata affermazione di diffamatorietà delle informazioni riportate sulla biografia presente sulla piattaforma. Al contrario, la diffida, al fine di far sorgere in capo al provider un obbligo di attivazione, avrebbe dovuto essere specifica e dettagliata[2] e avrebbe dovuto contenere in particolare «[…] a) le singole affermazioni ritenute non veritiere; b) le ragioni della asserita falsità e le fonti idonee a comprovarlo; c) le modifiche suggerite in guisa da consentire alla comunità degli utenti ed in particolare agli "amministratori" da quest'ultima delegati, l'esecuzione dei controlli richiesti all'esito dei quali, ove positivi, si sarebbe potuta disporre la modifica richiesta».

La Corte prosegue nel percorso argomentativo tracciato, ricordando le regole di base sulla responsabilità dei provider di servizi Internet così come dettate dagli artt. 16 e 17 del d.lgs. 70/2003. E, dunque, l'assenza di un obbligo generale di sorveglianza sui contenuti trasmessi o ospitati e la sussistenza di una responsabilità per i contenuti illeciti solo in caso di mancata attivazione a fronte della "conoscenza" del carattere illecito dei suddetti contenuti. Ed è proprio su quest'ultimo profilo che la Corte capitolina conclude il ragionamento condotto andando ad accertare il carattere diffamatorio o meno delle informazioni controverse.

Sul punto il Collegio non lascia spazio ad interpretazioni alternative: le informazioni contenute nella biografia dell'attore presente su Wikipedia non erano diffamatorie in quanto vere e supportate da idonee fonti, quali, tra tutte, sentenze passate in giudicato.

A fronte dell'assenza di diffamatorietà dei contenuti controversi la Corte di Appello si sofferma, quindi, sull'estensione degli obblighi a carico degli ISP nell'ipotesi di contenuti presuntivamente diffamatori, chiarendo come un obbligo di rimozione sussista a fronte di un ordine dell'autorità giudiziaria ovvero nel caso in cui i contenuti siano «univocamente lesivi dei diritti della persona». Certamente, concludono i giudici di ap-

[1] Cfr. App. Milano, 7 gennaio 2015, n. 29.

[2] Cfr. Trib. Firenze, 25 maggio 2012; App. Milano, 7 gennaio 2012, n.29.

pello, tale obbligo non sussiste in relazione a contenuti informativi di per sé non insultanti e corredati dall'indicazione di fonti che includono sentenze passate in giudicato.

3. Verso una nuova stagione della giurisprudenza italiana sulla responsabilità dei *provider*?

La decisione sin qui commentata riprende, sviluppandoli, dei percorsi argomentativi già tracciati dalla più recente e avanzata giurisprudenza nazionale intervenuta in materia di responsabilità dei fornitori di servizi Internet.
Un aspetto indubbiamente innovativo della decisione si rinviene nei passaggi conclusivi della stessa allorquando la Corte d'Appello sembra operare una distinzione tra contenuti chiaramente illeciti e contenuti che chiaramente illeciti non sono.
Nel primo caso, e quindi a fronte di un ordine dell'autorità competente che abbia accertato l'illiceità di un contenuto o quando ci si trova innanzi a contenuti "univocamente lesivi" dei diritti di terzi il provider che riceva una diffida specifica e dettagliata è tenuto a rimuovere i contenuti in questione. Nel caso in cui non sussistano tali condizioni, il provider, sembra sostenere la Corte, non può operare autonomamente una valutazione circa la lesività dei contenuti e deve, quindi, attendere un ordine dell'autorità competente prima di procedere alla rimozione degli stessi. Si tratta a ben vedere di uno dei punti cardine del regime di responsabilità degli ISP delineato dal legislatore comunitario e quindi trasfuso nella disciplina interna, che risponde all'esigenza di non demandare alla discrezionalità del *provider* delle scelte che, in quanto direttamente incidenti su diritti fondamentali, non possono che essere affidate alle istanze costituzionalmente preposte, prima tra tutte l'autorità giudiziaria ordinaria. Che sia l'inizio di una nuova stagione per la responsabilità dei *provider* nella giurisprudenza italiana?

Deindicizzazione globale degli URL su Google: sì del Garante Privacy, in attesa della Corte di giustizia

Filippo Frigerio

Garante per la protezione dei dati personali, provvedimento n. 557 del 21 dicembre 2017 [doc. web n. 7465315]

In tema di c.d. "diritto all'oblio", al fine di rendere effettiva la tutela assicurata dal diritto europeo, il provider è tenuto a dare seguito alle istanze di rimozione degli URL anche con riguardo alle versioni extraeuropee del motore di ricerca.

Sommario

1. I fatti rilevanti. - 2. Il diritto all'oblio. - 3. Le obiezioni di Google alla deindicizzazione globale. - 4. La decisione del Garante Privacy. - 5. I rapporti tra il diritto nazionale e il principio di territorialità. - 6. Conclusioni.

Keywords: *Google Spain*, Diritto all'oblio, Deindicizzazione, Deindicizzazione globale, Dati personali

1. I fatti rilevanti

Con ricorso del 4 agosto 2017, un professore universitario iscritto all'Anagrafe degli italiani residenti all'estero (AIRE) ha chiesto al Garante Privacy di ordinare a Google la deindicizzazione di 26 *link*, i quali si riferirebbero a contenuti "gravemente offensivi" della sua dignità e della reputazione. A parere del ricorrente, gli articoli a cui si riferiscono i *link* riguardano informazioni attinenti al suo stato di salute e ad asseriti reati dallo stesso commessi.

Egli ha affermato di non essere sottoposto ad alcun procedimento penale per i fatti attribuitigli. Questi contenuti risulterebbero quindi essere falsi e, a dimostrazione di ciò, sono sforniti di qualsivoglia supporto probatorio. Infine, gli articoli richiamati dai *link* di cui è causa conterrebbero sue fotografie ottenute e pubblicate senza aver mai richiesto il suo preventivo consenso.

Il ricorrente ha chiesto, quindi, il riconoscimento in proprio favore del diritto all'oblio nei confronti di Google, che non aveva dato seguito alle istanze rivoltele dal ricorrente. Deindicizzazione che – a parere del ricorrente – sarebbe dovuta avvenire globalmente e non limitatamente al territorio italiano ed europeo.

Al contrario, Google ha sostenuto che non esistessero i presupposti per il ricono-

scimento del diritto alla deindicizzazione per una serie di ragioni. In primo luogo, i contenuti contestati sono molto recenti (del 2017) e quindi non ricorrerebbe l'elemento temporale richiesto per poter accedere alla tutela richiesta. In seconda battuta, il ricorrente sarebbe un personaggio avente un "ruolo nella vita pubblica", in quanto professore universitario, imprenditore e autore di varie pubblicazioni. Infine, gli articoli riportano notizie di gravi reati commessi dal ricorrente che, a causa di questi ultimi, sarebbe addirittura destinatario di un'azione collettiva civile e penale.
Google, pertanto, non sarebbe in grado di determinare la verità della notizia, né avrebbe il dovere di farlo. Il ricorrente, infatti, può rivolgersi alle competenti Autorità giudiziarie per tutelare il proprio onore e la propria reputazione, laddove ritenga che questi siano stati lesi. In virtù della logica di funzionamento del motore di ricerca, quest'ultimo non è dotato della capacità di verifica sulla veridicità o meno di una notizia a cui rimanda il *link*.
Mette conto rilevare che, nel corso del procedimento, il ricorrente ha chiesto a Google di provvedere alla rimozione di una serie di altri URL mai indicati prima d'ora negli atti. La richiesta è legata al fatto che per ogni URL deindicizzato dai siti indicati nel ricorso (tra cui il sito www.ripoffreport.com) ne vengono creati altri di analogo tenore. Il ricorrente ha quindi richiesto la deindicizzazione permanente del suo nominativo dai siti indicati .

2. Il diritto all'oblio

Come noto, nel contesto digitale il diritto all'oblio, *rectius* il diritto a ottenere la deindicizzazione dal motore di ricerca degli *link* riguardanti l'interessato, trova il suo fondamento nella sentenza *Google Spain* della Corte di giustizia[1].
La portata di questo diritto ha formato oggetto di un ampio e corposo dibattito in dottrina e in giurisprudenza, al fine di circoscriverne e delimitarne con la maggiore cura possibile ambiti e confini, e così ridurre la discrezionalità del *provider* dei servizi nel riscontrare le istanze degli interessati. Sul punto è intervenuto pure il Working Party 29 con l'*opinion* WP225, che ha fornito delle linee guida per l'implementazione di questo diritto, proprio alla luce della sentenza *Google Spain*[2].
Oggi, quel diritto trova, o almeno parrebbe trovare, conferma positiva nel Regolamento (UE) 2016/679 ("GDPR"), precisamente nei considerando 65 e 66 e all'art. 17. Avuto riguardo all'ambito di applicazione del GDPR previsto dall'art. 3 dello stesso, le previsioni sul trattamento dei dati – e quindi anche del "diritto all'oblio" – si applicano anche ai titolari e ai responsabili non stabiliti nell'Unione europea quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi a soggetti interessati che si trovano nell'Unione, indipendentemente dall'esistenza di un'obbligazione di pagamento da parte dell'interessato.

[1] CGUE, C-131/12, *Google Spain* (2014).

[2] Article 29 Data Protection Working Party, *Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment On "Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González" C-131/12*, WP 225, Adopted on 26 November 2014.

In quest'ottica, quindi, vi sarebbero argomenti per sostenere l'obbligo del titolare di dare seguito a una istanza di cessazione del trattamento dei propri dati personali non solo a livello europeo, bensì globale – laddove ne ricorrano le condizioni e laddove risulti applicabile il GDPR.

3. Le obiezioni di Google alla deindicizzazione globale

Con specifico riferimento a quanto qui interessa, ovverosia alla questione della "deindicizzazione globale", Google si è fermamente opposta sostenendo in diritto che la tutela dei dati personali in questo caso ha come fondamento le disposizioni della direttiva (CE) 95/46, del Trattato dell'Unione Europea e del Trattato sul funzionamento dell'Unione Europea.
Come tali, pertanto, i diritti fatti valere hanno un ambito applicativo limitato al territorio europeo. Invero, la Corte di giustizia ha stabilito che il bilanciamento di interessi tra il diritto all'oblio e la libertà di informazione deve essere effettuato con riguardo alla normativa europea e dello Stato membro nel quale l'istanza è stata formulata e, comunque, nell'ambito dei sistemi giuridici dell'Unione europea.
La resistente ha inoltre aggiunto che la questione sulla deindicizzazione globale è attualmente all'esame della Corte di Giustizia dell'Unione Europea nella causa C-507/17.
In sede d'appello avverso un provvedimento della Commission Nationale de l'informatique e des Libertés (CNIL) (l'Autorità privacy nazionale), il Conseil d'État francese ha sospeso il giudizio e formulato tre questioni pregiudiziali alla Corte di giustizia, richiedendo sostanzialmente un'interpretazione autentica dell'ambito di applicazione dello stesso diritto sancito in prima battuta proprio dalla stessa Corte[3].
Le domande poste ai supremi Giudici europei sono le seguenti.

> «Se il «diritto alla cancellazione», come sancito dalla Corte di giustizia dell'Unione europea nella sentenza del 13 maggio 2014 1 sulla base delle disposizioni di cui agli articoli 12, lettera b), e 14, lettera a), della direttiva del 24 ottobre 1995 2 , debba essere interpretato nel senso che il gestore di un motore di ricerca, nel dare seguito a una domanda di cancellazione, è tenuto ad eseguire tale operazione su tutti i nomi di dominio del suo motore, talché i link controversi non appaiano più, indipendentemente dal luogo dal quale viene effettuata la ricerca avviata sul nome del richiedente, e anche al di fuori dell'ambito di applicazione territoriale della direttiva del 24 ottobre 1995.
> In caso di risposta negativa alla prima questione, se il «diritto alla cancellazione», come sancito dalla Corte di giustizia dell'Unione europea nella summenzionata sentenza, debba essere interpretato nel senso che il gestore di un motore di ricerca, nel dare seguito a una richiesta di cancellazione, sia tenuto solamente a sopprimere i link controversi che appaiono in esito a una ricerca effettuata a partire dal nome del richiedente sul nome di dominio corrispondente allo Stato in cui si ritiene sia stata effettuata la domanda di cancellazione o, più in generale, sui

[3] GU 2017, C 347, 22.

nomi di dominio del motore di ricerca corrispondenti alle estensioni nazionali di tale motore per tutti gli Stati membri dell'Unione europea.
Inoltre se, a complemento degli obblighi richiamati nel precedente punto, il «diritto alla cancellazione», come sancito dalla Corte di giustizia dell'Unione europea nella summenzionata sentenza, debba essere interpretato nel senso che il gestore di un motore di ricerca, quando accoglie una richiesta di cancellazione, è tenuto a sopprimere, con la tecnica del «blocco geografico», da un indirizzo IP che si ritiene localizzato nello Stato di residenza del beneficiario del «diritto alla cancellazione», i risultati controversi delle ricerche effettuate a partire dal nome di quest'ultimo, o persino, più in generale, da un indirizzo IP che si ritiene localizzato in uno degli Stati membri assoggettato alla direttiva del 24 ottobre 1995, e ciò indipendentemente dal nome di dominio utilizzato dall'utente di Internet che effettua la ricerca».

Al fine di evitare pronunce difformi, Google ha quindi chiesto al Garante Privacy di sospendere temporaneamente il procedimento, in attesa della decisione della Corte di giustizia sul caso di cui sopra.

4. La decisione del Garante Privacy

Accogliendo le doglianze del ricorrente e disattendendo le istanze di Google, il Garante Privacy non ha sospeso il giudizio e ha ordinato a quest'ultima di «rimuovere, entro venti giorni dalla ricezione del presente provvedimento, gli URL tuttora deindicizzati fra i risultati di ricerca ottenuti digitando il nome e cognome del ricorrente, sia nelle versioni europee che extraeuropee, estendendo tale attività anche agli Url già deindicizzati nelle versioni europee di Google».
Per quanto concerne le altre istanze del ricorrente, il Garante Privacy ha dichiarato l'inammissibilità della richiesta di deindicizzazione degli URL non indicati nell'interpello preventivo e nell'atto introduttivo e ha dichiarato il non luogo a provvedere in ordine alla richiesta di rimozione dei *link* che non vengono visualizzati dal motore di ricerca mediante digitazione del nome e cognome del ricorrente o deindicizzati nelle versioni europee del motore di ricerca Google.

5. I rapporti tra il diritto nazionale e il principio di territorialità

Per mezzo di questo provvedimento, il Garante Privacy ha esteso l'ambito applicativo del diritto alla deindicizzazione non solo all'interno dell'ambito dell'Unione europea, ma bensì a livello globale. Ciò significa che qualsiasi ricorrente cittadino italiano potrebbe chiedere e ottenere dal motore di ricerca un provvedimento che imponga la deindicizzazione dei risultati di ricerca che lo riguardano da tutte le versioni di Google disponibili nel mondo.

L'estensione a livello globale di questo diritto, allo stato non sancito da alcuna convenzione internazionale, pone inevitabili problemi in merito alla regolamentazione di Internet e al principio di territorialità e di sovranità.
È ancora oggetto di ampio dibattito, infatti, la decisione della Corte Suprema del Canada nella controversia *Google, Inc. v. Equustek Solutions, Inc.*[4]. I Supremi Giudici canadesi hanno confermato la decisione delle Corti inferiori che avevano riconosciuto il diritto del ricorrente di ottenere la deindicizzazione di taluni URL non solo in Canada, bensì a livello globale.
Una vittoria a metà, poiché, investita della questione, la United States District Court (Northern District of California)[5] ha negato efficacia nel territorio statunitense alla pronuncia per probabile violazione dell'art. 230 del Communication Decency Act del 1996. Questa fonte normativa si pone come scudo alla responsabilità del *provider*, con l'obiettivo di proteggere la libertà di espressione su Internet. Invero, ai sensi della legge statunitense, un *provider* come Google non può essere considerato quale editore delle informazioni presenti sul proprio servizio su richiesta di un fornitore di contenuti terzo.
Il Giudice americano ha quindi rilevato che Google rispetta i requisiti di cui all'art. 230 del Communication Decency Act e, pertanto, non può essere considerato responsabile delle informazioni fornite da terzi. Diversamente, sostiene il Giudice, i Tribunali canadesi hanno trattato Google come un editore, in violazione della legislazione sopra richiamata. Per questo motivo, l'ordine di rimozione non può essere riconosciuto negli Stati Uniti.
In Italia, in un caso riguardante la violazione di diritti d'autore, nella sentenza *DeltaTV v. Google/YouTube* del Tribunale di Torino il Collegio ha ordinato a Google/YouTube «la cancellazione e comunque la rimozione dai propri sistemi informatici, o dai sistemi informatici di terzi con cui le convenute intrattengano rapporti contrattuali per la memorizzazione e la conservazione, degli audiovisivi» di cui si discuteva nell'ambito di tale giudizio[6].
Con ciò, i Giudici hanno dimostrato di non ritenere sufficiente il c.d. *geoblocking*, ovverosia il mero oscuramento del contenuto ritenuto illecito in modo tale da renderlo inaccessibile alle connessioni provenienti da un determinato luogo o paese – da individuarsi mediante analisi dell'indirizzo IP. Nella motivazione, il Collegio ha precisato che «i video non sono stati rimossi ma solo oscurati, di modo che essi sono comunque visibili dall'estero ovvero dallo stesso territorio italiano con accorgimenti di facile approntamento (simulando cioè una connessione dall'estero)».

6. Conclusioni

La pronuncia qui annotata e le decisioni analizzate brevemente pongono problemi

[4] *Google Inc., v. Equustek Solutions, Inc.*, [2017] 1 S.C.R. 34 (Can.).

[5] *Google LLC v. Equustek Solutions, Inc.*, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017).

[6] Sia consentito richiamare F. Frigerio, *Il Tribunale di Torino interviene sulla responsabilità degli Internet Service Provider*, in *questa Rivista*, 1, 2017, 169 ss.

simili in materie completamente differenti tra di loro.

Se, da un lato, per taluni diritti potrebbe apparire facile individuare un "comune sentire" fra differenti sistemi giuridici, dall'altro lato la recente esperienza ha mostrato come l'esistenza di visioni diverse in merito alla tutela dello stesso diritto possa condurre a soluzioni opposte[7].

Se si consente a un Giudice di riconoscere validità a una propria pronuncia al di fuori dei confini nazionali e – conseguentemente – di creare un diritto là dove prima non c'era, il principio di territorialità viene inevitabilmente compromesso e con esso la certezza del diritto.

Occorre un ripensamento a livello globale della regolamentazione di Internet o sarà la auto-regolamentazione e l'attività incessante delle Corti a trovare le soluzioni adeguate a questi temi? Il dibattito è aperto.

[7] Il riferimento è alla decisione *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1181, 1194 (N.D. Cal. 2001), ancorché successivamente riformata dalla US Court of Appeals for the Ninth Circuit - 433 F.3d 1199 (9th Cir. 2006) rigettando le istanze di Yahoo!, Inc..

Note a Sentenza
Sezione comparata

Consumatori tedeschi vs. Facebook: la condanna del social network per violazione della normativa sul trattamento dei dati personali

Egle Urso

Corte distrettuale di Berlino, 24 gennaio 2018

La Corte Regionale di Berlino ha condannato Facebook per violazione delle norme sul trattamento dei dati personali, in un'azione intrapresa dall'Associazione Nazionale dei Consumatori, dichiarando l'illegittimità di alcune clausole ed impostazioni di default del servizio, sulla base di una mancata acquisizione del consenso all'utenza. La sentenza, alla vigilia dell'entrata in vigore del Regolamento sulla Protezione dei Dati Personali, afferma importanti principi su privacy e consenso, in linea con le indicazioni del legislatore europeo.

Sommario

1. Introduzione. – 2. Impostazioni di default e consenso. – 3. Termini e condizioni d'uso. – 4. "Facebook è gratis e lo sarà sempre"

Keywords: Facebook, Consenso, GDPR, Data protection, Dati personali

1. Introduzione

Lo scorso 28 gennaio, la Corte Regionale Tedesca con sede a Berlino ha, in prima istanza, condannato il noto *social network* per la violazione della normativa nazionale in materia di trattamento dei dati personali[1], oltre che della disciplina relativa alle condizioni di servizio a tutela del consumatore, in relazione ad alcune clausole ed impostazioni di *default*, in quanto funzionali a eludere le norme sull'acquisizione del consenso.

La sentenza, pubblicata alla vigilia dell'applicazione del nuovo Regolamento sulla Protezione dei Dati Personali (GDPR), arriva al termine di una battaglia legale durata più di due anni, intrapresa dall'Associazione dei Consumatori Tedeschi (Verbraucherzentrale Bundesverband – VZBV), e stabilisce importanti principi sulle modalità di acquisizione del consenso per il trattamento dei dati personali, oltre che sulla liceità di alcuni fra i più noti termini del servizio.

La Corte ha valutato la compatibilità delle clausole e impostazioni contestate con la

[1] Legge federale sulla protezione dei dati personali, (Bundesdatenschutzgesetz - BDSG).

vigente normativa, accogliendo circa la metà delle doglianze attoree, constatando in particolare:
la violazione della normativa sul trattamento dei dati e delle norme per l'acquisizione del consenso, in relazione ad alcune impostazioni di *default*;
la violazione delle norme sull'equità di termini e condizioni, in relazione ad alcune clausole inserite nella *policy* di Facebook, fra cui la clausola che impone agli utenti l'utilizzo del loro vero nome;
la liceità dello slogan "Facebook è gratis e lo sarà sempre".

2. Impostazioni di default e consenso

La Corte ha innanzitutto dichiarato invalide cinque clausole di *default* inserite nelle impostazioni del noto *social network*, sulla base di una mancata acquisizione del consenso informato all'utenza. Fra queste, un'impostazione pre-attivata nell'applicazione *mobile* che rileva la localizzazione degli utenti durante le chat ed una casella preselezionata nelle impostazioni privacy, che autorizza il collegamento della *Timeline* dell'utente a motori di ricerca esterni, rendendo in questo modo i profili facilmente accessibili tramite una semplice ricerca web.
Secondo la legge federale tedesca sulla protezione dei dati, che traspone la Direttiva Europea (Direttiva 95/46/CE), i dati personali possono essere raccolti e processati solo con il consenso dell'utente, e tale consenso dovrà essere ovviamente *«informato»*, e basato su una *policy* chiara ed accessibile con riferimento a natura, scopo e finalità del trattamento. Nel caso di specie, la Corte ha rilevato come tali impostazioni di *default* non possano costituire una lecita modalità di acquisizione del consenso, in quanto non forniscono informazioni chiare e complete sul trattamento dei dati personali degli utenti quando questi accedono ed utilizzano la piattaforma; pertanto, secondo la Corte tedesca gli utenti non essendo effettivamente consapevoli delle modalità di trattamento dei dati che forniscono a Facebook, sono indotti a prestare un consenso *«disinformato»*, che non può ritenersi conforme ai requisiti della normativa vigente, e l' utilizzo continuato del servizio, sottolinea ancora la Corte, può essere considerato alla stregua di un implicito consenso[2].
La posizione della Corte sull'acquisizione del consenso risulta perfettamente in linea, oltre che con la vigente normativa europea, con il nuovo GDPR, applicabile dal 25 maggio 2018. Il nuovo art. 4, n. 11, infatti, definisce il consenso come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento». La normativa specifica ancora, al Considerando 32, che il consenso debba essere espresso «mediante un atto positivo inequivocabile», escludendo invece tassativamente «il silenzio, l'inattività o la preselezione di caselle». Sul punto insiste anche il parere del Gruppo

[2] https://www.williamfry.com/newsandinsights/news-article/2018/02/21/german-court-finds-facebook-default-settings-unlawful

di Lavoro ex art. 29 della direttiva 95/46/EC[3], che sottolinea ancora una volta l'importanza della manifestazione chiara ed inequivocabile del consenso, e precisa come l'utilizzo di caselle pre-selezionate sia invalido sulla base del Regolamento e come il silenzio o l'inattività da parte dell'utente, insieme con la mera continuazione nell'utilizzo del servizio, non possano essere considerate quali indicazioni attive di un consenso.

3. Termini e condizioni d'uso

Lo scrutinio della Corte tedesca ha colpito inoltrealcune clausole presenti nei Termini e Condizioni del servizio (otto per la precisione), ed in particolare una clausola che autorizza il trasferimento di dati personali negli Stati Uniti ed un consenso pre-formulato all'utilizzo di nomi e foto profilo degli utenti per finalità commerciali, incluse profilazione e marketing. La Corte ha in particolare accolto le doglianze attoree, ritenendo che tali «dichiarazioni preformate» non possono costituire un «effettivo consenso» al trattamento dei dati, in quanto questo risulta «inquadrato in modo troppo vago».
Uno degli aspetti della sentenza che ha sicuramente destato più attenzione mediatica, è la dichiarazione di invalidità della clausola che permette agli utenti di registrarsi solo utilizzando il vero nome e cognome; tale pronuncia ha infatti destato delle perplessità, anche alla luce della recente normativa tedesca, entrata in vigore lo scorso gennaio, volta alla repressione di reati ed abusi commessi online attraverso *social network*, che prevede importanti sanzioni per la diffusione su tali piattaforme di *hate speach* e *fake news*
Secondo il giudicante tedesco, una clausola che condiziona la registrazione e l'utilizzo di un servizio all'uso del vero nome dell'utente, e non permette invece la registrazione sotto pseudonimi o anche in forma anonima, deve essere dichiarata invalida, poiché ritenuta una «modalità celata» di acquisizione del consenso al trattamento dei dati, in quanto l'utente, al fine di utilizzare i servizi offerti da Facebook, non ha altra scelta che fornire i propri dati personali, essendogli invece precluso un utilizzo in forma anonima o pseudonima
L'associazione dei consumatori aveva in realtà sostenuto, davanti alla Corte, che tale clausola fosse in contrasto con la normativa domestica sulle telecomunicazioni[4], che prevede invece l'obbligo per i *service providers* di permettere anche l'utilizzo anonimo (o sotto pseudonimo) ai propri utenti; la Corte tuttavia si è limitata a riconoscere l'illegittimità della clausola per viziata acquisizione del consenso, senza invece pronunciarsi sulla compatibilità con la suddetta normativa.
La decisione tedesca, offre qui alcuni interessanti spunti di riflessione.
Innanzitutto, la *policy* del *«real name»* che al più consente l'uso di diminutivi, abbreviativi o vezzeggiativi, di fatto permette a Facebook di raccogliere dati reali e precisi sui propri utenti, anche per successivi trattamenti, e di esercitare su questi un controllo in maniera molto più agevole.
In questo senso, è stato osservato come tale *policy* potrebbe risultare incompatibile con il nuovo principio di minimizzazione dei dati previsto dal GDPR (art. 5, c. 1, lett. c),

[3] Gruppo di Lavoro ex art. 29; *Linee guida sul Consenso,* 10 aprile 2018

[4] German Telemedia Act, Sezione 13 n. (6)

che impone che i dati personali siano «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati»[5]. Qualora si adotti questo approccio, e si consideri dunque non strettamente necessario fornire il vero nome e cognome al fine di fruire dei servizi di un *social network*, si dovrebbe riconsiderare la compatibilità con la imminente normativa, anche delle clausole di altri servizi che subordinano la registrazione a questo requisito.

Sotto un diverso profilo, invece, tale sentenza andrebbe letta anche alla luce sopra citata legge tedesca sull'*hate speech*, entrata in vigore solo pochi mesi fa, che si rivolge nello specifico ai maggiori *social media* e prevede importanti sanzioni per la mancata pronta rimozione (entro 24 ore) di contenuti manifestamente illeciti. Quali contenuti costituiscano effettivamente *hate speech* rimane impossibile da stabilire *a priori*, e proprio questo aspetto della normativa ha attirato diverse critiche da parte di coloro che ravvisano in una tale rigida disciplina una minaccia alla libertà di espressione online. In questo senso dunque, la registrazione tramite *real name* sarebbe rilevante in termini di *accountability* e di *enforcement* della disciplina in materia di diffamazione, permettendo a Facebook (insieme agli altri maggiori *social network* interessati dai nuovi obblighi), un più agevole controllo sull'utenza e facilitando, dunque, l'identificazione in caso di illeciti.

Tale *policy,* dunque, si porrebbe all'interno del dibattito fra coloro che vedono l'anonimato su internet quale garanzia non solo della privacy, ma anche della libertà di espressione, da un lato[6], e la necessità di assicurare un'*accountability* degli utenti nei confronti della comunità, dall'altro, anche in relazione alle nuove e più stringenti norme su diffamazione online e sull' *hate speech*. La Corte tedesca, tuttavia, come già accennato, evita di entrare nel merito della questione, dichiarando *a priori* la clausola invalida sulla base di una viziata acquisizione del consenso.

4. "Facebook è gratis e lo sarà sempre"

Gli attori avevano infine contestato al Social Network il suo ben noto slogan "Facebook è gratis e lo sarà sempre" quale forma di pubblicità ingannevole, in quanto gli utenti, seppure effettivamente non corrispondono una somma in denaro per l'utilizzo del servizio, pagano comunque con una diversa «valuta», ovvero i propri dati personali, che Facebook utilizza per finalità di marketing e pubblicitarie. La Corte tedesca ha tuttavia considerato la clausola valida, sulla base della considerazione che un "bene intangibile" come lo sono i dati, non può essere considerato un costo effettivo, e dunque, di conseguenza, lo slogan del sito non trae in inganno gli utenti.

La posizione della Corte sul punto è abbastanza anomala, e controcorrente rispetto al

[5] D. Stella - N. Casazza, *GDPR: Facebook condannata per violazione della privacy e della normativa a tutela dei consumatori,* in *il Quotidiano giuridico,* 13 marzo 2018

[6] Sul punto, l'opinione del Consiglio d'Europa nella Guida dei Diritti Umani per gli Utenti Internet nella quale si afferma come il principio dell'anonimato abbia lo scopo di «garantire una protezione contro la sorveglianza online e favorire la libertà di espressione» e in ciò, gli Stati membri dovrebbero rispettare la volontà degli utenti di Internet di non rivelare la loro identità, principio che va ovviamente bilanciato con la necessità di adottare misure per rintracciare gli autori di atti criminali, conformemente alle normative nazionali e comunitarie; vedi Raccomandazione CM/Rec(2014)6

trend generale delle Corti ed Autorità nazionali, che invece considerano i *data* quali veri e propri *asset* economici, soprattutto in relazione ai grandi colossi del web, quali Facebook e Google, che hanno consolidato nel tempo il loro potere di mercato proprio grazie ai dati degli utenti, e ovviamente basano su questi anche la maggior parte delle loro *revenues*.

In questo senso si inserisce, ad esempio, la posizione dell'Autorità Garante per la Concorrenza tedesca, che sta attualmente indagando su un presunto abuso di posizione dominante di Facebook nel mercato dei *social media*, ritenendo appunto come il potere di mercato di Facebook derivi proprio dalla quantità (e qualità) di dati da questo detenuti; in particolare, l'Ufficio Antitrust Federale ha recentemente presentato i risultati preliminari di un'indagine durata più di 20 mesi, nei quali ha concluso che Facebook ha abusato di una posizione dominante tra i *social network* ottenendo l'accesso a dati di terze parti, attraverso WhatsApp e Instagram, nonché tramite il monitoraggio delle attività degli utenti sul web.

Allo stesso modo anche la Commissione Europea[7], che ha avuto modo di pronunciarsi proprio sull'acquisizione dell'applicazione di messaggistica istantanea da parte di Facebook, ha pacificamente riconosciuto come i dati personali e le preferenze degli utenti abbiano un valore economico concreto e siano oggetto di importanti scambi commerciali , specialmente per aziende come Facebook, e che dunque i dati che gli utenti forniscono, seppure non siano beni tangibili, hanno natura di controprestazione non pecuniaria, dal cui sfruttamento queste aziende ricavano importanti guadagni.

Nonostante questa sentenza porti con sè importanti implicazioni con riguardo al trattamento dei dati e all'acquisizione del consenso da parte dei *social network*, la situazione è ancora in divenire, ed entrambe le parti hanno manifestato l'intenzione di procedere in appello. Non resta dunque che attendere il contributo del Giudice di secondo grado che dovrà, chiaramente, pronunciarsi sulle questioni sulla base del nuovo Regolamento, direttamente applicabile dal 25 maggio.

[7] Caso N. COMP/M. 7217- *Facebook/Whatsapp*

Note a Sentenza
Sezione Europa

Corte di giustizia

Caso Peugeot, secondo la Corte di giustizia UE un canale promozionale su YouTube non è un servizio di media audiovisivo

Ernesto Apa

Corte di giustizia dell'Unione europea, 21 febbraio 2018, causa C-132/17, *Peugeot Deutschland GmbH c. Deutsche Umwelthilfe eV*

Un servizio di media audiovisivo deve avere come obiettivo principale la fornitura di programmi allo scopo di informare, intrattenere o istruire il grande pubblico, pertanto un canale, ospitato su una piattaforma online come YouTube, che diffonda esclusivamente video pubblicitari di breve durata non può essere considerato un servizio di media audiovisivo ai sensi della direttiva 2010/13/UE

Sommario

1. Il caso. – 2. La decisione della Corte. - 3. Interrogativi.

Keywords: Servizi di media audiovisivi, Direttiva SMAV, Piattaforme video, Over-the-top, Comunicazione commerciale

1. Il caso

Con la sentenza del 21 febbraio 2018 (causa C-132/17), la Corte di giustizia dell'Unione europea si è pronunciata in via pregiudiziale sull'interpretazione da dare alla nozione di "servizio audiovisivo" ai sensi della direttiva sui servizi di media audiovisivi (2010/13/UE) del 10 marzo 2010 (direttiva SMAV).

Poiché la giurisprudenza comunitaria sulla direttiva SMAV, ed in particolare sull'ambito di applicazione della direttiva, è oltremodo esigua, l'esame della decisione della Corte di giustizia e la soluzione adottata per rispondere al quesito del giudice *a quo* presentano profili di sicuro interesse.

La questione pregiudiziale è stata sollevata nell'ambito di una controversia sorta in Germania tra la Peugeot Deutschland GmbH e la Deutsche Umwelthlife eV in relazione ad un breve video promozionale di un nuovo modello di autovettura Peugeot, della durata di circa quindici secondi, pubblicato il 17 febbraio 2014 su un canale video gestito dalla Peugeot Deutschland GmbH sulla piattaforma YouTube.

La Deutsche Umwelthlife eV, un'associazione per la protezione dell'ambiente, sosteneva che la mancata indicazione, in tale video, delle informazioni sul consumo di carbu-

rante e sulle emissioni specifiche di CO^2 dell'autovettura ivi presentata fosse contraria all'art. 5, par. 1, del Regolamento sulle informazioni per i consumatori in materia di consumo di carburante, emissioni di CO^2 e consumo di elettricità di autovetture nuove del 28 maggio 2004 (Verordnung über Verbraucherinformationen zu Kraftstoffverbrauch, CO2-Emissionen und Stromverbrauch neuer Personenkraftwagen). Tale disposizione, infatti, prevede l'obbligo per i costruttori e rivenditori che producono, fanno produrre, distribuiscono o utilizzano in qualunque altro modo materiale promozionale in relazione ad autovetture nuove di indicare i dati ufficiali sul consumo di carburante e sulle emissioni specifiche di CO^2.
Nel giudizio di primo grado, il Landgericht Köln, Tribunale del Land di Colonia, decideva in favore dell'associazione per la protezione dell'ambiente; successivamente la sentenza di primo grado veniva confermata in appello dall'Oberlandesgericht Köln, Tribunale superiore del Land di Colonia.
Adito quale giudice di ultima istanza, il Bundesgerichtshof, Corte federale di giustizia, osservava che lo stesso art. 5 del Regolamento, al par. 2, primo periodo, seconda parte del periodo, escludeva esplicitamente da tale obbligo «i servizi di radiodiffusione e i servizi di media audiovisivi ai sensi dell'articolo 1, paragrafo 1, lettera a), della direttiva 2010/13». Detta corte, pertanto, decideva di sospendere il procedimento e di sollevare una questione pregiudiziale interpretativa alla Corte di giustizia dell'Unione europea per chiedere se un canale video presente su una piattaforma online che consente all'utente di accedere a video pubblicitari di breve durata, sia da considerare un servizio di media audiovisivo ai sensi della direttiva SMAV.

2. La decisione della Corte

La Corte di giustizia, investita della questione relativa all'interpretazione della nozione di servizio di media audiovisivo, ed in particolare dei confini di tale categoria giuridica, ha escluso che il canale YouTube della Peugeot ricada nell'ambito di applicazione della direttiva SMAV. I giudici di Lussemburgo hanno infatti ritenuto che non possa essere qualificato come servizio di media audiovisivo un canale, ospitato su una piattaforma online come YouTube, che diffonda esclusivamente video di natura promozionale.
Tale conclusione è sorretta da una motivazione molto asciutta, che fa leva sugli scopi di natura promozionale perseguiti dal canale in questione, che secondo la Corte sarebbero incompatibili con la qualifica di servizio di media audiovisivo. Per meglio dire, le finalità di un servizio di media audiovisivo non potrebbero esaurirsi in obiettivi di carattere meramente commerciale, in quanto la definizione stessa di servizio di media audiovisivo statuisce che l'«obiettivo principale [del servizio] è la fornitura di programmi al fine di informare, intrattenere o istruire il grande pubblico» (art. 1, par. 1, lett. *a*), punto i) della direttiva SMAV, il cui testo inglese ha il seguente tenore: «*the principal purpose of which is the provision of programmes, in order to inform, entertain or educate*»).
Anche il considerando 22 della direttiva richiama le finalità che concorrono a sagomare l'identità giuridica dei servizi di media audiovisivi: «la definizione di servizi di media audiovisivi dovrebbe comprendere i mezzi di comunicazione di massa in quanto mezzi

d'informazione, d'intrattenimento e di istruzione destinati al grande pubblico e includere le comunicazioni audiovisive commerciali».
A giudizio della Corte, un canale YouTube come quello della Peugeot persegue una finalità diversa, di natura pubblicitaria, e non soddisfa quindi il requisito teleologico che, ai sensi della direttiva, identifica necessariamente i servizi di media audiovisivi. Tale scopo promozionale è di per sé sufficiente ad escludere il canale YouTube in questione dall'ambito di applicazione della direttiva SMAV.
La Corte non nega, che, come Peugeot aveva sostenuto, un video pubblicitario possa informare, intrattenere o istruire gli spettatori. Del resto, anche la dottrina che enfatizza il carattere persuasivo della pubblicità (nell'accezione negativa di pressione emotiva diretta ad escludere le difese razionali), riconosce che essa possiede un insopprimibile gradiente informativo, che era evidenziato autorevolmente già da Paolo Barile e Sergio Fois. Tuttavia, sottolinea la Corte, se pure è vero che un video pubblicitario può informare, intrattenere o istruire il pubblico, «ciò avviene al solo scopo e come strumento per raggiungere il fine promozionale».
In realtà, il considerando 22, sopra citato, esorta ad includere le comunicazioni commerciali, e infatti la definizione di servizio di media audiovisivo consta di due punti, tra loro alternativi, di cui solo il primo evoca le finalità di informazione, intrattenimento, istruzione, mentre il secondo si concentra su un profilo esclusivamente promozionale: «Ai fini della presente direttiva si intende per: a) "servizio di media audiovisivo": i) un servizio, quale definito agli articoli 56 e 57 del trattato sul funzionamento dell'Unione europea, che è sotto la responsabilità editoriale di un fornitore di servizi di media e il cui obiettivo principale è la fornitura di programmi al fine di informare, intrattenere o istruire il grande pubblico […];ii) una comunicazione commerciale audiovisiva». Quindi, sembra che un servizio di media audiovisivo possa consistere semplicemente in una comunicazione commerciale audiovisiva.
La sentenza in commento si interroga su quale sia la portata dello scarno riferimento alla comunicazione commerciale operato al punto ii).
La Corte inizia con l'esame del significato di "comunicazione commerciale audiovisiva", che indica «immagini, sonore o non sonore, che sono destinate a promuovere, direttamente o indirettamente, le merci, i servizi o l'immagine di una persona fisica o giuridica che esercita un'attività economica. Tali immagini accompagnano o sono inserite in un programma dietro pagamento o altro compenso o a fini di autopromozione. Tra le forme di comunicazione commerciale audiovisiva figurano, tra l'altro, la pubblicità televisiva, la sponsorizzazione, la televendita e l'inserimento di prodotti» (art. 1, par. 1, lett. *h*), della direttiva SMAV).
La nozione di "comunicazione commerciale audiovisiva" richiama anche il concetto di "programma", la cui comprensione è quindi necessaria per completare un'analisi che si muove per intero in ambito definitorio. Un "programma" è definito come «una serie di immagini animate, sonore o non, che costituiscono un singolo elemento nell'ambito di un palinsesto o di un catalogo stabilito da un fornitore di servizi di media la cui forma e il cui contenuto sono comparabili alla forma e al contenuto della radiodiffusione televisiva. Sono programmi, ad esempio, i lungometraggi, le manifestazioni sportive, le commedie di situazione (sitcom), i documentari, i programmi per bambini e le fiction

originali» (art. 1, par. 1, lett. *b*), della direttiva SMAV).
La Corte di giustizia, esaminando la definizione di comunicazione commerciale, osserva che essa deve necessariamente accompagnare un programma, o inserirsi all'interno dello stesso, a fronte di un corrispettivo, o comunque di un compenso, o per finalità di autopromozione. I giudici concludono che il canale YouTube della Peugeot presenta video che non si accompagnano ad alcun programma, rappresentando bensì «elementi individuali ed autonomi gli uni dagli altri».
Secondo l'interpretazione propugnata dalla Corte, quindi, la nozione di comunicazione commerciale ai sensi della direttiva SMAV presuppone che il messaggio promozionale sia inserito nell'ambito di un tessuto editoriale, trovando collocazione ancillare rispetto a un programma, ossia a un frammento di palinsesto (o un catalogo non lineare) a carattere informativo, istruttivo o di intrattenimento (come sembra confermare anche l'elenco esemplificativo di programmi: «i lungometraggi, le manifestazioni sportive, le commedie di situazione (sitcom), i documentari, i programmi per bambini e le fiction originali»).
Ne consegue che, per i giudici di Lussemburgo, un servizio di media audiovisivo non potrà risolversi in una mera comunicazione pubblicitaria, avulsa da un contesto editoriale.
Tale conclusione sembra dare luogo ad una sorta di "assorbimento ermeneutico", per cui il punto ii) della definizione di servizio di media audiovisivo, che *ictu oculi* si direbbe giustapposto, diverso ed anzi alternativo al punto i), finisce col risolversi in quest'ultimo. Come si è ricordato sopra, la definizione di servizio di media audiovisivo è organizzata su due livelli: uno si riferisce a un complesso di programmi organizzati da un editore, che persegua lo scopo di informare, intrattenere o istruire il grande pubblico, l'altro si esaurisce in una comunicazione commerciale. Il primo livello è articolato, ruota intorno al concetto di pluralità e organizzazione, mentre il secondo è semplice, contempla un elemento singolo; uno è basato su finalità editoriali, l'altro su uno scopo commerciale. Apparentemente, quindi, sembrerebbe che un servizio di media audiovisivo possa essere dato dall'uno o dall'altro: nel caso Peugeot, però, la Corte di giustizia giunge a conclusioni diverse, negando di fatto uno statuto autonomo al punto ii) e ritenendo che le comunicazioni commerciali non siano idonee a integrare un servizio di media audiovisivo, il quale, per esser tale, dovrà sempre e comunque contenere i programmi di cui al punto i), eventualmente (ma non necessariamente) accompagnati a comunicazioni commerciali.
I due livelli, quindi, per la Corte non si giustappongono: il primo identifica il servizio di media audiovisivo, il secondo, quando è presente, concorre con il primo e va a completarlo, venendone per così dire inglobato.

3. Interrogativi

Questo tipo di interpretazione, affermando il carattere irriducibilmente informativo, istruttivo o di intrattenimento dei servizi di media audiovisivi, si propone di risolvere alcune incongruenze nella formulazione delle definizioni della direttiva SMAV. Nel

farlo, nega spazio a servizi di media audiovisivi che abbiano una connotazione eminentemente promozionale, schiudendo così nuove contraddizioni.
In diversi Stati (inclusi Regno Unito, Germania e Italia) sono saldamente radicati canali di c.d. "*home shopping*", dedicati in maniera esclusiva alla programmazione di televendite, le quali costituiscono una *species* del *genus* comunicazione commerciale per espressa previsione normativa (in base alla definizione, sopra ricordata, di comunicazione commerciale, «Tra le forme di comunicazione commerciale audiovisiva figurano, tra l'altro, […] la televendita […]»).
Dato ancor più rilevante, secondo il considerando 101 della direttiva SMAV «La presente direttiva si dovrebbe applicare ai canali esclusivamente dedicati alla televendita o all'autopromozione, che non comprendono programmi tradizionali quali notiziari, trasmissioni sportive, film, documentari, opere teatrali» e, soprattutto, a mente dell'art. 25 della direttiva «La presente direttiva si applica, per analogia, ai canali televisivi dedicati esclusivamente alla pubblicità e alle televendite, nonché ai canali televisivi dedicati esclusivamente all'autopromozione».
Si potrebbe sostenere che per i soli canali televisivi (quindi servizi lineari) il legislatore comunitario abbia voluto introdurre un'eccezione, che ha richiesto una norma *ad hoc* la quale semmai conferma che la regola generale è stata correttamente ricostruita dalla Corte di giustizia. Ma, a parte che la Corte nella motivazione non argomenta sul punto e non circoscrive mai il suo discorso ai soli servizi *on demand*, va considerato che la traduzione italiana dell'art. 25 sembra infelice nella parte in cui afferma che l'applicazione avverrebbe in via analogica: con «per analogia» (che peraltro sarebbe comunque un termine non corretto, essendo riferito a una fattispecie regolata da espressa previsione normativa) si è malamente tradotto, infatti, il «*mutatis mutandis*» presente in altre versioni della direttiva SMAV, ad esempio in quelle inglese, francese e spagnola. L'espressione «*mutatis mutandis*» non suggerisce un'applicazione analogica o comunque un'estensione dell'ambito di applicazione, ma piuttosto una modulazione delle regole applicabili, essendo evidente che un palinsesto di tal fatta mal si concilierebbe con il rispetto di alcuni obblighi (è infatti espressamente esclusa l'applicazione del capo VI, dell'art. 20 e dell'art. 23 della direttiva SMAV). L'art. 25, che tra l'altro non sarà toccato dal processo di revisione (c.d. *REFIT*) della direttiva SMAV, deve probabilmente il suo *wording* incerto al fatto di essere una riscrittura dell'art. 19 della direttiva Televisione senza frontiere (poi evoluta nella direttiva SMAV), in base al quale alcune disposizioni si applicavano, *mutatis mutandis*, ai canali esclusivamente dedicati alle televendite.
La sentenza in commento, nel richiedere quale requisito necessario che un servizio di media audiovisivo persegua finalità di informazione, intrattenimento e istruzione e nell'escludere che detto servizio possa essere costituito da sole comunicazioni commerciali, che non si accompagnino né interrompano alcun programma, non sembra tener conto di questi riferimenti, al punto che non vengono neanche citati nella ricostruzione del contesto normativo, o comunque non affronta il tema di come l'interpretazione proposta dalla Corte si concili con essi.
In secondo luogo, può essere notato un passo marginale della sentenza, in cui la Corte, replicando a un argomento – invero alquanto specioso – della Peugeot, nega che la natura pubblicitaria vada riferita esclusivamente alle immagini del prodotto oggetto

di promozione o che rechino messaggi reclamistici: la Corte ritiene che l'intero video, comprese quindi le immagini che non riproducono contenuti commerciali, debba essere considerato unitariamente e presenti, nel suo complesso, uno scopo pubblicitario, essendo tale la finalità che ne avvince i vari elementi e lo informa nella sua totalità.
Questa notazione, apparentemente ovvia, può presentare rilievo pratico alla luce delle modalità con cui sono oggi, sempre più frequentemente, costruiti alcuni contenuti televisivi di natura incerta, o comunque "ibrida", che pur avendo pregio editoriale per gran parte della propria durata, presentano, nella parte finale, un messaggio promozionale. Tali contenuti dovranno essere strutturati in maniera conveniente, onde evitare di essere attratti per intero nel computo dell'affollamento pubblicitario, che oggi nella prassi è spesso circoscritto alla sola "coda" di natura schiettamente pubblicitaria.
Infine, sebbene il caso fornisse l'opportunità di chiarire se un canale su YouTube possa, in presenza dei requisiti fissati dal legislatore, essere qualificato come servizio di media audiovisivo, la Corte non ha colto l'occasione ed ha omesso di affrontare il tema. O almeno, non l'ha affrontato esplicitamente: si può sostenere, infatti, che la linea argomentativa seguita dalla Corte, protesa ad accertare se il canale in questione possedesse carattere informativo, educativo o di intrattenimento, implica che qualora la risposta fosse stata positiva, il canale YouTube della Peugeot sarebbe stato un servizio di media audiovisivo, mentre se la natura di servizio di media audiovisivo fosse esclusa in radice dalla distribuzione esclusiva mediante la piattaforma YouTube, non sarebbe stato necessario interrogarsi sulla natura dei contenuti diffusi nell'ambito del canale.
Però, a parte l'intrinseca debolezza che sempre accompagna l'*argumentum a silentio*, c'è da considerare che la Corte potrebbe semplicemente aver valutato diversamente la priorità logica di un argomento rispetto a un altro, ed essendo sufficiente l'esame delle definizioni per escludere che ricorressero i presupposti per qualificare il canale Peugeot come servizio di media audiovisivo, potrebbe aver deciso di non interrogarsi su altri elementi che parimenti potevano condurre ad escludere l'applicabilità della direttiva.
La questione relativa alla natura e al regime giuridico dei canali YouTube è dibattuta, sebbene la decisione adottata da Ofcom a giugno 2017 nel caso P110 Limited sembra far venir meno il principale argomento secondo cui i canali YouTube, ontologicamente, non sarebbero qualificabili come servizi di media audiovisivi.
La Corte avrebbe potuto dire una parola definitiva e chiara su un punto di non secondaria importanza, ma ha tralasciato di farlo, rassegnando una decisione che presenta significative lacune.

Note a Sentenza
Sezione Europa

Corte Europea

I gesti simbolici, anche se provocatori, rientrano nell'ambito della critica politica

Marina Castellaneta

Corte europea dei diritti dell'uomo, 13 marzo 2018, *Stern Taulats e Roura Capellera c. Spagna*, ricc. 51168/15 e 51186/15

I gesti simbolici e provocatori utilizzati per esprimere una critica politica nei confronti di figure pubbliche godono della protezione offerta dall'art. 10 della CEDU che assicura il diritto alla libertà di espressione. In particolare, nei casi di critica politica, espressa attraverso l'atto di bruciare l'immagine dei reali di uno Stato, l'ingerenza delle autorità nazionali deve essere particolarmente limitata proprio per assicurare il pluralismo e il dibattito pubblico. La critica politica gode di una tutela rafforzata soprattutto se manifestata nei confronti di figure pubbliche che sono sottoposte a uno scrutinio più rigoroso da parte della collettività rispetto ai privati. L'atto provocatorio, che non incita alla violenza, non può essere qualificato come forma di hate speech.

Sommario

1. Premessa. – 2. La ricostruzione della vicenda all'origine della pronuncia di Strasburgo. – 3. L'inquadramento di gesti simbolici tra gli atti di critica politica. – 4. L'obbligo di "stretta interpretazione" della fattispecie dell'*hate speech* nel dibattito politico.

Keywords: Libertà di espressione, Critica politica, *Hate speech*, Elementi costitutivi, Proporzionalità della sanzione

1. Premessa

La previsione di reati *ad hoc* all'interno degli ordinamenti nazionali riguardanti offese indirizzate a particolari categorie di persone di alto rango con incarichi che comportano l'esercizio di un potere pubblico incontra un limite grazie alla Corte europea dei diritti dell'uomo. Se a livello nazionale in non pochi ordinamenti è riconosciuta una particolare protezione a componenti di famiglie reali, capi di Stato o di Governo o finanche politici, la Corte di Strasburgo, con la sentenza *Stern Taulats e Roura Capellera c. Spagna* (ricc. 51168/15 e 51186/15) depositata il 13 marzo 2018, ha rafforzato il diritto alla libertà di espressione rispetto alla tutela dell'immagine di figure pubbliche con un ruolo determinante nel Paese come, con riguardo al caso di specie, i reali di Spagna, Juan Carlos I e la regina Sofia. La pronuncia, a nostro avviso, è di particolare rilievo anche perché i principi in essa affermati possono condurre a rivedere scelte legislative

nazionali volte a rafforzare la normale protezione del diritto alla reputazione nei confronti di coloro che rivestono ruoli di Governo o di rappresentanza dello Stato posti, così, sul piano interno, in una posizione privilegiata rispetto agli altri individui (si veda oltre, per l'Italia, l'art. 595 del codice penale). La sentenza, inoltre, chiarisce l'ampio perimetro di applicazione della libertà di espressione ai sensi della Convenzione che copre anche l'utilizzo di gesti simbolici e provocatori e permette di identificare i criteri per qualificare un'espressione (nella forma verbale o di un gesto simbolico) tra i casi di *hate speech*.

2. La ricostruzione della vicenda all'origine della pronuncia di Strasburgo

Il ricorso alla Corte europea era stato presentato da due cittadini spagnoli condannati per offesa alla Corona in base all'art. 490, par. 3, del codice penale. I due ricorrenti, nel corso della visita istituzionale del re di Spagna (in quel periodo Juan Carlo I) a Gerona, in Catalogna, nel 2007, avevano dato fuoco alla fotografia, collocata in una piazza, che ritraeva la coppia reale. L'*Audiencia Nacional*, sezione penale, aveva condannato i due autori ritenendo che l'intento fosse quello di vilipendere i reali, descritti come forza occupante della comunità catalana. La condanna detentiva pari a 15 mesi era stata commutata in una sanzione di 2.700 Euro ciascuno. I due avevano presentato un ricorso alla Corte costituzionale poiché, a loro avviso, era stato violato il diritto alla libertà di espressione garantito dalla Costituzione spagnola. Tuttavia, la Corte costituzionale sosteneva che il gesto implicava un incitamento all'odio e alla violenza verso il re e la monarchia e aveva ritenuto che non vi fosse stata alcuna violazione del diritto alla libertà di espressione. Così, i due giovani hanno presentato un ricorso alla Corte europea dei diritti dell'uomo adducendo una violazione dell'art. 10 che assicura il diritto alla libertà di espressione[1].

Ed invero, Strasburgo ha accertato che si era verificata un'ingerenza nella libertà di espressione dei ricorrenti, prevista dalla legge (come richiesto dalla stessa Convenzione il cui art. 10 ammette limitazioni al diritto in esame), e funzionale a perseguire un fine legittimo come la tutela della reputazione o la prevenzione dei disordini, ma ha dovuto sciogliere l'aspetto più problematico e controverso tra le parti ossia se detta ingerenza potesse essere considerata come necessaria in una società democratica. Sul punto, come è naturale, le parti erano su posizioni divergenti: per i ricorrenti era stato compresso il diritto alla libertà di espressione nell'ambito di un contesto di critica politica, senza che vi fosse alcun bisogno sociale imperativo da proteggere; per il Governo spagnolo, invece, la necessità della misura sanzionatoria era dovuta alla circostanza che

[1] Tra la numerosa bibliografia si vedano, tra gli altri, B. Hale, *Political speech and political equality*, in *Freedom of Expression, Essays in honour of Nicolas Bratza,* Oisterwijk, 2012, 177 ss.; M. Oetheimer - A. Cardone, *Articolo 10*, in S. Bartole - P. De Sena - V. Zagrebelsky (a cura di), *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2012, 397 ss.; M. Verpeaux, *Freedom of expression,* Strasbourg, 2010, 159 ss.; P. Caretti, *Art. 10, Libertà di espressione,* in S. Bartole - B. Conforti - G. Raimondi (a cura di), *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali,* Padova, 2001, 337 ss.; M. Oetheimer, *L'harmonisation de la liberté d'expression en Europe*, Paris, 2001.

l'atto di bruciare l'immagine dei reali costituiva un incitamento all'odio e alla violenza. Proprio tale aspetto ha permesso alla Corte di fornire taluni chiarimenti sui criteri per inquadrare atti non violenti in sé, legati a una contestazione e, quindi, espressione di una propria idea, tra quelli di incitamento all'odio. Ed invero, l'importanza della pronuncia è proprio nel fatto che la Corte ha considerato irrilevante, ai fini dell'indicata qualificazione, la circostanza che successivamente rispetto all'atto contestato si fossero verificati taluni disordini, aspetto che, invece, i tribunali spagnoli avevano ritenuto di particolare rilievo giustificando così la misura sanzionatoria in quanto necessaria – per la protezione di un bisogno sociale imperativo - in una società democratica.

3. L'inquadramento di gesti simbolici tra gli atti di critica politica

Il primo aspetto considerato dalla Corte europea è l'inquadramento dell'atto in discussione - ossia il gesto simbolico di dar fuoco a un'immagine - tra quelli ascrivibili alla discussione/critica politica. La Corte europea, nell'interpretare l'art. 10 della Convenzione e, in particolare, le limitazioni ammissibili all'indicato diritto in quanto misure necessarie in una società democratica, in diverse pronunce, ha tenuto a sottolineare che l'ingerenza dello Stato nei casi di manifestazioni della libertà di espressione nella critica politica è più limitata rispetto ad altre situazioni pur contemplate dall'art. 10. In via generale, le eccezioni poste alla libertà di espressione – sicurezza nazionale, integrità territoriale, ordine pubblico, prevenzione dei disordini e dei reati, protezione della salute e della morale, protezione della reputazione o dei diritti altrui, tutela delle informazioni confidenziali e dell'autorità e imparzialità del potere giudiziario – vanno già interpretate restrittivamente rispetto alla libertà in esame, che garantisce la realizzazione di un duplice diritto (quello di esprimersi e quello di ricevere informazioni a vantaggio, quindi, dell'intera collettività). A ciò si aggiunga che con riguardo alla discussione politica, queste eccezioni assumono una portata ancora più ristretta tenendo conto, evidentemente, dell'importanza della libertà di espressione ai fini della stessa realizzazione della democrazia che passa, come è ovvio, attraverso un dibattito pubblico anche aspro e il pluralismo delle opinioni. A tal proposito, infatti, la Corte europea, con riferimento a notizie che riguardano politici, uomini di governo, individui che rappresentano lo Stato, ha affermato che il margine di apprezzamento concesso agli Stati nell'individuazione di limitazioni è «*particulièrement restreinte*», a differenza dei casi di ingerenza degli Stati per motivi legati alla tutela della morale in cui le autorità nazionali godono di «*une certaine marge d'appréciation*»[2]. Pertanto, l'obbligo di non ingerenza al fine di garantire la realizzazione della libertà di espressione come manifestazione di una propria idea ha un carattere più stringente sugli Stati nel caso di dibattito politico. Così, la Corte europea, già in passato, nell'individuare i parametri da prendere in considerazione per accertare la conformità di limiti alla libertà di espressione nell'arena politica ha sancito che «*It must be recalled that, according to the Strasbourg Court's case-law, there is little scope under*

[2] In tale direzione la sentenza del 21 giugno 2012, *Schweizerische Radio-und Fernsehgesellschaft SRG c. Svizzera*, ric. 34124/06.

Article 10 § 2 of the Convention for restrictions on political speech or on debate on questions of public interest»[3].

In questa direzione, d'altra parte, si muovono anche altri organismi di garanzia posti a tutela dei diritti umani nell'ambito di trattati internazionali di carattere regionale e universale. Basti considerare, in questo senso, la Commissione africana dei diritti dell'uomo, che opera nell'ambito della Carta africana dei diritti dell'uomo e dei popoli del 27 giugno 1981, adottata dall'Organizzazione per l'Unità africana (dal 2001 Unione africana), che sin dalla decisione del 31 ottobre 1998 nel caso *Media Rights Agenda, Constitutional Rights Project, Media Rights Agenda e Constitutional Rights Project c. Nigeria* (ricc. 105/93-128/94-130/94-152/96), con riguardo all'applicazione dell'art. 9 che assicura la libertà di espressione, ha rilevato che «*it should be assumed that criticism of the government does not constitute an attack on the personal reputation of the head of state. People who assume highly visible public roles must necessarily face a higher degree of criticism than private citizens; otherwise public debate may be stifled altogether*»[4]. Nello stesso senso, la Corte interamericana dei diritti dell'uomo, nella pronuncia *Herrera-Ulloa c. Costa Rica* (n. 107) del 2 luglio 2004, con riguardo all'art. 13 della Convenzione americana dei diritti dell'uomo, ha affermato che gli uomini pubblici e i politici devono essere pronti a ricevere critiche più aspre rispetto a quelle rivolte a privati. Sul piano della tutela universale dei diritti dell'uomo, nell'ambito del Patto sui diritti civili e politici del 1966, il Comitato dei diritti dell'uomo, nelle constatazioni rese il 31 ottobre 2005, nel caso *Bodrožić c. Serbia e Montenegro,* ha accertato la violazione dell'art. 19 del Patto, che assicura la libertà di espressione e ha affermato che «*in circumstances of public debate in a democratic society, especially in the media, concerning figures in the political domain, the value placed by the Covenant upon uninhibited expression is particularly high*»[5].

L'orientamento generale degli organi di garanzia nel senso di limitare le ingerenze degli Stati nel dibattito politico ha trovato conferma nella sentenza della Corte europea che, proprio in ragione delle peculiarità nei casi di critica politica e dell'ampliamento del diritto alla libertà di espressione in questo contesto, ha accertato, in via preliminare, se il gesto di dare fuoco all'immagine dei reali potesse essere qualificato come libertà di espressione nel dibattito politico proprio in ragione dell'indicata variabilità del margine di discrezionalità degli Stati nelle possibili limitazioni all'indicato diritto.

Ed invero, l'atto in esame è stato qualificato dalla Corte tra quelli con un evidente significato politico proprio perché il gesto in sé è una messa in scena, una rappresentazione di una critica alla monarchia in generale e, in particolare, a quella spagnola. Sul punto, la Corte tiene a ricordare che l'art. 10 della Convenzione non si limita a tutelare

[3] Si vedano le sentenze *Wingrove c. Regno Unito*, ric. 17419/90 (1996), *Sürek c. Turchia (n. 1),* ric. 26682/95 (1999) e *Nilsen e Johnsen c. Norvegia,* ric. 23118/93 (1999). Cfr. A. Lester, *The right to offend,* in *Freedom of Expression*, cit., 297 ss.

[4] Così il par. 74. La vicenda aveva al centro la decisione del Governo nigeriano di sospendere l'attività di alcuni giornali che erano stati critici verso il Presidente (il provvedimento è nel sito http://caselaw.ihrda.org/doc/105.93-128.94-130.94-152.96/view/). Va ricordato che con il Protocollo di Ouagadougou (Burkina Faso), in vigore dal 25 gennaio 2004, è stata istituita la Corte africana.

[5] Il Comitato, nel provvedimento indicato, ha accolto il ricorso presentato da un giornalista che aveva pubblicato un articolo critico nei confronti di un uomo politico accusandolo di aver dato supporto a Slobodan Milošević (CCPR/C/85/D/1180/2003, comunicazione n. 1180/2003).

unicamente le espressioni inoffensive, ma anche quelle che «disturbano, offendono o scioccano». I due ricorrenti avevano scelto di bruciare la fotografia al termine di una manifestazione politica contro la monarchia, nell'ambito di un dibattito di interesse pubblico come l'indipendenza della Catalogna, proprio con l'obiettivo di criticare i reali e la forma di Governo da loro rappresentata, senza che il gesto contenesse un attacco personale al re, finalizzato a offendere. Una critica senza dubbio aspra su ciò che il re rappresentava ossia una monarchia che, per i ricorrenti, era responsabile dell'occupazione della Catalogna. La fotografia bruciata – osserva la Corte - è un elemento simbolico collegato in modo chiaro, evidente e diretto alla critica politica e l'averla collocata a testa in giù implica un rigetto totale della monarchia. L'atto aveva un fine provocatorio e anche la dimensione dell'immagine mirava a richiamare l'attenzione della collettività presente. Pertanto, si è trattato della messa in scena di una provocazione funzionale a richiamare anche l'attenzione dei media e ad alimentare un dibattito pubblico sulla monarchia e l'indipendenza della Catalogna. Con la conseguenza, quindi, che hanno potuto trovare applicazione i parametri propri della giurisprudenza della Corte europea in materia di critica politica.

Pertanto, ci sembra che la Corte così come concede libertà ai giornalisti nella scelta della forma degli articoli, ritenga necessario, per assicurare un'ampia applicazione del diritto alla libertà di espressione, lasciare spazio a ogni individuo nella scelta di mezzi di diverso genere, naturalmente non violenti, per manifestare una critica politica. In questo contesto, poi, con la sentenza che qui si commenta, ci sembra che la Corte assuma una posizione netta nel negare una protezione speciale – in sostanza un privilegio – a politici o figure di governo e di rappresentanza dello Stato, in modo, quindi, del tutto diverso rispetto a numerosi ordinamenti nazionali, incluso quello spagnolo che all'art. 490 del codice penale citato in precedenza accorda l'indicato privilegio. La posizione della Corte europea, d'altra parte, è in linea con quanto affermato nella Joint Declaration su "Current Challenges to Media Freedom" adottata il 30 novembre 2000 dal Relatore speciale sulla libertà di espressione delle Nazioni Unite, dal Rappresentante sulla libertà dei Media dell'OSCE e dal Relatore speciale dell'Organizzazione interamericana sui diritti dell'uomo nella quale è stata affermata l'importanza di dibattiti pubblici su questioni di interesse generale e che «*public figures are required to accept a greater degree of criticism than private citizens; in particular, laws which provide special protection for public figures, such as desacato laws, should be repealed*». Nella stessa direzione, il Comitato dei Ministri del Consiglio d'Europa, nella Dichiarazione sulla libertà dei dibattiti politici nei *media* adottata il 12 febbraio 2004, al principio n. VI, ha stabilito che «*Political figures should not enjoy greater protection of their reputation and other rights than other individuals, and thus more severe sanctions should not be pronounced under domestic law against the media where the latter criticise political figures. This principle also applies to public officials; derogations should only be permissible where they are strictly necessary to enable public officials to exercise their functions in a proper manner*» [6]. D'altra parte, la stessa scelta effettuata nell'art. 10, par. 2, ossia di ammettere una limitazione alla libertà di espressione con riguardo a determinati ambiti come quello giudiziario proprio per garantirne l'imparzialità e l'autorità dei giudici, senza prevedere una specificazione *ad hoc* per i politici, imponga alla Corte nonché

[6] Il testo è nel sito http://www.coe.int.

ai legislatori e ai giudici nazionali, di non creare situazioni privilegiate per i politici o altre figure pubbliche rappresentative dello Stato[7]. Nei confronti di questi soggetti, e in particolare di ciò che rappresentano, il grado di esagerazione e provocazione può essere particolarmente alto, senza che gli Stati possano prevedere strumenti speciali o ingerenze nei confronti di chi manifesta il proprio pensiero. La Corte, a nostro avviso, è particolarmente attenta a non permettere che gli Stati trasformino il legittimo diritto alla reputazione dei politici in un privilegio per determinate categorie di persone che sono, in quanto soggetti pubblici, dotati di non pochi poteri e, quindi, già beneficiari di una protezione particolare[8]. Pertanto, una legge interna che protegge in modo speciale una determinata categoria di persone pubbliche non è conforme allo spirito della Convenzione e «l'interesse di uno Stato a proteggere la reputazione del proprio capo di Stato non può giustificare il conferimento di una protezione speciale nei casi in cui sia in gioco il diritto ad informare e ad esprimere le proprie opinioni su questo soggetto» (par. 35 della sentenza).

Una conclusione che conferma quanto stabilito nel principio n. III della citata Dichiarazione nella quale si afferma che «*Political figures have decided to appeal to the confidence of the public and accepted to subject themselves to public political debate and are therefore subject to close public scrutiny and potentially robust and strong public criticism through the media over the way in which they have carried out or carry out their functions*» e che dovrebbe portare a ripensamenti in diversi ordinamenti. Questo, anche con riferimento all'Italia perché l'art. 595, c. 3, del codice penale, nei casi di diffamazione a mezzo stampa prevede la reclusione da sei mesi a tre anni o una multa non inferiore a 516 Euro, fissando un aumento di pena se l'offesa è rivolta a un corpo politico, amministrativo o giudiziario o a una sua rappresentanza o autorità costituita in collegio.

4. L'obbligo di "stretta interpretazione" della fattispecie dell'*hate speech* nel dibattito politico.

Quanto detto non esclude che una limitazione possa e, anzi, debba essere applicata nei casi di forme di espressione che promuovono o incoraggiano l'intolleranza fino ad arrivare all'*hate speech*. In diverse occasioni, la Corte europea ha riconosciuto, a partire dalla sentenza del 23 settembre 1994 (*Jersild c. Danimarca*, ric. 15890/89), non solo conforme al testo convenzionale, ma anche necessario l'intervento degli Stati che limitano la libertà di espressione quando la manifestazione di detta libertà è qualificabile come incitamento all'odio, proprio perché l'*hate speech* non è protetto dal diritto alla libertà di

[7] Cfr., tra le tante, la sentenza del 25 giugno 2002, *Colombani e altri c. Francia*, ric. 51279/99, con la quale la Corte ha ritenuto che la norma francese sulla libertà di stampa, che attribuisce uno *status* speciale ai capi di Stato esteri accordando loro una protezione assoluta, è incompatibile con la Convenzione. Va ricordato che con legge *Perben II* del 9 marzo 2004, relativa in generale alla lotta alla criminalità organizzata, è stato modificato l'art. 36 della legge sulla stampa del 29 luglio 1881 proprio a seguito della sentenza *Colombani*, con la soppressione della reclusione nei casi di offesa a capi di Stato esteri. Si veda M. Castellaneta, *La libertà di stampa nel diritto internazionale e europeo*, Bari, 2012.

[8] Nella sentenza *Mamère c. Francia* (ric. 12697/03), del 7 novembre 2016, la Corte europea ha sottolineato che in relazione a questioni di interesse generale e nell'ambito di un dibattito pubblico «*a degree of immoderation is allowed*» (par. 25).

espressione[9]. E questo la Corte lo ha fatto sia considerando il principio dell'abuso del diritto di cui all'art. 17 della Convenzione il quale sancisce che nessuna disposizione della Convenzione «può essere interpretata come implicante il diritto per uno Stato, gruppo o individuo di esercitare un'attività o compiere un atto mirante alla distruzione dei diritti o delle libertà riconosciuti nella Convenzione...»[10], sia tenendo conto delle restrizioni alla libertà di espressione ammesse ai sensi dell'art. 10, par. 2 e, quindi, anche quando l'incitamento all'odio non ha una portata tale da distruggere i valori della Convenzione. È evidente che l'*hate speech* non solo non può ottenere alcuna protezione visto che colpisce, in modo discriminatorio, la dignità della persona, negando così il godimento sistematico di alcuni diritti umani fondamentali, ma deve essere fronteggiato dagli stessi Stati, come precisato nella raccomandazione R(97)20 del 30 ottobre 1997 dal Comitato dei Ministri del Consiglio d'Europa che ha chiesto agli Stati di combattere l'*hate speech* che riguarda «*all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance...*».

È così centrale individuare gli elementi che per la Corte fanno ricadere una determinata manifestazione della libertà di espressione tra gli atti che costituiscono incitamento all'odio e, quindi, giustificato oggetto di divieto da parte delle autorità nazionali[11]. Un punto, questo, che ci appare di particolare importanza anche rispetto a futuri casi che potrebbero arrivare all'attenzione della Corte proprio con riferimento al rapporto tra aspra critica politica e *hate speech*.

Il Governo in causa si è difeso sostenendo che i giudici nazionali avessero applicato la giurisprudenza della stessa Corte di Strasburgo in relazione alle pronunce sui discorsi all'odio. Ed è così evidente che l'accoglimento del ricorso contro lo Stato da parte della Corte europea mostra le difficoltà applicative, in taluni casi, delle norme convenzionali come interpretate dalla Corte, con un sostanziale fraintendimento delle sentenze internazionali da parte dei giudici nazionali. Ed invero, nel caso in esame, i tribunali interni hanno dato particolare rilievo alle modalità con le quali è stata espressa la propria opinione – ossia il dar fuoco a una fotografia dei reali – e alle conseguenze, ossia i disordini pur se successivi alla manifestazione. Un caso, quindi, per i tribunali interni, di *hate speech* legato alle modalità esteriori di manifestazione di un pensiero piuttosto che al contenuto dell'opinione sottesa al gesto simbolico. La Corte europea, invece, ha dato rilievo, ai fini del corretto inquadramento della fattispecie, ad aspetti legati al messaggio in sé, con ciò riconoscendo ampia libertà nelle modalità con le quali esprimere un'opinione, senza violenza fisica. Sul punto, infatti, la Corte di Strasburgo ha precisato che l'atto era inquadrabile come espressione di dissenso e di critica politica, necessa-

[9] Si veda, per un esame completo della giurisprudenza della Corte, il documento dello *Steering Committee for Human Rights*, CDDH(2017)R87, add. III, 13 luglio 2017.

[10] Cfr. M. E. Villiger, *Article 17 ECHR and freedom of speech in Strasbourg pratice,* in *Freedom of Expression*, cit., 321 ss.

[11] Cfr. G. Pitruzzella - O. Pollicino - S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake news,* Milano, 2017; M. Castellaneta, *L'*hate speech*: da limite alla libertà di espressione a crimine contro l'umanità*, in G. Venturini - S. Bariatti (a cura di)*, Diritti individuali e giustizia internazionale, Liber Fausto Pocar*, Milano, 2009, 157 ss.; I. Hare, *Extreme Speech Under International and Regional Human Rights Standards,* in I. Hare - J. Weinstein (a cura di), *Extreme Speech and Democracy*, Oxford, 2009, 62 ss.; A. Weber, *Manual on hate speech,* Strasbourg, 2009.

rio ad attirare l'attenzione dei media, rilevando, altresì, che la tecnica utilizzata non è andata «al di là del ricorso a un certo grado di provocazione», permesso nell'esercizio della libertà di espressione in caso di diffusione di un messaggio critico nel dibattito politico. La circostanza che i ricorrenti abbiano bruciato la fotografia dei reali è stata solo un modo per esprimere l'insoddisfazione e la protesta, necessaria anche a garantire il pluralismo. D'altra parte, ci sembra evidente che l'atto in sé non aveva alcuna manifestazione di violenza nei confronti di persone o cose, trattandosi unicamente di un gesto simbolico, privo di conseguenze sui destinatari del messaggio[12]. Inoltre, non erano indicati simboli del passato che potessero richiamare la commissione di crimini contro l'umanità, situazione che, invece, porta la Corte a ritenere che la diffusione di un'immagine sia *hate speech*, come avvenuto di recente con la decisione del 13 marzo 2018 nel caso *Nix c. Germania* (ric. 35285/16), con la quale la Corte europea ha stabilito la non violazione della Convenzione da parte dello Stato in causa i cui giudici avevano condannato un blogger per la diffusione di immagini di gerarchi e simboli nazisti, pur in assenza di un incitamento alla violenza, con ciò giustificando le norme interne che reprimono la diffusione di immagini e simboli relativi a organizzazioni incostituzionali, in particolare nel caso di simboli nazisti, che richiamano la commissione di crimini di guerra e contro l'umanità.

Pertanto, appare evidente che proprio la circostanza che la Corte, nel caso *Stern Taulats*, abbia deciso in senso opposto rispetto allo Stato in causa, non ritenendo che l'atto di bruciare la fotografia dei reali potesse essere inquadrato nell'ambito dell'*hate speech*, conferma la necessità di circoscrivere l'applicazione dei limiti alla libertà di espressione in un dibattito politico a casi davvero eccezionali. Già in precedenza, d'altra parte, la Corte ha affermato che l'applicazione dell'art. 17 è possibile solo se è "del tutto chiaro" che quanto dichiarato a titolo di libertà di espressione sia manifestamente contrario ai valori convenzionali[13].

Per quanto riguarda l'ulteriore profilo indicato in precedenza, ossia la valutazione delle conseguenze, sul punto è condivisibile la posizione della Corte europea: l'atto in sé non ha portato a manifestazioni di discriminazione o intolleranza nei confronti di gruppi o individui e, certo, ad accogliere la posizione del Governo in causa secondo il quale la classificazione dell'atto tra quelli di *hate speech* era dovuta al fatto che aveva «…*donné lieu à des agissements violents*», ossia a proteste successive dovute all'imputazione dei due ricorrenti, si arriverebbe a un'applicazione del tutto contraria a quella affermata in modo costante dalla Corte europea perché si provocherebbe un allargamento del perimetro di applicazione delle eccezioni e del principio dell'abuso del diritto rispetto invece alla libertà di espressione. Pertanto, la Corte non ha dato rilievo agli incidenti (diremmo

[12] Sulle limitazioni giustificate dalla necessità di impedire l'incitamento alla violenza, si veda G. Bonello, *Freedom of expression and incitement to violence*, in *Freedom of Expression*, cit., 349 ss.

[13] Si veda la decisione *Belkacem c. Belgio* (ric. 34367/14) del 20 luglio 2017 con la quale la Corte ha dichiarato il ricorso irricevibile ritenendo giustificata la condanna di un cittadino belga, portavoce dell'organizzazione radicale salafita "Sharia4Belgium", poi dissolta, condannato dai giudici nazionali per aver diffuso su "YouTube" un video in cui inveiva contro alcuni politici e invitava alla *jihad*. Cfr. M. Castellaneta, *La Corte europea dei diritti umani e l'applicazione del principio dell'abuso del diritto nei casi di hate speech*, in *DUDI*, 2017, 745 ss.
Sulla necessità dell'assoluta chiarezza dell'*hate speech* si veda la sentenza del 17 dicembre 2013, *Perincek c. Svizzera*, ric. 27510/08, par. 114, confermata dalla Grande Camera con sentenza del 15 ottobre 2015.

non di particolare gravità) che, per di più, si erano verificati dopo qualche giorno ed erano stati provocati più dalla repressione penale che dalla manifestazione dei due ricorrenti. A ciò si aggiunga che manifestare in modo aspro un proprio pensiero politico, anche bruciando una fotografia, non ha un collegamento diretto o indiretto con l'incitamento ad atti di violenza, ma costituisce solo un modo per esprimere la propria insoddisfazione e protesta e, quindi, non può essere classificato come un atto manifestamente contrario ai valori convenzionali. Va ricordato che già in passato, sempre con riferimento alla Spagna, la Corte aveva valutato un caso di offesa al re e *hate speech*. Anche in quell'occasione, con la sentenza del 15 marzo 2011, *Otegi Mondragon c. Spagna* (ric. 2034/07), la Corte, rispetto alla condanna penale del portavoce del gruppo parlamentare dei separatisti baschi che aveva indicato il re di Spagna come colui che aveva imposto il regime monarchico con violenza, aveva ritenuto violato l'art. 10 perché, anche se il linguaggio era provocatorio e ostile, non vi era stato incitamento alla violenza o espressioni lesive della dignità umana e, quindi, non era configurabile l'*hate speech*.
Esclusa la possibilità di applicare l'art. 17, la Corte ha così effettuato una valutazione sulla proporzionalità della sanzione, test dal quale prescinde se si configura un caso di *hate speech*, ma non allorquando si tratta di testare l'ingerenza nella libertà di espressione in base alle limitazioni indicate al par. 2 dell'art. 10 della Convenzione e ha ritenuto la sanzione prevista ossia la pena del carcere sproporzionata nel contesto di un dibattito politico.

Secret filming and the right to inform under an European constitutional perspective. The case of *Alpha Doryforiki v. Greece*

Giovanni De Gregorio

European Court of Human Rights, 22 Februrary 2018, *Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece*, app. 72562/10

In the case in question, the European Court of Human Rights dealt with the boundaries of the right to inform in relation to use of secret tools of recording by journalists to conduct interviews on matters of public interest. In particular, the facts involved three video filmed secretly involving a Greek politician. The videos were broadcasted on TV by the applicant which, then, was sanctioned by the Greek authorities. Regarding the first video, the Court ruled that the Greek Courts had violated the applicant, as broadcaster, freedom of expression by imposing sanctions for having secretly filmed video of a politician in a gambling arcade. However, the Court held that there had been no violation in respect of the two other videos filmed secretly on private premises. In its reasoning, the ECtHR observed that the Greek authorities had not considered that the first video was not recorded on private premises and, consequently, the interference with the official's privacy rights under art. 8 ECHR was, therefore, significantly less serious than the interference related to the other two videos where the Greek courts ruled in favour of the right to privacy of the politician, taking into account, in particular, the modalities exploited to obtain information together with the journalistic duties and obligations of the broadcaster.

Summary

1. Introduction. – 2. The facts. – 3. The ECtHR decision. – 4. Journalism and secret filming: not a first time for the ECtHR – 5. Is there a lesson learnt?

Keywords: Freedom of expression, Data protection, Right to private and family life, Right to inform, Journalism

1. Introduction

The case, here analysed, deals with the exercise of the right to inform by journalists and its relative limit in relation to the protection of privacy of the person filmed by hidden recording tools.

As a preliminary remark, since the case involves the conflict between two fundamental rights, it is necessary to contextualise the relationship between freedom of expression

and privacy in the European framework and, in particular, by looking at the degree of protection recognised to these fundamental rights. Indeed, both these rights, which strongly conflict to each other almost by nature, enjoys a degree of protection which is not absolute but relative[1] being subject to exceptions enshrined both in the European Convention of Human Rights[2] (hereinafter, "ECHR") and the Charter of Fundamental Rights of the European Union.[3] Moreover, as a general clause, it should be mentioned the prohibition of the abuse of a right meaning that, in the system of protection of fundamental rights, one right cannot prevail generally over the other ones, leading to their destruction.[4] Since a fundamental right cannot prevail generally over another one, the balancing activity is at the core of the entire system of protection of fundamental rights in Europe. For this reason, as it will appear clear in this case, the right to privacy and to inform need to be balanced and such activity is not prior established but is based on the assessment of each situation through a case-by-case analysis. However, in order to understand better the implications of such approach on judicial outcomes, it is necessary to look at interpretative criteria provided by the European Court of Human Rights (hereinafter, "ECtHR" or "Strasbourg Court") which can be considered as a guide when dealing with similar journalistic activities.

2. The facts

It is time to focus on the main facts of the case in question.[5] The relevant events occurred in January 2002, when the applicant company, the broadcaster of the Greek television channel Alpha, transmitted a TV show named "Jungle" (*Ζούγκλα*) in which

[1] See, in particular, O. Pollicino - M. Bassini, *Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis*, in A. Savin - J. Trzaskowski (eds.), *Research Handbook on EU Internet Law*, Cheltenam UK, 2014, 508 ss.; F. J. Borgesius - S, Kulk, *Privacy, freedom of expression, and the right to be forgotten in Europe,* Cambridge, 2018.

[2] According to art. 8, para. 2, ECHR: «There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others». According to art. 10, para. 2, ECHR: «The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary».

[3] According to art. 52, para. 1, of the Charter: «Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others».

[4] According to art. 17 ECHR: «Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention». A similar clause is enshrined in art. 54 of the Charter.

[5] See ECtHR, *Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece*, app. 72562/10 (2018).

three videos, realised by a hidden camera, showed a member of the Hellenic Parliament (and, in particular, the chairman of the inter-party committee on electronic gambling) while gambling in an arcade. In particular, the first video showed the Parliamentarian entering in the gambling arcade and playing on two machines. The other two videos showed two meetings between the parliamentary deputy and the associates of the television broadcaster during which the first video was shown to the politician.[6]
The broadcastings in questions did not go unnoticed. Indeed, in May 2002, after having held a hearing with the broadcaster, the National Radio and Television Council (*Εθνικό Συμβούλιο Ραδιοτηλεόρασης*) considered that the hidden camera report in question was not compliant with the Greek law and ordered the broadcaster to pay 200,000 euros, obliging also to transmit the content of such decision.[7] During the proceedings, the broadcaster acknowledged the use of the hidden camera. However, according to the applicant, the use of such technique was justified by the fact that the Parliamentarian was a public figure and that it could be no other ways to verify his gambling activity as nobody would have relied on such events without broadcasting the images in question. On the contrary, the members of National Radio and Television Council argued that, in the event that the use a hidden camera would be generally justified by referring to an overriding public interest, citizens would fear to be subject to extortion.
Against such decision, the broadcaster lodged an appeal with the Greek Supreme Administrative Court (*Συμβούλιο της Επικρατείας*) in order to obtain its annulment. The case, then, was referred to the Plenary of the Supreme Administrative Court considering, in particular, that the broadcaster complained the violation of his right to freedom of expression not only as enshrined in the Greek Constitution but also under art. 10 ECHR.
In 2010, the Plenary dismissed the application considering that the act of recording by secret means an image focused on a specific person constitutes a violation of the right to personal image, as protected by art. 9, para. 1, of the Greek Constitution and art. 8, para. 1, of the ECHR. As a result, the TV broadcasting of images gathered through secret means cannot be covered by the legitimate exercise of the right to inform, considering that the news has been obtained violating an individual fundamental right. Therefore, the application of annulment based on reasons of journalistic interest and public interest was dismissed.
Consequently, the broadcaster decided to lodge an application to the ECtHR complaining, *inter alia*, the violation of its right to freedom of expression.

3. The ECtHR Decision

Before to describe the decision of the ECtHR, it will be appropriate to preliminary summarise the arguments of the applicant and the Greek Government.

[6] Some days later, the videos were broadcasted again during the TV show named "Yellow Press" (*Κίτρινος Τύπος*) by the same broadcaster.

[7] See Greek National Radio and Television Council, decision 214/162/23.05.2002. The decision of this authority was then confirmed by the Minister of Press and Media with the decision 3156/E/11.02.2003.

As already expressed, on the one hand, the broadcaster claimed that the decision of the National Radio and Television Council consisting in the imposition of administrative sanctions had violated its right to freedom of expression, and, in particular, the right to impart information. In particular, according to the broadcaster, the transmission of the first video in question was justified by the fact the Parliamentary was a public figure and its participation in gambling activities was a matter of public interest, especially due to its role as chairman of the parliamentary committee on electronic gambling. The same considerations applied for the other two videos in which, according to the applicant, it was necessary to represent the behaviour of Parliamentarian consisting in the attempt to persuade the associates of the broadcaster to present the facts in another way.

On the other hand, the Governments supported the opposite position according to which there was a violation of the right to privacy of the Parliamentarian. Indeed, a restriction of the right to inform of the broadcaster did not occurr since the sanction imposed regarded the illicit reproduction of the videos and not the broadcasting of them. According to the Government, there was not a violation of the right to inform and, even in the case the Court recognised it, the interference would have been justified by the fact that the applicant reported the facts by illegitimate means (i.e. a hidden camera) without either the consent or the awareness of the person involved. The Governments clarified that the applicant was aware that by filming and broadcasting the videos in question had breached art. 370A, para. 2, of the Greek Criminal Code. In particular, the Government observed that the wide protection afforded to the press did not mean that journalists were not obliged to respect national legislation and the Code on Journalistic Ethics. Moreover, the videos did not meet a public interest since the modalities were aimed at increasing the level of the TV audience, an aim which cannot justify a restriction of the right to personal identity.

Once having briefly clarified the positions of the parties, it is time to look at the ECtHR decision. Unlike the position of the Governments regarding the lack of the interference with the right to inform, the Strasbourg Court considered, instead, that the interference with the broadcaster freedom of expression existed and, moreover, the Court considered the above-mentioned argument as groundless since neither the ECtHR nor the national courts, can impose to the media the techniques of reporting to adopt in a particular case.[8]

Then, the Strasbourg Court analysed whether the interference in question met the conditions to restrict freedom of expression according to art. 10, para. 2, ECHR. In particular, since the restriction was prescribed by the Greek law and there was a legitimate aim to «protect the reputation and rights of the other», the Court focused on

[8] See ECtHR, *Jersild v. Denmark*, app. 15890/89 (1994). According to para. 31: «[...] At the same time, the methods of objective and balanced reporting may vary considerably, depending among other things on the media in question. It is not for this Court, nor for the national courts for that matter, to substitute their own views for those of the press as to what technique of reporting should be adopted by journalists. In this context the Court recalls that Article 10 (art. 10) protects not only the substance of the ideas and information expressed, but also the form in which they are conveyed. [...]» See, also, *Stoll v. Switzerland*, app. 69698/01, para. 146 (2007).

the necessary character of restriction in a democratic society[9] following these criteria: the contribution of the report to a debate of public interest; the degree of notoriety of the person affected and the subject of the report; the prior conduct of the person concerned; the circumstances under which the video was taken; the content, form and consequences of the broadcast; the severity of the sanction.[10]

Firstly, the Court considered that the report was matter of public interest, in particular, because «the widespread use of gambling constituted a debate of considerable public interest» and «the report was not without political import» since the interest of the public is related also the fact the conduct of the deputy was particularly relevant due to its role of chairman of an inter-party committee on electronic gambling.[11]

Indeed, regarding the degree of notoriety of the person involved, the Court clarified that the «public was entitled to be informed about certain aspects of the private life of public figures»[12]. In the case in question, the ECtHR observed that the national courts have taken into consideration the role of the Parliamentarian as a public figure even not expressly mentioning it in their reasoning. Moreover, according to the ECtHR, the subject of the videos was not the gambling issue *per se* but the Parliamentarian activity. The report, actually, did not focus on gambling as a social issue but to the figure of the politician as a gambler.

While the Court did not add any other relevant element regarding the prior conduct of the person involved, concerning the circumstances in which the videos were obtained, the Strasbourg Court clarified preliminary that «notwithstanding the vital role played by the media in a democratic society, journalists cannot, in principle, be released from their duty to obey the ordinary criminal law on the basis that, as journalists, Article 10 affords them a cast-iron defence»[13]. Indeed, the use of a hidden camera is not generally prohibited but subject to specific conditions. By looking at the facts, since the first video was obtained in a public place, the expectation of the person involved impose a different assessment of the use of a hidden camera to record videos rather than in the case of the other two videos filmed in private premises.

Then, the ECtHR addressed the last two elements. Whilst, regarding content and the effects of the broadcasting the Court observed only that the main effect was the removal of the Parliamentary from the parliamentary group which he belonged to, the Strasbourg Court recognised that the sanction originally imposed by the Greek authorities was proportionate having considered, *inter alia*, its lenient amount and the impact of the TV as channel of communication in spreading the videos concerned.

Having said that, the ECtHR agreed with the Greek authorities in relation to the conflict between the right to impart information and the right to protect privacy. The

[9] See, recently, ECtHR, *Pentikäinen v. Finland*, app. 11882/10 (2015), paras. 87-91; *Bédat v. Switzerland*, app. 56925/08 (2016), paras. 48-54; *Couderc and Hachette Filipacchi Associés v. France*, app. 40454/07 (2015), paras. 82-93.

[10] See ECtHR, *Couderc,* cited above, para. 93; *Axel Springer AG v. Germany*, app. 39954/08 (2012), paras. 90-95; *Von Hannover v. Germany (no. 2)*, app. 40660/08 and 60641/08 (2012), paras. 109-113.

[11] See ECtHR, *Alpha Doryforiki*, cited above, para. 52.

[12] See ECtHR, *Karhuvaara and Iltalehti v. Finland*, app 53678/00 (2004).

[13] See ECtHR*, Stoll*, cited above, para. 102; *Bladet Tromsø and Stensaas v. Norway*, app. 21980/93 (1999), para. 65; *Monnat v. Switzerland*, app. 73604/01 (2006), para. 66.

sanction was applied based on the way the information was obtained and to the journalistic duties and obligations of the applicant company. According to the ECtHR, these elements are reasonable as far the second and third video are concerned. On the contrary, regarding the first video, the Court observed that the Greek authorities did not take into account the circumstances under which it was obtained. Despite the use of the hidden camera to obtain the video, the Court recognised relevance to the fact that it was not recorded in private premises and that the interference with its fundamental rights was less serious. Indeed, the Strasbourg Court stated that «the domestic authorities should have included in their assessment the fact that [the politician], by entering a gambling arcade, could legitimately have expected his conduct to have been closely monitored and even recorded on camera, especially in view of the fact that he was a public figure»[14].

For these reasons, only regarding the first video, the Court ruled that, in assessing the case in question, national authorities did not balance proportionally the measures with the result that they have restricted the broadcaster right to freedom of expression and its legitimate aim consisting in the right to impart information over a subject of public interest. While, concerning the second and third videos, the applicant's complaints were rejected.

4. Journalism and secret filming: not a first time for the ECtHR

Once having provided this general framework, it is possible to focus on some aspects of this decision. This case deals with a quite common practice in the field of investigative journalism.[15] Indeed, hiding either the identity of the journalist or the tools used to report are only two of the techniques through which reporters try to make available to the society situations of public interest. Here, the traditional question was related to the lawfulness of such activity, i.e. the limits of the right to inform.

The relevant events of the case in question were not new for the ECtHR. In *Haldimann*,[16] the Strasbourg Court found that, in the framework of a report about malpractices in insurance brokerage, the act of secretly filming a person (making him or her unrecognisable), which was not a public figure and in private premises, was a proportionate exercise of the right to inform. Indeed, according to the ECtHR, the interference in the private life of the broker had not been serious enough to override the public interest in receiving information on the alleged malpractice in the field of insurance brokerage. While, in *Alpha Doryforiki,* in relation to the second and third videos, the Court recognised that the filming of a video with the above-mentioned modalities but involving a public figure in a private premise was not covered by the right to inform.

[14] See ECtHR, *Alpha Doryforiki*, cited above, para. 78.

[15] See S. Peron, *Il giornalismo d'inchiesta*, in *Responsabilità Civile e Previdenza*, 11, 2010, 2262 ss. See, generally, C. L. LaMay, *Journalism and the debate over privacy*, New York, 2003.

[16] See ECtHR, *Haldimann v. Switzerland*, app. 21830/09 (2015). See F. Furlan, *Haldimann c. Svizzera: via libera a giornalismo investigativo e registrazioni nascoste*, in *Quaderni Costituzionali*, 2, 2015, 466 ss.

At first glance, although the two cases are very similar, however, the outcomes are opposite. This is an example of how the concrete application of the balancing between fundamental rights can lead to different judicial outcomes even in cases dealing with the same conflict of rights and similar facts. At this point, comparing the two above-mentioned decision will be an exercise which allows to better analyse this framework.[17]

In order to understand the reason of such differences, it is necessary to deeply focus on the relevant facts of the *Haldimann* case. The Strasbourg Court dealt with a case involving three Swiss journalists which agreed to organise and film by using two hidden cameras an interview between a fake customer and an insurance broker in order to highlight malpractices in the insurance brokerage and, then, broadcast the video on a weekly TV programme on consumer protection. At the end of the interview, one of the journalists introduced herself explaining what it was happening to the broker which refused to answer any other question. As programmed, some sequences of such interview were broadcasted, however, making the broker's voice and face unrecognisable.

Without analysing all the steps of the proceedings which have led to the decision of the Strasbourg Court in *Haldimann*, starting from such brief explanations of the relevant facts, it is possible to underline at least two elements in favour of the right to privacy of the broker.

Firstly, the person involved is not a politician but only an insurance broker which, consequently, cannot be considered a public figure as also specified by the Strasbourg Court.[18] As a result, the broker can rely on his right to privacy which would tolerate less interference than in cases which involve public figures.

Secondly, and maybe most importantly, the video was filmed not in a public place but in private premises. In this case, that reliance according to which an individual can expect to be filmed in a public place cannot be applied since the case is more similar to the second and third videos contested in *Alpha Doryforiki*. Both these circumstances constitute clues in order to consider the right to privacy as predominant over the right to inform in *Haldimann*.

One, instead, is the main argument in favour of the right to inform. The content of the video was not focused on the broker but on the specific problem of public interest (i.e. malpractices in the insurance brokerage). Indeed, unlike the *Alpha Doryforiki* case, the documentary had not aimed to directly criticised the broker but realised to denounce specific commercial practices. Furthermore, the image of the broker was modified in order not to allow its recognition. These circumstances, instead, support a more proportionate restriction of the right to privacy favouring the right to inform. However, regarding this last point, it is not clear the reasons according to which, in *Alpha Doryforiki,* the Court considered the second and third videos as affecting more

[17] A similar exercise can be done by looking at the following ECtHR's decisions. See ECtHR, *Delfi AS v. Estonia*, app. 64669/09 (2015); *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary,* app. 22947/13 (2016). See J.T. Papp, *Liability for Third-Party Comments before the European Court of Human Rights - Comparing the Estonian Delfi and the Hungarian Index-MTE Decisions Hungarian*, Hungarian Yearbook Of International Law And European Law, 2016.

[18] See ECtHR, *Haldimann,* cited above, para. 52.

the right to privacy of the Parlamentarian, instead of considering them part of the gambling issue. Indeed, the fact that a public figure, which was covering at that time the role of chairman of the inter-party committee on electronic gambling, behave in a non-transparent way (i.e. trying to renegotiate the facts regarding his gambling activities) would be a matter of public interest regarding which the public deserves to be informed. As already anticipated, the qualification of a person as a public figure increases the threshold of tolerance regarding the intrusion in his or her private life.
In other words, it seems that, by looking theses cases under this perspective, maybe the two decisions could be decided in opposite way, so that, in *Alpha Doryforiki*, having as example the *Haldimann* case, the Strasbourg Court could strike the balance in favour of the right to inform even for the second and third video considering, in particular, the role of the person involved in the public life. While, in Haldimann, the ECtHR could make prevail the right to privacy considering that the broker was not a public figure and the video was recorded in private premises.
At this point, it is necessary to raise questions about why the Court has reached to these conclusions. In order to explain such distinguishing, it is necessary to refer to a specific paragraph of the *Haldimann* decision. Indeed, the Strasbourg Court observed that «the applicants deserved the benefit of the doubt intended to comply with the ethical rules applicable to the present case regarding the method used to obtain information»[19]. This means that the respect of the ethics of journalism as defined by Swiss law, citing the example of their limited use of the hidden camera, was taken into account by the journalists. In particular, the Swiss journalist has protected the right to privacy of the broker making him unrecognisable. The safeguard of the right to inform as provided for by 10 ECHR to journalists in relation to reporting on issues of general interest is subject to the condition that they act in good faith and on an accurate factual basis providing "reliable and precise" information in accordance with the ethics of journalism. On the contrary, in *Alpha Doryforiki*, the journalists were aware of the fact that their conduct was illicit according to Greek criminal law and, for this reason, the lack of good faith can be considered the true reason which has led the Strasbourg Court to give a strong relevance to conducts of journalists as *discrimen* in such two decisions.
Consequently, the more relevant difference for the ECtHR between these two cases has been the respect of the rules provided by national laws regarding journalistic ethics. As a result, the rules provided for by the law and the code of conducts in the field of journalist activities should be considered as a fundamental element in order to assess whether the reporter have acted in good faith, even when an event of public interest or a public figure are involved.

5. Is there a lesson learnt?

The analysis of this decision, together with its precedent, seems to confirm the introductory remarks according to which the specific facts of each case can strongly influence the balancing of fundamental rights impacting on the final outcome. Indeed,

[19] *Ibidem*, para. 61.

as analysed, in two similar cases, the Strasbourg Court reached two opposite decisions. Focusing on the case in question, as appeared clear, the ECtHR recognises a broad margin of the right to inform by acknowledging that a person cannot expect the same level of privacy in a public place as in private premises. While, especially with regard to second and third videos, the Court clarified that, even when a public figure is involved, the right to inform finds, however, its limit in the respect of the right to privacy. This last consideration would be particularly important for reporters whose activities should, moreover, comply with their duties and responsibilities according to national rules as stated in *Haldimann*. For this reason, it would be necessary to read these cases together without considering the case in question a *revirement* of the Strasbourg Court. Maybe, such balance would be influenced in the next future by the implementation of art. 85 of the General Data Protection Regulation[20] which leaves to Member States a broad margin of discretion[21] in balancing privacy with freedom of expression in journalistic activities. In any case, due to the fragmentation of the code of conducts of journalists across the Contracting States, it is not possible to rely on a unique source of reference for journalistic activities.

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[21] According to art. 85, para. 1, of the Regulation: «Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression».

Cronache e commenti

Sull'eccesso di delega del decreto legislativo di adeguamento del Codice Privacy alla disciplina del Regolamento (UE) 679/2016

Giovanni De Gregorio

Sommario

1. Introduzione: tra principi e criteri direttivi. – 2. L'eccesso di delega: l'orientamento della Corte costituzionale. – 3. Il caso del recepimento della direttiva SMAV. – 4. Il caso dei coordinamenti e dei riordini di materie. – 5. Conclusione: rileggere i principi e i criteri direttivi alla luce della *ratio* della legge delega per il recepimento del Regolamento (UE) 679/2016.

Keywords: Codice privacy, Data protection, Dati personali, Eccesso di delega, GDPR

1. Introduzione: tra principi e criteri direttivi

Molte riflessioni sono state fatte riguardo lo schema di decreto legislativo elaborato dalla Presidenza del consiglio sulla base della proposta ricevuta dalla Commissione incaricata di adeguare la normativa italiana alle disposizioni del Regolamento (UE) 679/2016 (di seguito, "Regolamento Privacy")[1] come previsto dalla l. 163/2017 (di seguito, "Legge di Delegazione").

Fra le questioni maggiormente dibattute particolare attenzione è stata posta riguardo il potenziale eccesso di delega da parte del Governo nell'esercizio del potere delegato dal Parlamento.[2] In particolare, le questioni principali sollevate vertevano su una questione formale e una sostanziale. Da un lato, si è dibattuto sulla scelta riguardante

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[2] Sul tema della delega legislativa si vedano, in particolare, A.A. Cervati, *La Delega Legislativa*, Milano, 1972; M. Cartabia, *I decreti legislativi integrativi e correttivi: virtù di Governo e vizi di costituzionalità?*, in V. Cocozza - S. Staiano (a cura di), *I rapporti tra Parlamento e Governo attraverso le fonti del diritto. La prospettiva della giurisprudenza costituzionale*, Torino, 2001, 71; A. Ruggeri, *A proposito di deleghe, delegificazioni (ed altro) e dei possibili rimedi volti a porre ordine nel sistema delle fonti*, in P. Caretti - A. Ruggeri (a cura di), *Le deleghe legislative: riflessioni sulla recente esperienza normativa e giurisprudenziale*, Atti del convegno, Pisa, 11 giugno 2002, Milano, 2003, 1 ss. ; P. Ilari, *Brevi riflessioni in tema di delega legislativa: il superamento del modello costituzionale*, in *Studi Urbinati* 56(1), 2005, 75 ss.; AA. VV., *La delega legislativa*. Atti del convegno svoltosi a Roma, Palazzo della Consulta, 24 ottobre 2008, Milano 2009; F. Modugno, *La delega legislativa nell'esperienza delle due ultime legislature*, in federalismi.it, 19 ottobre 2015.

l'abrogazione dell'intero Codice Privacy, dall'altro, sull'eliminazione delle sanzioni penali, quest'ultima poi risolta con l'aggiunta delle fattispecie concernenti la cessione di rilevanti quantità di dati e l'acquisizione fraudolenta di dati.

Risolta la questione attinenti agli aspetti sanzionatori, la questione principale ruotava attorno al comprendere se il Governo avesse agito nei limiti della propria delega optando per l'abrogazione dell'intero d. lgs. 196/2003 (di seguito, "Codice Privacy") anziché per le singole disposizioni incompatibili con quest'ultimo. L'abrogazione *in toto* del Codice Privacy è stata una soluzione criticata da chi ha basato il proprio giudizio su un'interpretazione letterale della delega[3] trascurando la sua *ratio* ossia l'adeguamento della disciplina nazionale al Regolamento Privacy[4].

Il presente lavoro tuttavia non mira a ricostruire esaustivamente l'ambito di discrezionalità del Governo nell'esercizio del potere delegato ma si pone l'obbiettivo di riflettere su una fattispecie ancora oggi singolare avente ad oggetto un decreto legislativo che recepisce una misura europea direttamente applicabile quale un Regolamento UE. A differenza dal caso delle direttive europee, in questo caso il recepimento cerca di soddisfare due obbiettivi principali: da un lato, similmente a quanto accade nel caso delle Direttive, il recepimento mira a riempire quei margini di discrezionalità lasciati al legislatore nazionale, dall'altro, mira a riordinare la disciplina nazionale al fine di evitare incompatibilità con il Regolamento. Occorre sottolineare come quest'ultimo *step* non costituisca un passaggio obbligato visto che le disposizioni nazionali in contrasto con il Regolamento devono considerarsi come non applicabili in quanto il giudice nazionale è tenuto alla disapplicazione vista la prevalenza del diritto UE su quello nazionale. Tuttavia, il recepimento svolge una funzione orientata a garantire la certezza del diritto chiarendo quali disposizioni sono abrogate e quali devono intendersi compatibili con il quadro europeo di riferimento. Sotto quest'ultimo profilo occorre analizzare il caso di specie.

Non resta quindi che analizzare attraverso la lente del diritto costituzionale il grado di discrezionalità che il legislatore delegato può esercitare nei confronti delle linee di intervento legislative stabilite dal delegante sulla base dei cc.dd. principi e criteri direttivi,

[3] Secondo l'art. 13, c. 3, della Legge di Delegazione: «Nell'esercizio della delega di cui al comma 1 il Governo è tenuto a seguire, oltre ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti principi e criteri direttivi specifici: a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679; b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679; c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679; d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679; e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse».

[4] Secondo l'art. 13, c. 1, della Legge di Delegazione: «Il Governo è delegato ad adottare […] uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE».

riflettendo, quindi, sul caso di specie attinente all'adeguamento della disciplina italiana in materia di privacy alle disposizioni del Regolamento Privacy.

2. L'eccesso di delega: l'orientamento della Corte costituzionale

In tema di eccesso di delega, il testo costituzionale all'art. 76 non fornisce particolari criteri interpretativi se non riferendosi al fatto che l'esercizio della funzione legislativa non può essere delegato al Governo se non con determinazione di principi e criteri direttivi e soltanto per tempo limitato e per oggetti definiti. Tali criteri sono risultati nel corso del tempo tutt'altro che rigidi come suffragato da una vasta giurisprudenza della Consulta.

Secondo il costante orientamento della Corte costituzionale[5], il controllo di conformità della norma delegata alla norma delegante richiede un confronto tra gli esiti di due processi ermeneutici paralleli: l'uno, relativo alle norme che determinano l'oggetto, i principi e i criteri direttivi indicati dalla delega, da svolgere tenendo conto del complessivo contesto in cui esse si collocano ed individuando le ragioni e le finalità poste a fondamento della stessa; l'altro, relativo alle norme poste dal legislatore delegato, da interpretarsi nel significato compatibile con i principi e i criteri direttivi della delega[6].

Il contenuto della delega e dei relativi principi e criteri direttivi deve essere identificato, dunque, accertando il complessivo contesto normativo e le finalità che la ispirano, tenendo conto che i principi posti dal legislatore delegante costituiscono non solo la base e il limite delle norme delegate, ma strumenti per l'interpretazione della loro portata. Queste vanno, quindi, prese in considerazione, nel significato compatibile con detti principi, i quali, a loro volta, vanno interpretati avendo riguardo alla *ratio* della delega ed al complessivo quadro di riferimento in cui si inscrivono.

Al legislatore delegato spettano margini di discrezionalità nell'attuazione della delega, sempre che ne sia rispettata la *ratio* e che l'attività del delegato si inserisca in modo coerente nel complessivo quadro normativo di riferimento[7]. Occorre, infatti, tenere conto della possibilità, intrinseca allo stesso strumento della delega, soprattutto ove riguardi interi settori di disciplina o comunque organici complessi normativi, che il legislatore delegato introduca disposizioni che costituiscano un coerente sviluppo e un completamento delle indicazioni fornite dal legislatore delegante, nel quadro della fisiologica attività che lega i due livelli normativi[8].

A tal proposito, può inoltre richiamarsi l'orientamento della Corte, secondo cui l'art. 76 della Costituzione «non osta all'emanazione di norme che rappresentino un coerente sviluppo e, se del caso, anche un completamento delle scelte espresse dal legislatore delegante; va escluso, infatti, che le funzioni del legislatore delegato siano limitate ad una mera scansione linguistica delle previsioni dettate dal delegante, essendo consenti-

[5] C. Cost., 25 novembre 2016, n. 250.

[6] C. Cost., 29 ottobre 2015, n. 210.

[7] C. Cost., 23 marzo 2016, n. 59; 5 giugno 2015, n. 98.

[8] C. Cost., 9 luglio 2015, n. 146; 6 ottobre 2014, n. 229.

to al primo di valutare le situazioni giuridiche da regolamentare e di effettuare le conseguenti scelte, nella fisiologica attività di riempimento che lega i due livelli normativi, rispettivamente, della legge di delegazione e di quella delegata»[9].
Se per un verso, si deve escludere che l'art. 76 riduca la funzione del legislatore delegato ad una mera "scansione linguistica" delle previsioni stabilite dal legislatore delegante, per altro verso va ribadito che l'ambito della discrezionalità lasciata al delegato, muta a seconda della specificità dei criteri fissati nella legge delega[10]; tuttavia, è necessario considerare che, per quanta ampiezza debba riconoscersi al potere di completamento del legislatore delegato, il libero apprezzamento del medesimo non può uscire dai margini di una legislazione vincolata, quale è, per definizione, la legislazione su delega[11].
La Corte ha però precisato anche i limiti generali atti a contenere la discrezionalità del legislatore delegato. Da un lato, il libero apprezzamento del legislatore delegato «non può mai assurgere a principio od a criterio direttivo, in quanto agli antipodi di una legislazione vincolata, quale è, per definizione, la legislazione su delega»[12]; dall'altro, però, il delegante non può precludere «ogni margine di scelta nell'esercizio della delega»[13] in modo da permettere al potere delegato la possibilità di tenere in considerazioni il caso concreto da regolare.

3. Il caso del recepimento della Direttiva SMAV

Una volta definite le suddette linee guida generali, occorre soffermarsi su un caso che in passato ha fatto discutere in materia di eccesso di delega. Una simile questione era emersa riguardo il presunto eccesso di delega nell'adozione da parte del Governo del d.lgs. 44/2010 (di seguito, "Decreto Romani") rispetto a quanto previsto dalla direttiva 2007/65/CE[14] (di seguito, "Direttiva SMAV"), che aveva il compito di recepire e, più in generale, adeguare la normativa italiana con il quadro normativo e giurisprudenziale proprio dell'ordinamento dell'Unione europea. In particolare, l'art. 26 della l. 88/2009 attribuiva la delega al governo esclusivamente per recepire quanto previsto dalla Direttiva SMAV prevendo, inoltre, ulteriori criteri senza però prevedere una esplicita modifica generale delle norme del Testo unico dei servizi di media audiovisivi e radiofonici (di seguito, "TUSMAR").[15]
Secondo l'art. 26 della legge delega, oltre i criteri generali previsti di cui all'art. 2 della

[9] C. Cost., 5 giugno 2003, n. 199; 3 luglio 2002, n. 308.

[10] C. Cost., 6 dicembre 2012, n. 272; 11 aprile 2008, n. 98.

[11] C. Cost., 8 ottobre 2010, n. 293.

[12] C. Cost., 12 ottobre 2007, n. 340.

[13] C. Cost., 3 giugno 1998, n. 198; 5 aprile 2012, n. 80.

[14] Direttiva 2007/65/CE del Parlamento europeo e del Consiglio dell'11 dicembre 2007 che modifica la direttiva 89/552/CEE del Consiglio relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti l'esercizio delle attività televisive.

[15] Sul punto si vedano M. Cuniberti, *La tutela degli utenti*, in F. Bassan - E. Tosi (a cura di), *Diritto degli audiovisivi*, Milano, 2012, 305 ss.; O. Pollicino, *Il decreto Romani ed eccesso di delega ex articolo 76 della Costituzione*, in MediaLaws, 18 dicembre 2010.

stessa[16], il legislatore delegato doveva attenersi alle seguenti dettagliate condizioni: «a) l'inserimento di prodotti è ammesso nel rispetto di tutte le condizioni e i divieti previsti dall'articolo 3-octies, paragrafi 2, 3 e 4, della direttiva 89/552/CEE[17], come introdotto dalla citata direttiva 2007/65/CE; b) per le violazioni delle condizioni e dei divieti di cui alla lettera a) si applicano le sanzioni previste dall'articolo 51 del testo unico di cui al decreto legislativo 31 luglio 2005, n. 177, per la violazione delle disposizioni in materia di pubblicità, sponsorizzazione e televendite, fatto salvo il divieto di inserimento di prodotti nei programmi per bambini, per la cui violazione si applica la sanzione di cui all'articolo 35, comma 2, del medesimo decreto legislativo 31 luglio 2005, n. 177».
Il Decreto Romani sembrava oltrepassare tali limiti legiferando al di fuori di quanto oggetto di regolazione da parte della Direttiva SMAV in merito a due profili connessi, uno più generale, l'altro più specifico.[18] Da un punto di vista generale, l'ambito di applicazione della Direttiva SMAV non sembrava comprendere alcuna regolazione del *web* (eccetto per l'ipotesi molto specifica del *webcasting*). Come appare chiaro dal considerando 16, è escluso qualsiasi servizio trasmesso sul *web,* in particolare «i servizi con-

[16] Tra questi occorre, in particolare, segnalare l'art. 2, c. 1, lett. *b)* che recita: «b) ai fini di un migliore coordinamento con le discipline vigenti per i singoli settori interessati dalla normativa da attuare, sono introdotte le occorrenti modificazioni alle discipline stesse, fatti salvi i procedimenti oggetto di semplificazione amministrativa ovvero le materie oggetto di delegificazione».

[17] Direttiva 89/552/CEE del Parlamento europeo e del Consiglio del 3 ottobre 1989, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi).

[18] La restrittività della delega risulta chiara dalla relazione illustrativa del disegno di legge (n. 1078) la quale si riferiva in modo specifico ai criteri identificati: «La nuova direttiva definisce il concetto di "servizi di media audiovisivi compiendo una distinzione tra servizi lineari, che designano i servizi di televisione tradizionale, internet, la telefonia mobile che i telespettatori ricevono passivamente, e servizi non lineari, cioè i servizi di televisione a richiesta che i telespettatori scelgono di vedere (servizi di video *on demand*, ad esempio). In tema di pubblicità, in particolare, la direttiva definisce esplicitamente il concetto di «inserimento di prodotti» (*product placement*) e stabilisce il quadro giuridico in materia, fissando tra l'altro il principio del divieto di inserimento di tali prodotti, ma demandando agli Stati membri la decisione in merito alla eventuale deroga a tale principio. La disposizione dell'articolo 17 del disegno di legge è volta a definire l'ambito di esercizio della discrezionalità riservata allo Stato in materia di inserimento dei prodotti, attraverso lo strumento della novella al testo unico della radiotelevisione, di cui al decreto legislativo 31 luglio 2005, n. 177. L'opportunità del recepimento delle norme in tema di inserimento dei prodotti nel nostro Paese risiede nella necessità di garantire un trattamento omogeneo e non penalizzante alle opere audiovisive prodotte in Italia, aumentandone la competitività nel contesto europeo e introducendo, nel contempo, regole certe a tutela degli utenti. Un differente approccio, infatti, comporterebbe comunque la diffusione nel nostro Paese di opere audiovisive contenenti il product placement prodotte in Paesi dove la legislazione lo consente, con la conseguenza che eventuali effetti negativi sugli utenti non sarebbero neanche compensati da un beneficio in termini di opportunità di crescita del prodotto nazionale audiovisivo. Occorre, inoltre, considerare che le stringenti regole previste dalla direttiva per la diffusione del product placement, quali il divieto dell'inserimento di prodotti a base di tabacco, di sigarette, di prodotti medicinali o cure mediche, la sua esclusione nei programmi per bambini e soprattutto il principio di salvaguardia dell'integrità del programma e dello spettatore, ove integralmente recepite, rendono trasparente e regolamentata una pratica di fatto già utilizzata da molti Paesi europei. La direttiva, nel consentire l'inserimento del product placement, ha mutuato l'approccio già seguito in Francia, ovvero quello di una tolleranza di tale pratica nel rispetto di determinate condizioni più stringenti rispetto ai criteri di inserimento della pubblicità classica, proprio in considerazione dell'opportunità di una regolamentazione il più possibile omogenea del prodotto audiovisivo. In tema di sanzioni, infine, si dispone l'estensione alla disciplina de qua delle norme recate dal menzionato testo unico di cui al decreto legislativo n. 177 del 2005, ivi comprese le misure previste dall'articolo 35, comma 2, del testo unico per i casi di particolare gravità».

sistenti nella fornitura o distribuzione di contenuti audiovisivi generati da utenti privati a fini di condivisione o di scambio nell'ambito di comunità di interesse». Rispetto a tale indirizzo, il Decreto Romani dimostrava invece di occuparsi della prestazione di servizi audiovisivi in Internet contrariamente al suddetto ambito di applicazione della Direttiva SMAV.

Sotto un profilo più specifico relativo ai profili di violazione del diritto d'autore, l'unica disposizione rilevante della Direttiva SMAV concerneva la richiesta agli Stati membri di assicurare che i fornitori di servizi media soggetti alla loro giurisdizione non trasmettano opere cinematografiche al di fuori dei periodi concordati con i titolari dei diritti. La *ratio* di tale disposizione mirava a risolvere finalmente la questione delle cc.dd. "finestre di trasmissione".

Oltre tale cornice, l'art. 6 del Decreto Romani, invece, prevedeva l'aggiunta di un nuovo art. 32-*bis al* TUSMAR, rubricato "protezione del diritto d'autore". In particolare, il c. 2, lett. a) del suddetto articolo effettivamente recepiva quanto previsto dal nuovo art. 3-*quinques* della direttiva, mentre invece la lett. b) prevedeva un qualcosa del tutto nuovo e sconnesso dall'opera di recepimento della direttiva prevedendo che fornitori di servizi di media audiovisivi, operando nel rispetto dei diritti d'autore e dei diritti connessi, «si astengono dal trasmettere o ri-trasmettere, o mettere comunque a disposizione degli utenti, su qualsiasi piattaforma e qualunque sia la tipologia di servizio offerto, programmi oggetto di diritti di proprietà intellettuale di terzi, o parti di tali programmi, senza il consenso di titolari dei diritti, e salve le disposizioni in materia di brevi estratti di cronaca».

Come già sottolineato, in questo caso, la delega legislativa non sembrava ricomprendere tali interventi. Come risulta dalla relazione illustrativa dello schema di decreto legislativo, il Governo decise di introdurre le modifiche proposte al fine di tener conto della necessità di ridurre alcuni profili di ambiguità del testo originario che hanno formato oggetto di rilievi da parte della Commissione europea e disciplinare autonomamente aspetti non presi espressamente in considerazione dalle direttive comunitarie, ma non in contrasto con le finalità di tutela ad esse sottesi. Chiaramente senza tenere in considerazione i dettagliati criteri contenuti nella delega.

La questione non passò inosservata tanto che un importante *broadcaster* televisivo convinse il giudice *a quo*, nel corso di un processo avente ad oggetto l'applicazione di una disposizione del TUSMAR che era stata aggiunta a seguito del recepimento della Direttiva SMAV, di sollevare di fronte alla Consulta una questione di costituzionalità del Decreto Romani per un suo supposto eccesso di delega in relazione ad un diverso aspetto innovativo rispetto a quanto previsto dalla direttiva europea, vale a dire con riferimento alla questione della quantificazione dei cc.dd. affollamenti pubblicitari.

Nonostante le precise indicazioni fornite dalla legge delega, la Corte, investita della questione, rigettò la doglianza relativa al vizio di eccesso di delega rispetto all'oggetto e da violazione dei principi e criteri direttivi[19]. Principi che come lo stesso *broadcaster* aveva indicato come specifici rinvenendosi nella Direttiva SMAV, nonché nella stessa legge di delega, all'art. 2 e 26 (quest'ultimo recante criteri specifici relativi alla disciplina del c.d. *product placement*). Al contrario, secondo il *broadcaster*, la norma delegata

[19] C. Cost., 29 ottobre 2015, n. 210.

non era necessaria, da un lato, ai fini dell'attuazione della Direttiva SMAV, dall'altro eccedeva l'oggetto della delega. Secondo la Corte costituzionale, la modifica all'art. 38 del TUSMAR – nel modulare i limiti di affollamento pubblicitario in funzione delle oggettive diversità degli operatori – risultava coerente con la *ratio* della Direttiva SMAV (come espressamente individuata dalla Corte di giustizia)[20], in quanto volta a realizzare la equilibrata tutela degli interessi delle emittenti televisive, da un lato, e di quelli dei consumatori – telespettatori, dall'altro.

Il caso appena analizzato costituisce un tipico esempio di doppio parametro di costituzionalità (europeo e nazionale) dell'esercizio del potere delegato rispetto alle indicazioni del legislatore delegante. In questo caso, nonostante la specificità dei principi, il riconoscimento dell'ampio margine di discrezionalità del Governo nell'esercizio della delega da parte della Corte costituzionale suggerisce come nei casi di recepimento o adeguamento della normativa europea debbano tenersi in considerazione non solo il dettato della delega nazionale ma anche la *ratio* della misura europea. La suddetta decisione spinge a riflettere sull'ampiezza del potere discrezionale del legislatore delegato, in particolare, considerato che, anche in casi di così di dettaglio, la Consulta non ha riconosciuto un eccesso di delega nelle scelte del legislatore delegato ma, anzi, ha ritenuto che quest'ultimo avesse ampio margine di manovra nell'implementazione della Direttiva SMAV.

Tale approccio sembra confermare la necessità di adottare un approccio basato non tanto sul contesto letterale della delega fornita dal legislatore ma sulla *ratio* di quest'ultima.

Venendo al caso oggetto di analisi nel presente lavoro, le disposizioni della Legge di Delegazione sembrano maggiormente assimilarsi alla fattispecie dell'adeguamento e del coordinamento delle discipline piuttosto che al limitare l'introduzione di innovazioni da parte del legislatore delegato che vadano oltre l'oggetto della delega o la sua *ratio*.

4. Il caso dei coordinamenti e dei riordini di materie

A questo punto, al fine di inquadrare ancor più approfonditamente la questione, sembra opportuno richiamare brevemente la giurisprudenza della Consulta riguardante le leggi che delegano il Governo al coordinamento e al riordino di materie visto che, in particolare, la Legge di Delegazione fa espresso riferimento al concetto di "adeguamento" e "coordinamento".

Seppur nel caso di specie non si tratti di un intervento di riordino interno ma di adeguamento rispetto ad un Regolamento europeo, il fatto che il legislatore delegante non abbia introdotto dettagliate previsioni ma abbia delegato il Governo soltanto attraverso criteri volti all'adeguamento della precedente disciplina in materia di privacy, spinge a tenere in considerazione, per analogia, quei casi in cui il Governo è stato delegato in passato a coordinare normative già esistenti, seppur interne, piuttosto che ulteriormente soffermarsi sulla giurisprudenza in materia di recepimento di norme europee (di cui il caso del recepimento della Direttiva SMAV sopramenzionato ne costituisce

[20] CGUE, C-234/12, *Sky Italia* (2013).

un esempio).
In questo caso, inoltre, l'interesse per la materia del coordinamento rispetto al recepimento è dovuta ad ulteriori due motivi. Da un lato, considerato che le norme del Regolamento sono direttamente applicabili (salvo alcune eccezioni), l'operazione richiesta al legislatore delegato era maggiormente rivolta al coordinamento e non di certo al tradizionale recepimento delle norme europee. Dall'altro, la questione dell'eccesso di delega relativo ad eventuali previsioni del Regolamento europeo non è oggetto del dibattito che si focalizza soltanto sulla scelta relativa all'abrogazione dell'intero Codice Privacy. Infatti, ciò che interessa in quest'analisi non è giustificare l'attività innovativa del legislatore delegato rispetto alla delega o al Regolamento ma valutare la conformità dell'adeguamento e del coordinamento della disciplina rispetto alla *ratio* della Legge di Delegazione. Non si tratta quindi di valutare la conformità di scelte sostanziali legate al recepimento delle norme italiane al parametro europeo ma piuttosto di scelte formali legate alla scelta di abrogare il Codice Privacy, di fatto adeguando e coordinando l'intera materia. In altre parole, occorre scrutinare il grado di discrezionalità del legislatore delegato riguardo alle modalità con cui adeguare la materia.
In materia di delega per il coordinamento e riordino di discipline in essere, la Corte ha già affermato che tale attività può essere non solo formale se l'obiettivo è quello della coerenza logica e sistematica della normativa riordinata[21]. Inoltre, un criterio più generale sembra, inoltre, emergere dalla sentenza n. 308/2002 (richiamata anche da pronunce successive)[22]. In quella circostanza, la Corte ha affermato che il legislatore delegato ha il potere «di valutare le situazioni giuridiche da regolamentare e di effettuare le conseguenti scelte, nella fisiologica attività di "riempimento" che lega i due livelli normativi, rispettivamente, della legge di delegazione e di quella delegata».
Riguardo al significato del coordinamento, la Corte ha precisato che «[c]oordinare (non solo formalmente) vuol dire […] anche adeguare la disciplina al nuovo quadro complessivo, derivato dal sovrapporsi, nel tempo, di norme dettate in vista di situazioni e di assetti diversi, anche eliminando dai testi legislativi norme la cui ratio originaria non trova più rispondenza nell'ordinamento, e che quindi non appaiono più razionalmente riconducibili, quanto meno nella loro portata originaria, all'assetto in vigore»[23].
Da questi brevi passi qui richiamati si comprende come l'attività di coordinamento del potere delegato possa estendersi oltre la forma della delega al fine di poter soddisfare gli obbiettivi concreti della legge delega.
Tali brevi osservazioni sembrano confermare il necessario approccio sistematico ai principi e ai criteri direttivi che non possono essere presi in considerazione isolatamente e letteralmente ma devono essere collocati in una cornice di riferimento di carattere teleologico.

[21] C. Cost., 28 gennaio 2005 n. 52; 28 gennaio 2005, n. 53.

[22] C. Cost., 3 luglio 2002, n. 308.

[23] C. Cost. 24 giugno 2003, n. 220; 30 gennaio 2009, n. 21.

5. Conclusione: rileggere i principi e i criteri direttivi alla luce della *ratio* della legge delega per il recepimento del Regolamento (UE) 679/2016

Occorre chiedersi, quindi, se e in base a quali fattori possa identificarsi un eccesso di delega da parte del Governo nell'esercizio del proprio potere delegato al fine dell'adeguamento della disciplina italiana al Regolamento Privacy.
Occorre ribadire che, nel caso di specie, il fattore che ha fatto scaturire il dibattito sull'eccesso di delega non deriva dall'assenza di conformità della normativa di adeguamento rispetto ad una prescrizione europea come (non) avvenuto nel caso SMAV ma rispetto ad un aspetto formale, quasi letterale, contenuto nella Legge di Delegazione con la quale il Parlamento ha delegato il Governo per il recepimento – tra l'altro, non obbligatorio se non per alcuni aspetti – di una misura direttamente applicabile.
A questo punto, in merito ai principi e i criteri direttivi, occorre ricordare che, oltre le previsioni dell'art. 13 della Legge di Delegazione, le quali come ricordato mirano al coordinamento e all'adeguamento della disciplina italiana a quella europea, è necessario considerare anche i principi generali dettati dall'art. 31 della l. 234/2012 come richiamata dall'art. 2 della Legge di Delegazione. In particolare, l'art. 2, c. 1, lett. *b)* prevede che «ai fini di un migliore coordinamento con le discipline vigenti per i singoli settori interessati dalla normativa da attuare, sono introdotte le occorrenti modificazioni alle discipline stesse, anche attraverso il riassetto e la semplificazione normativi con l'indicazione esplicita delle norme abrogate, fatti salvi i procedimenti oggetto di semplificazione amministrativa ovvero le materie oggetto di delegificazione».
Tale previsione sembra confermare che la *ratio* della Legge di Delegazione, facendo riferimento alle "modificazioni occorrenti" al fine dell'attuazione della normativa europea, garantisse al legislatore delegato margine di manovra riguardo la singola scelta formale. Inoltre, come appare chiaro nel caso di specie, non si è in presenza di specifiche indicazione da parte del legislatore delegante che restringono la discrezionalità del legislatore delegato ma, al contrario, di ampi spazi di coordinamento entro i cui limiti va esercitata la funzione legislativa delegata.
Lo schema di decreto non prevede alcuna innovazione rispetto alla disciplina passata prevista dal Codice Privacy e non sembra porsi in contrasto con le indicazioni della Legge di Delegazione. Diverso sarebbe stato qualora il Governo avesse introdotto norme in contrasto con il Regolamento Privacy o avesse mantenuto disposizioni nazionali incompatibili con quest'ultimo.
Proprio, l'abrogazione del Codice Privacy, seppur da molti interpretata come un grave *vulnus* valoriale, non può costituire un limite ad un potere esercitato ai fini dell'adeguamento e del coordinamento e non dell'attività innovativa o additiva del legislatore delegato. Per tale motivo, le censure mosse riguardo l'eccesso di delega relativo all'abrogazione del Codice Privacy non trovano un riscontro concreto nella pratica né nella giurisprudenza costituzionale non essendosi verificata alcuna attività che abbia comportato un eccesso del potere delegato ma soltanto una sistematizzazione più efficiente della disciplina esistente, specialmente al fine di soddisfare l'interesse generale dell'ordinamento ad avere una normativa chiara per gli operatori e contenuta in unico

documento nonché a rispettare quel principio di leale collaborazione che lega l'Italia in qualità di Stato membro all'Unione europea.

Il referendum svizzero sul canone radiotelevisivo: una conferma della centralità del servizio pubblico

Giulio Enea Vigevani

Keywords: Svizzera, Servizio pubblico, Canone radiotelevisivo, Referendum, Media audiovisivi

Il 4 marzo 2018, i cittadini svizzeri hanno respinto con il 71,6% una richiesta referendaria che mirava all'abolizione del canone radiotelevisivo nazionale[1].
In particolare, il quesito referendario mirava a modificare l'art. 93 della Costituzione federale[2], introducendo i commi 3-6, secondo i quali:

> «3. La Confederazione mette periodicamente all'asta concessioni per la radio e la televisione.
> 4. La Confederazione non sovvenziona alcuna emittente radiofonica o televisiva. Può remunerare la diffusione di comunicazioni ufficiali urgenti.
> 5. La Confederazione o terzi da essa incaricati non possono riscuotere canoni.
> 6. In tempo di pace la Confederazione non gestisce emittenti radiofoniche e televisive proprie».

Si prevedeva altresì che, alla data dell'entrata in vigore delle nuove norme, le concessioni con partecipazione al canone sarebbero state revocate senza indennizzo.
Agli svizzeri, in sintesi, si offriva un'opzione netta: il passaggio a un sistema dei media audiovisivi interamente fondato sul principio di concorrenza, senza possibilità per la Confederazione di sovvenzionare o di gestire emittenti radiotelevisive, se non in ipotesi del tutto marginali. Un'alternativa radicale, che avrebbe inciso in maniera profonda

[1] Per un approfondimento, si rinvia al documento "Votazione popolare del 4 marzo 2018 Spiegazioni del Consiglio federale".

[2] L'attuale testo dell'art. 93 della Costituzione svizzera, rubricato "Radiotelevisione" prevede che:
«1. La legislazione sulla radiotelevisione nonché su altre forme di telediffusione pubblica di produzioni e informazioni compete alla Confederazione.
2. La radio e la televisione contribuiscono all'istruzione e allo sviluppo culturale, alla libera formazione delle opinioni e all'intrattenimento. Considerano le particolarità del Paese e i bisogni dei Cantoni. Presentano gli avvenimenti in modo corretto e riflettono adeguatamente la pluralità delle opinioni.
3. L'indipendenza della radio e della televisione nonché l'autonomia nella concezione dei programmi sono garantite.
4. Devono essere considerati la situazione e i compiti di altri mezzi di comunicazione sociale, soprattutto della stampa.
5. I ricorsi in materia di programmi possono essere deferiti a un'autorità indipendente di ricorso».

sul sistema mediatico e, di riflesso, sui processi di formazione dell'opinione pubblica in una democrazia caratterizzata dal pluralismo linguistico e dal ricorso sistematico a istituti di democrazia diretta.

Il risultato può sorprendere, anche per la onerosità dell'imposta su cui i cittadini elvetici erano chiamati a pronunciarsi; il canone in Svizzera ammonta a 451 franchi svizzeri annui, pari a circa 380 euro, anche se in prossimità della consultazione si è prevista per il 2019 una riduzione a 365 franchi.

Resta che i cittadini svizzeri, dopo un dibattito piuttosto approfondito e una notevole affluenza alle urne - ha votato circa il 54% degli aventi diritto - hanno a grande maggioranza ritenuto opportuno mantenere il ruolo primario della radiotelevisione pubblica nel sistema dei media audiovisivi.

Le ragioni di tale risultato vanno evidentemente ricercate nella radicalità del quesito – si tratta del primo caso in Europa in cui si chiede al corpo elettorale di decidere della permanenza stessa di una televisione pubblica nel sistema dei media – e nel peculiare contesto svizzero, ove le emittenti pubbliche hanno avuto un ruolo significativo nel preservare l'identità nazionale e il multilinguismo. Sarebbe, dunque, privo di senso trarre da tale consultazione referendaria valutazioni generali sullo stato di salute dei media pubblici in Europa; merita, comunque, di essere sottolineata la smentita di quella narrazione, diffusa in molti Paesi, secondo cui essi non sarebbero altro che "relitti del passato", sopravvissuti nell'era digitale soprattutto in ragione della volontà dell'*establishment* politico di non perdere il controllo di un formidabile strumento di formazione del consenso.

Come si è accennato, l'oggetto del referendum era chiaro: era in gioco la sopravvivenza del servizio pubblico radiotelevisivo, considerato *inter alia* tra i più autorevoli e apprezzati nel panorama europeo.

Esso è esercitato dagli anni '30 dalla Società svizzera di radiotelevisione (SSR), un'associazione di diritto privato senza scopo di lucro che dispone di sette reti televisive e di diciassette reti radiofoniche che coprono le quattro regioni linguistiche e culturali svizzere e che è finanziata per circa il 75% dal canone.

La SSR opera sulla base della legge federale sulla radiotelevisione del 24 marzo 2006 e della concessione del Consiglio federale. Essa è organizzata come *holding* nazionale, dotata di quattro società regionali che trasmettono nelle quattro lingue ufficiali della Confederazione. I principali organi sociali sono l'Assemblea dei delegati, composta da membri nominati dalle società regionali, e il Consiglio di amministrazione, ove siedono i presidenti delle società regionali, tre componenti designati dall'Assemblea stessa e due nominati dal Consiglio federale. La gestione aziendale è affidata al direttore generale, nominato dall'Assemblea dei delegati. Nel complesso, le norme costituzionali, la legislazione e il modello di *governance* adottato hanno garantito un alto grado di indipendenza dal potere politico e di autonomia gestionale, specie nella scelta della programmazione.

L'approvazione della richiesta referendaria avrebbe inciso in modo drastico anche sul sistema dei media locali: avrebbe ridotto sensibilmente le entrate delle radio locali e delle televisioni regionali che adempiono un mandato di servizio pubblico, finanziate anch'esse in larga parte con i proventi del canone, le quali provvedono a garantire a

tutte le regioni della Confederazione un'offerta equivalente, in particolare per quanto concerne l'informazione locale[3].

Nel complesso, era probabile che l'abolizione del canone avrebbe messo in crisi il sistema dell'audiovisivo in un paese di piccole dimensioni e con quattro lingue nazionali, ove gli aiuti di Stato sembrano indispensabili a garantire la presenza di media con una programmazione di alta qualità in ogni regione linguistica e, soprattutto, a promuovere la libera formazione delle opinioni e lo sviluppo culturale in modo indipendente da interessi economici, specie stranieri, in un contesto privo di un mercato pubblicitario interno abbastanza vasto.

In questo senso, gli oppositori alla riforma – e in particolare il Consiglio federale[4] – sottolineavano come il successo di tale iniziativa avrebbe indebolito drasticamente l'offerta delle emittenti con un mandato di servizio pubblico, non consentendo loro di adempiere la tradizionale funzione di coesione sociale e di scambio tra le regioni, le comunità linguistiche, le culture, le religioni e i gruppi sociali. Ed è probabile che, senza aiuti statali, si sarebbe drasticamente impoverito il panorama dei media nazionali e regionali e non vi sarebbe più stata una adeguata copertura nelle aree periferiche o in quelle delle lingue minoritarie.

Inoltre, si sottolineava da più parti come, in un'età nella quale la produzione audiovisiva – specie attraverso i nuovi media – spinge a una omologazione dei contenuti, il servizio pubblico potesse costituire un baluardo per la diffusione della cultura "popolare" nazionale, anche come finanziatore di film realizzati nel territorio svizzero.

Tra gli argomenti di discussione ve n'era uno strettamente connesso con il sistema costituzionale svizzero e in particolare con il largo utilizzo degli istituti di democrazia diretta.

Gli oppositori ritenevano che solo i media pubblici potessero garantire l'esistenza di un'informazione indipendente, pluralistica ed equivalente in tutte le regioni, essenziale per la formazione di una opinione pubblica consapevole, specie nei dibattiti che precedono le consultazioni referendarie.

Al contrario, dalle posizioni dei sostenitori del referendum e in particolare dell'Unione Democratica di Centro, il partito della destra "populista" elvetica, emergeva una generale diffidenza per il giornalismo professionale, finanziato direttamente o indirettamente dallo Stato, e la rivendicazione di un rapporto senza filtri con l'opinione pubblica[5].

In questo senso, l'esito elettorale può essere letto come la conferma in capo alla SSR di quel compito di collante della società, per gli svizzeri evidentemente ancora essenziale per mantenere un sistema fondato sulla democrazia diretta nell'era digitale[6].

Il risultato della consultazione può essere altresì considerato una risposta del corpo elettorale svizzero in controtendenza rispetto a un discorso pubblico che vede con sempre più sospetto l'intermediazione di soggetti professionali nel mercato delle idee

[3] Dagli anni '90, una parte dei proventi del canone è distribuita anche a emittenti private con una concessione di servizio pubblico. Attualmente ne beneficiano 13 televisioni regionali e 21 radio locali.

[4] Si v. la sintesi della posizione adottata dalla maggioranza del Consiglio federale, disponibile online.

[5] Ciò è criticamente evidenziato da P. Ruetschi, *Se la Svizzera dice addio alla TV pubblica*, in *La Repubblica*, 19 febbraio 2018, 25.

[6] K. Frick-J. Samochowiec-D. Gürtler, *Public 4.0, L'avenir de la SSR à l'ère numérique*, Zurigo, 2016, 53 ss.

e che invece tende a esaltare il legame diretto tra leader e massa, che si sviluppa principalmente attraverso la rete e, in particolare, i *social media*.

Proprio in questa prospettiva, si può forse trarre dalla vicenda svizzera qualche considerazione più generale sullo stato di salute del modello "duale" pubblico/privato che caratterizza la gran parte degli ordinamenti europei e sulla perdurante esigenza di un servizio pubblico nel mondo dei media audiovisivi.

Il fatto stesso che si sia promosso il referendum mostra come la presenza di un soggetto pubblico finanziato dallo Stato non sia più un postulato; condizioni per la sua legittimazione sono la fiducia dei cittadini e l'individuazione di una giustificazione per la sua peculiare posizione nel sistema dei media audiovisivi e per la sua sottrazione alle regole generali dell'attività di impresa e della concorrenza.

D'altra parte, l'esito così netto a favore del mantenimento del servizio pubblico induce, anche fuori dai confini della Confederazione, a dubitare dell'opportunità di procedere a una sua frettolosa e disinvolta liquidazione e semmai a riflettere sul fondamento costituzionale del servizio pubblico, in un panorama mediatico profondamente trasformato dallo sviluppo delle tecnologie digitali e delle piattaforme proprietarie a pagamento. E il caso svizzero mostra come tale fondamento sia da rinvenire *in primis* in una concezione della radiotelevisione pubblica quale *agorà* aperta – luogo ove rappresentare l'identità e il pluralismo culturale di una nazione – e quale "ponte", luogo di confronto tra le differenti e sempre più polarizzate opzioni ideologiche presenti nelle società. In questa prospettiva, che ha come precondizione l'esistenza di media pubblici autonomi rispetto al potere politico ed economico, il servizio pubblico potrebbe assumere quel ruolo "istituzionale" di garanzia della democrazia dialogica, auspicato ancora di recente da organismi sovrannazionali[7].

[7] Si veda a ultimo la Raccomandazione CM/Rec(2018)1 del Comitato dei ministri del Consiglio d'Europa agli Stati membri del 7 marzo 2018 sul pluralismo e la trasparenza della proprietà dei media, ove si coglie una forte preoccupazione sugli effetti della c.d. "*filter bubble*" che discenderebbe dalle dinamiche dell'informazione in rete e, in questa prospettiva, si attribuisce allo Stato il compito di garantire «*the crucial role of independent public service media organisations in fostering public debate, political pluralism and awareness of diverse opinions. States should accordingly guarantee adequate conditions for public service media to continue to play this role in the multimedia landscape, including by providing them with appropriate support for innovation and the development of digital strategies and new services*» (punto 2.9 delle linee guida).

"Street heart": urban murals as common goods

Giovanni Maria Riccio, Federica Pezza

Summary

1. Street art: sketching out a definition. – 2. The relationship between street art and Copyright law. -3.Criminal offences or protectable works?.- 4. A constitutional approach. Street art as common goods. - 5. Our proposal: how would it work?- 6. Conclusions and further considerations.

Keywords: Street art, Intellectual property, Copyright, Common goods, Protectable works

1. Street Art: sketching out a definition

Perfection of the lines, softness of the colours, harmony of the shapes. You are passionate for art, you are in Italy and this is precisely what you are looking for. Anyway, that's not all about Raphael and Michelangelo. And it's not all about museums. Life goes on and so art does. And that's why in this very moment we are facing the new phenomenon of street art. The first issue when it comes to street art is giving a definition. This is due to its non-established[1] character, the phenomenon embraces a series of various artistic techniques. In general terms, the expression is used to refer to those artworks which are realised in urban contexts, open to the access of the general public and, normally, without authorisation. Born in the 70's in New York City, at its very beginning, street art only consisted in simple signatures and words (what is now called "graffiti"). This was a way for Big Apple's cool kids (and a certain "Taki"[2] was the coolest apparently) to identify themselves and being somehow recognisable in that chaotic city. During the time, the phenomenon spread to Europe, further developing and focusing on images rather than words. For this purpose, street artists employed a number of techniques, including spray cans, brushes and palettes.

Eventually, a further note on the development of street art in Italy will be necessary. Interestingly enough, in fact, also our traditional country has a role to play in this game. And this role would be massive, according to someone. Precisely, the "Italian Taki" was a guy, called Fernando de Filippi, who, in the same period, started attaching his politically engaged posters on the walls of Milan and other Italian and European

[1] F. Haskell, *Le metamorfosi del gusto: studi su arte e pubblico nel XVIII e XIX secolo*, Torino, 1989; G. Dorfles, *Le oscillazioni del gusto. L'arte d'oggi tra tecnocrazia e consumismo*, Torino, 1970.

[2] For more information see https://en.wikipedia.org/wiki/TAKI_183 .

metropolis[3]. Keith Haring, first, then the new generation of street artists have worked intensively in Italy. « Contradiction is everywhere», said De Filippi in his posters. As the contradictions, also his art quickly developed and spread to other and different cities, first in Italy and then in Europe.
Don't be surprised Raphael lover. As the same artist used to write «Contradictions are everywhere».

2. The relationship between street art and Copyright law

The main issue when it comes to street art[4] is assessing whether or not it would be protectable under Copyright law[5]. In fact, the ephemeral nature of the work and the originality threshold imposed might both represent an obstacle.
In Italy, the relevant provisions to be considered are included in the Law 22 April 1941 no. 633 (Italian Copyright law, hereinafter ICL). Following Art. 1 of the mentioned law, protection is granted to all the creative intellectual works. Also, it is given «no matter the way and the type of expression»[6]. Eventually, article 2 no. 4 ICL includes artistic creations in its non-exhaustive list of copyrightable works.
Therefore, in Italy, differently from other countries, there is no codified fixation requirement. This means that a non-durable work of art is likely to be protected in our legal system.
Plus, even considering the requirement as existent, no issues would arise for street art given that one thing is the need for a tangible embodiment of the work and another, very different, is its non-alterable nature. As the Court pointed out in Creative Records[7], «while some works are intrinsically impermanent, others have only an ephemeral nature» and protection can be denied only in the first of these cases.
In the same way, moving to the originality standard, no problems arise. The notion of creativity, in fact, has always been interpreted extensively by the Italian doctrine and jurisprudence, observing that the presence of a «creative act»[8], even a minimum one,

[3] See A. Riva *La Street Art? L'ha inventata Ferdinando de Filippi. Quarant'anni fa*, 2015.

[4] See C.Y.N. Smith, *Community Rights to Public Art*, in 90 *St. John's Law Review*, 2016, 369-371: «For the purpose of this Article, an appropriate definition of "public art" is art in any media intended and displayed in the public domain, usually outside or in public buildings and accessible to all persons. "Community" is defined as 'the people with common interests living in a particular area»; see also P.N. Salib, *The Law of Banksy: Who Owns Street Art?,* in 82 *U. of Chi. L. Rev.* 2015; 2298; E. Bonadio *Copyright protection of street art and graffiti under UK law*, in *Intellectual Property Quarterly*, 2017.

[5] No matters arise for protectability *latu sensu*, given that our system is an open list one. In this sense, see for instance Italian Supreme Court, July 19, 1990, no. 7397, and Court of Catania, October 1, 2007, in *AIDA*, 2008, 738 (where protection was given to geographical charts).

[6] See Art. 1, Italian Copyright Law.

[7] See C. Cosentino *La tutela delle opere di Street art tra diritto d'autore e regole proproetarie,* to be published in *Rivista Critica del Diritto Privato*, 2017.

[8] See Court of Torino, May 25, 2009, in *AIDA,* 2010, 639; Z. Algardi, *Considerazioni sul plagio dell'opera scientifica*, in *AIDA*, 1972, 460, and Court of Torino, May 27, 2011.

would be enough for protection to be granted[9]. Even tags[10], consisting in mere words, could be protectable[11] due to their peculiar lettering style[12].

3. Criminal offences or protectable works?

The main issue with this kind of art, which is also its key feature, is the fact it is normally non-authorised.
This is precisely where our fairy tail finishes and the list of criminal offences starts.
In Italy the relevant provisions to look at are article 639 Criminal Code titled "Defacement or foul of someone else goods"(*Deturpamento ed imbrattamento di cose altrui*) and article 635 Criminal Code on "Damaging" (*Danneggiamento*). Both the articles are likely to be applied to street art. And in fact, recently, the Tribunal of Bologna, condemned the street artist "AliCè"[13] for the infringement of art 639 Criminal Code, given that «neither the condition of the walls nor the international reputation of the artist were likely to limit the liability» [14].
The question, in this sense, is whether or not a behaviour constituting a criminal offence can also originate a somehow protectable work[15]. And the answer, given by Italian Copyright law, is a positive one, given that our system is neutral and the lawfulness of the work is not regarded as a condition for the grant of protection[16].
However, as we will see, although not affecting its protectability, the circumstance street art attaches to someone else walls might pose other questions to the interpreter (below).

4. A constitutional approach. Street art as common goods

In particular, one has to strike a balance between the right of the artist on his creation

[9] Furthermore, the same idea might be at the basis of different expressions and all of these shall be deemed as protectable. See Italian Supreme Court, November 28, 2011, no. 25173, in *Foro it.*, 2012, I, 74 and Court of Bologna, May 9, 2007, in *AIDA*, 2010, 639.

[10] For a definition see UrbanDictionary.com.

[11] This is possible considering them as artistic works rather than literary works. See J. Hughes, *Size Matters (or Should) in CopyrightLaw,* in 74 *Forham L. Rev.*, 2005, 575.

[12] See C. Lerman, *Protecting Artistic Vandalism: Graffiti and Copyright Law*, in 2 *NYU J. Intell. Prop. & Ent. L.*, 2012, 295. A similar conclusion can be reached on the basis fonts are protectable .

[13] Court of Bologna, February 15, 2016, no. 674 (*Alicè* case), unpublished.

[14] A different outcome was reached in Cass. Pen., April 5, 2016 no. 16371 ("*Manu Invisibile*" case). In this context in fact the Court dismissed the claim against the artist basing on those same two elements not considered as relevant in the *Alicè* case.

[15] This is not possible in the UK and the US, because of the "clean hands doctrine". See *Primeau v. Granfteld*, 193 F. 911, 912 (2d Cir. 1911) and A.P. Herbert, *Uncommon Law*, Methuen, 1935.

[16] P. Greco – P. Vercellone, *I diritti sulle opere dell'ingegno*, in *Tratt. dir. civ.* di Vassalli, Torino, 1974, 52 ss.; App. Roma October 10, 1957, *AIDA,* 1958, 590 ss.; Pret. Bologna, April 20, 1971, in *Giust. civ.,* 1971, 694 ss.

and the property right of the owner of the building. Our thesis moves from this premise and criticises the approach generally taken by the doctrine. This results, in fact, in the erroneous conviction that the ownership of the artworks is for the owner of the embodiment, who will be able to dispose of and even destruct the artistic creation[17].
However this approach does not persuade. In fact, not only it doesn't take into account the right of integrity of the artist but, mainly, it does not consider that this kind of artworks is, in most of the cases, removable[18]. With the result that, in this scenario, the relationship between the owner of the wall and the artwork will not be comparable to the one existing between the painting and its canvas but, rather, between the painting and the wall it attaches to. Therefore, unless a sell and purchase agreement took place, the owner of the wall does not seem to have any right over the artwork.
However, in our view, this approach is not methodologically correct, as it does not provide a real answer to the issue of the property of the works and does not take into account the peculiarities of non authorized urban art.
On the contrary[19], by taking the distance from the typical private/ public property dichotomy, the works of street art should be considered as "*common goods*"*;* in other words, according to the definition given by the Rodotà Commission, those goods constituting «the expressions of utilities functional to the exercise of fundamental rights and the free development of the person» *(«cose che esprimono utilità funzionali all'esercizio dei diritti fondamentali nonché al libero sviluppo della persona»)*[20].
A similar theory, based on a Constitutional notion of property, finds its reason in the social and cultural role played by art for the society[21]. This cultural value, we argue, is particularly high in the case of street art, which, by its own nature, is intrinsically related to the context it is conceived in.
Specifically, there would be a twofold relationship between the artwork and the community, with each of the actors reciprocally influencing the other.
On one side, as the artist Stilk notices, «street art reacts to the context»[22]. Let's take for example the famous San Gennaro of Naples, reproducing an religious icon of the city, or also, in the same area, that artwork from Banksy representing a saint with a gun, expression of the artist attempt to summarise the contradictions of the city. Indeed, they both belong to the community they live in.

---

17 In this sense C. Agostini, *Street Art e diritto: il caso di Yulier P. e la normativa italiana*, 29 September 2017, in www.replegal.it.

18 In Italy these interventions, due to the damages they might cause, have to be previously authorised; cfr. art. 50 del Codice dei beni culturali: «*È vietato, senza l'autorizzazione del soprintendente, disporre ed eseguire il distacco di affreschi, stemmi, graffiti, lapidi, iscrizioni, tabernacoli ed altri elementi decorativi di edifici, esposti o non alla pubblica vista*».

19 G.M. Riccio, *Una modesta proposta per la street art*, in *Il Lavoro culturale*, 1 June 2017.

20 S. Rodotà, *Il terribile diritto. Studi sulla proprietà privata e i beni comuni*, Bologna, 2013, 465 ss.; M.R. Marella, *Il diritto dei beni comuni. Un invito alla discussione*, in *Riv. crit. dir. priv.*, 2011, 103 ss.; *Commissione Rodotà - per la modifica delle norme del codice civile in materia di beni pubblici* ,14 June 2007 - *Proposta di articolato*, Ministero della Giustizia.

21 J. Sax, *Playing Darts with a Rembrandt: Public and Private Rights in Cultural Treasures,* Ann Arbor, 1999, 6.; A.M. Honoré, *Ownership* in A.G. Guest (ed.), in *Oxford Essays in Jurisprudence*, London - New York,1961; R. Pound, *The Law of Property and Recent Juristic Thought* in 25 *American Bar Association Journal*, 1939, 997.

22 D. Lynskey, *Street artist Stilk: 'I felt invisible and it was my way to showing out I'm here'*, in *The Guardian*, 2015.

Also, often, street artists deliberately employ elements of the building as a part of their creation. In this sense, the context materially contributes to the final work, with the result that a simple window might become the opened mouth of a terrible monster[23], an apse a truly original kite and even a pre-existent artwork can be the basis for a new one[24].

On the other side, street art does influence – incredibly – the community it attaches to, often constituting a means for improving a depressed area. In Italy, a good example is provided by an interesting project, "Big City Life", recently developed in the area of Tor Marancia[25] in Rome and involving the participation of 20 international artists with the purpose of decorating – and bringing to life – the buildings of this suburban area. Interestingly, sometimes it is the same community, and not the local authorities, to independently promote and finance similar initiatives.

5. Our proposal: how would it work?

Recognising the common good nature of street art is the first step for shaping an adequate legal solution. In fact, the consequence of this approach is the need for the adoption of a different notion of ownership, to be conceived in terms of stewardship rather than property[26].

This is particularly interesting in the case of removal of the work from his original physical support. Who is entitled to remove the work? Is there any notification obligation over the owner of the physical support, as in the US VARA regulation or not?

In our opinion, this choice might be granted to a public administrative authority, which could be entitled to take any decisions regarding the artistic value of the work, the possibility to remove or to destroy the work itself or even to dislocate into another place, in order to ensure the preservation of the work, where its artistic and cultural values are recognized.

In Italy, this administrative role would be played by the "Superintendence of Cultural Heritage" (*Soprintendenza per i beni culturali*), assisted, for this purpose, from a commission of experts and entitled to any relevant decisions. In particular, in the case a conflict between the artist and the owner of the building arises, the latter shall communicate to the Authority his intention of destroying the work[27]. Then, together with the Commission, the Superintendence, within (for example and as a proposal) 30 days maximum, will decide whether to authorise the destruction of the work or financing its removal, in order to promote its safeguard.

[23] See the artworks by Blu.

[24] See "San Gennaro" by Jorit and "Saint with a Gun" by Bansky.

[25] Find more details at the following link http://www.bigcitylife.it

[26] T. Cheng–Davies, *A work of art is not just a barrel of pork: the relationship between private property rights, moral rights doctrine and the preservation of cultural heritage,* in *Intellectual Property Quarterly*, 2016.

[27] This communication might be given by any means, even a simple e-mail. As reported also in the text below, the choice of not notifying to a public authority, instead of to the artist, could have the advantage of not forcing the artist, who often works under anonymity, to reveal his identity, exposing himself to the risk of penalties.

6. Conclusions and further considerations

The proposed solution would be beneficial for all of the involved parties. First of all, when compared to the model provided under the VARA[28] in the US, this system is particularly beneficial to the owner of the building. In fact, he would not be imposed anymore transactional costs related to the excessive burden of sending a notification to the artist, being sufficient the communication to the local Authority of his intention to destruct or remove the artwork.

In the same way, the artist, often operating anonymously or under pseudonymous, would be given the opportunity of protecting his right without having to disclose his identity. The main benefit would obviously be for the community. In fact, the connection existing between street art and its context makes the adoption of a civil code based approach, according the full ownership of the artwork to the owner of the building, particularly risky for its cultural value.

Similarly, leaving the protection of the work to the intention of the artist, by the instrument of moral rights, might not be sufficient for its safeguard. In fact, apart from enjoying a weaker position, the same artists might not be interested in protecting their work[29], preferring to accept the risks connected with its ephemeral nature. Differently, the solution of attributing to a specific Authority the decisions over street art is more likely to effectively guarantee the collective access to these works and to preserve the cultural heritage of the State. Moreover, a centralised decision-making system in this context, if adequately supported, would have the benefit of ensuring quicker, objective and impartial decisions, contributing in the same time to the development of good practices in the field.

In conclusion, all the players may have an advantage by this solution (artists, owners of the building, citizens, the State).

More issues, however, are yet to be solved. And in fact, an adequate administrative body has to be established or, where already existing, supported by a Commission of experts. Also, a good balance between the safeguard of the artistic work and the artist integrity right has to be found. In particular, one question in this sense will be determining those cases, if any, where the photographic reproduction of the work can be considered sufficient for its preservation.

This is just a proposal, not necessarily a solution and a starting point of discussion, not only in Italy.

---

[28] For a criticism of the provisions D. Burton, *Artists' Moral Rights: Controversy and the Visual Artists Rights Act,* 48 *S.M.U. L. Rev,* 1995, 639-642; D.S. Ciolino, *Moral Rights and Real Obligations: A Property-Law Framework for the Protection of Authors' Moral Rights,* in 69 *Tul. L. Rev.,* 1995, 935-938. See also J. Lipton, *Moral Rights and Supernatural Fiction: Authorial Dignity and the New Moral Rights Agenda*, in 21 *Fordham IP, Media & Ent. L. J.,* 2011, 537-539 and E. Damich, *The Visual Artists Rights Act of 1990: Toward a Federal System of Moral Rights Protection for Visual Art,* in 39 *Cath. U. L. Rev.*, 1990, 945-946 .

[29] This was what recently happened in Bologna, where the artist Blu opposed the relocation of its artworks in a museum, for the exhibition organised by the association Genus Bononiae. Consequently, the artist preferred to destroy its own artworks rather than closing them in a museum. See M. Smargiassi, *Bologna, Blu cancella tutti i suoi murales: "No alla street art privatizzata"*, in *La Repubblica*, 3 December 2016.

Fake news e libertà di informazione

Filippo Donati

Sommario

1. Premessa. – 2. Il quadro normativo attuale. – 3. Libertà di informazione e *fake news*. – 4. Conclusioni.

Tag: *Fake news,* Libertà di informazione, Internet Service Provider, DDL Gambaro, Disinformazione

1. Premessa

Come ha da tempo chiarito Paolo Barile, la mera diffusione di notizie false non può essere considerata in sé e per sé illecita, a meno che non leda diritti o valori costituzionalmente rilevanti[1]. In questa prospettiva si è saldamente collocata la giurisprudenza costituzionale, secondo cui la libertà di informazione riconosciuta dall'art. 21 Cost. può essere limitata soltanto per la tutela di altri valori di rilevanza costituzionale che possano entrare in conflitto con essa, quali sono i valori attinenti all'onore, alla reputazione ed alla riservatezza della persona; all'ordine pubblico; alla sicurezza dello Stato; al regolare svolgimento della giustizia; alla tutela di alcune forme di segreto[2].

La diffusione di internet sembra tuttavia aver mutato il quadro di riferimento. Nessuno dubita che internet abbia contribuito a rafforzare le possibilità di esercizio della libertà di informazione, sia sotto il profilo "attivo" del "diritto di informare" (perché oggi ciascuno può trasmettere idee e notizie in tempo reale in ogni parte del mondo e senza costi), sia sotto il profilo "passivo" del "diritto all'informazione" (perché oggi la rete mette a disposizione dei cittadini una quantità di fonti informative fino a pochi anni fa neppure immaginabile). Tuttavia le nuove potenzialità trasmissive offerte da internet favoriscono anche la possibilità di diffondere su larga scala notizie sbagliate, distorte o manipolate, che pure vengono presentate come vere (le cosiddette "*fake news*"). La più recente tecnologia permette inoltre l'utilizzo di robot che creano artificialmente falsi profili e falsi contenuti, che gli utenti generalmente scambiano per veri. L'anonimato garantito alle comunicazioni in rete, inoltre, rende generalmente difficile, se non impossibile, identificare l'autore delle *fake news*. Tutto questo genera una crescente disinformazione che può condizionare i comportamenti politici, sociali e le scelte economiche di ampi strati della popolazione.

Non meraviglia dunque che il tema delle *fake news*, cioè della possibilità di limitare la

[1] P. Barile, *Diritti dell'uomo e libertà fondamentali,* Bologna, 1984, 229.

[2] Cfr. per tutte C. Cost. 11/1968 e 98/1968.

diffusione in rete di notizie oggettivamente false oppure rappresentate in maniera distorta e fuorviante, sia da qualche tempo oggetto di accese discussioni in Italia e all'estero. Sotto questo profilo, emblematiche sono le polemiche correlate alla campagna politica di Trump, che secondo molti commentari avrebbe beneficiato degli effetti di una strategia di informazione che ha fatto largo uso di notizie o false, o rappresentate in maniera distorta o comunque non verificabili. In effetti si è progressivamente rafforzata la consapevolezza che, grazie alla diffusione di *fake news* mediante un sapiente utilizzo di Internet e delle più moderne tecnologie informatiche, il dibattito politico può essere facilmente condizionato a favore di un candidato o a danno di un altro. Assai recenti sono inoltre le polemiche sulla vaccinazione obbligatoria che, pur essendo indispensabile per garantire la salute dei cittadini, ha incontrato inaspettate resistenze in una considerevole fascia della popolazione a seguito della diffusione sulla rete di notizie circa la presunta pericolosità dei vaccini, che secondo l'amministrazione della sanità sono del tutto prive di fondamento scientifico.
Nell'ambito di un dibattito sempre più acceso sugli effetti distorsivi che la diffusione di *fake news* può avere sulla formazione dell'opinione e quindi, in ultima analisi, sulle scelte dei cittadini e sul funzionamento della democrazia, si sono moltiplicati gli appelli all'introduzione di forme di controllo volte a prevenire o comunque a sanzionare la diffusione in rete delle notizie false. In Germania è attualmente all'esame del Bundestag una proposta di legge che punisce severamente i fornitori di accesso a internet che non provvedono entro 24 ore alla rimozione di notizie segnalate come false[3]. In Italia è stata recentemente presentata una proposta di legge per sanzionare la diffusione in rete fake news[4].
Per valutare proposte del genere è opportuno partire da un breve richiamo al quadro normativo di riferimento.

2. Il quadro normativo attuale

Nel nostro ordinamento, la diffusione di notizie false, esagerate o tendenziose non è vietata di per sé, ma solo quando essa comporti un turbamento dell'ordine pubblico (art. 656 c.p.). La Corte costituzionale ha ritenuto che una previsione del genere non determina un'illegittima restrizione alla libertà di diffondere idee e informazioni, in quanto «la tutela costituzionale dei diritti, come quello cui ha riguardo l'art. 21 Cost., ha sempre un limite non derogabile nell'esigenza che attraverso il loro esercizio non vengano sacrificati beni anche essi voluti garantire dalla Costituzione, e che tale deve ritenersi non solo la tutela del buon costume, cui l'articolo stesso fa espresso riferimento, ma anche il mantenimento dell'ordine pubblico, che è da intendere come ordine legale

[3] Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG).

[4] Disegno di legge n. 2688 dei senatori Gambaro e altri, recante "disposizioni per prevenire la manipolazione dell'informazione *online*, garantire la trasparenza sul *web* e incentivare l'alfabetizzazione mediatica", comunicato alla Presidenza il 7 febbraio 2017.

su cui poggia la convivenza sociale»[5]. L'ordine pubblico, secondo la ricostruzione che emerge dalla giurisprudenza costituzionale, è un concetto volto a tutelare le norme che esprimono i valori fondamentali della società, la cui osservanza ed attuazione è ritenuta indispensabile per l'esistenza dell'ordinamento giuridico[6].

La falsità della notizia può inoltre rilevare con riguardo all'esercizio del diritto di cronaca. Infatti, secondo il mai superato insegnamento, enunciato in due famose sentenze della Corte di cassazione[7], l'esercizio del diritto di cronaca è legittimo anche se incide su diritti altrui (onore, riservatezza ecc.) laddove sussistano tre concorrenti condizioni: (i) la verità oggettiva o quanto meno "putativa" del fatto esposto, (ii) l'interesse pubblico alla conoscenza dei fatti riferiti e (iii) la forma civile dell'esposizione. La verità del fatto, oggettiva e putativa, rileva quindi solo al fine dell'attribuzione di responsabilità a carico di chi pubblica una notizia lesiva di altrui interessi. La verità della notizia, invece, non è considerata dall'ordinamento come presupposto per consentirne o meno la libera diffusione.

Le conclusioni sopra richiamate non sono contraddette neppure dalla disciplina sul cosiddetto negazionismo. Sul tema, com'è noto, si è aperto un acceso dibattito a seguito delle sentenze della Corte europea dei diritti dell'uomo nel caso Perinçek c. Svizzera. La Corte EDU ha ritenuto che la condanna, fondata sulla norma incriminatrice elvetica che punisce chi pubblicamente neghi, minimizzi grossolanamente o cerchi di giustificare un genocidio o altri crimini contro l'umanità, viola l'art. 10 CEDU, in quanto tale limitazione alla libertà di espressione non risulta "necessaria in una società democratica"[8]. Sul piano nazionale, la l. 115/2016 ha considerato il negazionismo (ovvero il negare l'esistenza della Shoah, di un crimine di genocidio o di guerra come definiti dallo Statuto di Roma, istitutivo della Corte penale internazionale) non come illecito in sé e per sé considerato, ma come circostanza aggravante dei delitti di propaganda nazista e di istigazione o incitamento alla commissione di atti razzisti.

La mera circostanza che una notizia sia falsa, in definitiva, non è oggi sufficiente per giustificare una restrizione alla sua circolazione.

3. Libertà di informazione e *fake news*

Un recente disegno di legge ha previsto l'introduzione in Italia di un generale divieto di trasmettere on line notizie non veritiere[9].

Il disegno di legge in questione propone infatti di introdurre un nuovo art. 656-*bis* del codice penale secondo cui, se il fatto non costituisce un più grave reato, «chiunque pubblichi o diffonda notizie false, esagerate o tendenziose che riguardino dati o fatti

[5] C. Cost. 19/1962 e 199/1972.

[6] Sull'ordine pubblico come complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale» cfr., *ex multis,* le sentenze della C. Cost. 81/2017, 118/2013, 35/2011, 226/2010, 50/2008, 222/2006, 428/2004, 407/2002.

[7] Cass. civ., sez. I, 18 ottobre 1984, n. 5259 e Cass. pen., sez. un., 30 giugno 1984, n. 8959, *Ansaloni.*

[8] CEDU, *Perinçek c. Svizzera*, ric. 27510/08 (2015).

[9] Cfr. nota 4.

manifestamente infondati o non veritieri, attraverso s*ocial media* o altri siti che non siano espressione di giornalismo *online*» è punito con l'ammenda fino a euro 5.000. Questa norma, si legge nella relazione illustrativa del disegno di legge, sarebbe necessaria »per limitare e prevenire la diffusione delle cosiddette *fake news* che rischiano di creare allarmi infondati tra la popolazione».

Il disegno di legge introduce inoltre la responsabilità dei gestori dei siti *internet* in caso di pubblicazione o diffusione di notizie non attendibili o veritiere. La proposta impone ai gestori dei siti l'obbligo di effettuare un costante monitoraggio di quanto diffuso sulle proprie piattaforme *web*, compresi i commenti degli utenti, con particolare riguardo a frasi offensive e a informazioni verso le quali viene manifestata un'attenzione diffusa e improvvisa, per valutarne l'attendibilità e la veridicità. Quando i gestori rintracciano simili anomalie o ricevono segnalazioni in questo senso sono tenuti alla rimozione di tali contenuti dalla piattaforma. I gestori che non procedono in tal senso sono soggetti ad un'ammenda fino ad euro 5.000. E' prevista la possibilità per i gestori di avvalersi delle segnalazioni degli utenti circa contenuti o condotte illecite ravvisate sul portale (art. 7 del disegno di legge).

Questo progetto di legge, se fosse approvato, finirebbe per introdurre una surrettizia forma di censura, del tutto incompatibile con le garanzie offerte dalla nostra Costituzione alla libertà di informazione. Esso comporterebbe inoltre una patente violazione della disciplina nazionale ed europea sulla responsabilità degli Internet Service Provider. L'art. 15, par. 1, della direttiva 2000/31/CE, infatti, vieta alle autorità nazionali di adottare misure che impongano ad un prestatore di servizi di *hosting* di procedere ad una sorveglianza generalizzata sulle informazioni che esso memorizza. In attuazione di tale previsione, l'art. 17 del d.lgs. 70/2003 ha escluso la possibilità di assoggettare l'*hosting provider* a un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, o a un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. La Corte di giustizia, con giurisprudenza ormai consolidata, ha del resto ritenuto incompatibile con la direttiva 2000/31 l'imposizione a un *hosting provider* dell'obbligo di approntare una sorveglianza generalizzata al fine di prevenire la diffusione in rete di contenuti illeciti[10].

La direttiva 200/31/CE e il d.lgs. 70/2003 prevedono peraltro a carico dell'host provider un obbligo di informare l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite, ed a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in loro possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite. Inoltre il fornitore di servizi di *hosting* è tenuto immediatamente a rimuovere i contenuti illeciti su richiesta dell'autorità competente.

Ben più convincente è quindi l'approccio, diametralmente opposto a quello del disegno di legge sopra richiamato, che emerge dalla dichiarazione congiunta "su libertà d'informazione, *fake news*, disinformazione e propaganda", firmata a Vienna il 3 marzo 2017 dal Relatore Speciale delle Nazioni Unite per la libertà di opinione e espressione, dal Rappresentante sulla libertà dei media dell'OSCE (Organizzazione per la sicurezza

[10] Cfr. CGUE, C-70/10, *Scarlet Extended* (2011), p.to 40 e C-360/10, *SABAM* (2012), p.ti 44 ss.

e la cooperazione in Europa) e dai Relatori speciali per la libertà di espressione dell'Organizzazione degli Stati americani e della Commissione africana per i diritti umani e dei popoli.
La dichiarazione di Vienna muove dalla consapevolezza del crescente tasso di disinformazione e di propaganda nei social media, e dei danni che da ciò possono conseguirne per gli individui e per la società nel suo complesso.
In questa prospettiva, viene sottolineato il ruolo decisivo giocato da Internet e dalle tecnologie digitali nel permettere agli individui di trasmettere e mettere in circolazione idee e informazioni che possono determinate forme di disinformazione e di propaganda. Nello stesso tempo, tuttavia, si esprime una forte preoccupazione per l'adozione, da parte degli ISP, di misure volte a limitare l'accesso o la circolazione di dati sulla base di algoritmi o altri meccanismi automatici di riconoscimento e rimozione, laddove si tratti di misure non trasparenti che possano arbitrariamente limitare la libera diffusione di idee e notizie in rete.
La Dichiarazione di Vienna ha quindi ribadito il principio, ben noto al legislatore europeo, secondo cui gli ISP non possono essere ritenuti responsabili per i contenuti immessi in rete da terzi, se non quando rifiutino di adempiere a un ordine di rimozione adottato dalla competente autorità nel rispetto dei principi del contraddittorio e del diritto di difesa dei soggetti interessati. La Dichiarazione di Vienna ha quindi ribadito che l'imposizione agli ISP dell'obbligo di adottare sistemi di filtraggio preventivo dei dati trasmessi in rete, costituirebbe una illegittima violazione della libertà di informazione.
La Dichiarazione di Vienna ha infine ribadito che l'introduzione di un generale divieto di diffusione delle informazioni basato su concetti vaghi o ambigui, tra cui ad esempio quelli di "false informazioni" o "informazioni non obiettive", comporterebbe una illegittima violazione dei principi in materia di libertà di informazione.

4. Conclusioni

Il nostro ordinamento prevede numerosi strumenti volti a reprimere la diffusione di idee e notizie lesive di interessi costituzionalmente protetti. Le enormi potenzialità trasmissive oggi offerte dalla rete rendono necessario rafforzare questi strumenti e adattarli alle particolari caratteristiche di Internet. Sempre più avvertita, ad esempio, è l'esigenza di individuare adeguati strumenti per la protezione del diritto d'autore contro le violazioni commesse on line[11]. Al riguardo l'Autorità per le garanzie nelle comunicazioni ha adottato un regolamento[12] che, ferme restando le eventuali procedure autoregolamentate di *notice and take down*, prevede un apposito procedimento dinanzi all'Autorità (aggiuntivo e non sostitutivo della tutela giurisdizionale) volto ad accertare e reprimere eventuali violazioni del diritto d'autore commesse in rete. Il procedimento

[11] Al riguardo cfr. da ultimo CGUE, C-610/15, *Stichting Brein c. Ziggo BV, XS4ALL Internet BV* (2017), con specifico riferimento alla diffusione di opere protette dal diritto d'autore mediante piattaforme di condivisione online

[12] Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del d.lgs. 70/2003, approvato con la delibera del 12 dicembre 2013, n. 680/13/CONS.

così delineato assicura una tutela rapida, da parte di un soggetto indipendente e dotato di adeguata competenza tecnica, nel pieno rispetto dei principi in materia di diritto di difesa e di tutela del contraddittorio. Questo regolamento potrebbe costituire un modello utilizzabile anche per fronteggiare violazioni on line di altri diritti fondamentali.
Più difficile è invece immaginare forme di intervento volte a bloccare la diffusione di notizie e idee solo perché ritenute false. I principi in materia di libertà di informazione sanciti dalla Costituzione, dalle Carte europee dei diritti e dalla Dichiarazione di Vienna, unitamente alla disciplina nazionale e europea sulla responsabilità degli ISP, non permettono di introdurre un generico divieto di trasmettere *fake news*, e neppure di imporre obblighi di controllo e di filtraggio a carico degli ISP sulle informazioni immesse in rete dai loro utenti.
Sotto questo profilo lasciano perplessi i tentativi di autoregolazione proposti recentemente da Google e Facebook, ovvero l'introduzione di algoritmi che limitano la diffusione di notizie false o anche la limitazione degli introiti pubblicitari sulle pagine web che sono solite diffondere *fake news*. In questo modo si legittima infatti l'introduzione di forme censorie basate su un dato, la verità della notizia, che potrebbero prestarsi ad usi distorti e incompatibili con i nostri principi costituzionali.
Altrettanto dubbie paiono le proposte, da più parti avanzate, volte ad abolire l'anonimato sulla rete. La giurisprudenza ha riconosciuto, in alcune decisioni, la responsabilità dell'ISP che copra l'anonimato di persone che abbiano immesso in rete contenuti illeciti[13]. Non esiste tuttavia per gli ISP un obbligo generalizzato di identificazione degli utenti che veicolano contenuti in rete. Da una parte sarebbe senz'altro opportuno introdurre strumenti che permettano di segnalare le notizie generate automaticamente da robot, per mettere gli utenti in condizione di valutare adeguatamente tali notizie. Vietare la diffusione di notizie non riconducibili ad un autore ben identificato è però cosa ben diversa: una limitazione del genere potrebbe infatti ridurre il pluralismo delle fonti e scoraggiare la diffusione di notizie e di idee critiche nei confronti dei detentori di potere politico o economico, in contrasto con i principi desumibili dalla nostra Costituzione. E' noto che la cosiddetta primavera araba, che ha messo in crisi alcuni regimi autoritari, è nata da notizie e opinioni critiche diffuse in rete da oppositori del regime che hanno sfruttato la garanzia di anonimato.
Dobbiamo quindi rassegnarci alla diffusione di notizie false in rete? La domanda è ovviamente retorica. Gli strumenti per combattere la diffusione di idee e notizie ingiustamente lesive di valori costituzionalmente protetti, che il nostro ordinamento già prevede, andrebbero rafforzati e adattati alla particolarità della comunicazione on line. Non esiste però un principio costituzionale che giustifica la possibilità di limitare la circolazione di una notizia soltanto perché la stessa è ritenuta (da chi?) non veritiera. Lo strumento per combattere le "bufale" che non siano lesive di beni costituzionalmente protetti, pertanto, deve passare dal libero confronto tra le idee in un sistema pluralistico e trasparente. L'idea di affidare a soggetti, pubblici o privati, il compito di vagliare la verità o l'attendibilità di una notizia, e conseguentemente di decidere se la stessa possa

[13] Trib. Bologna 26 novembre 2001; Trib. Belluno 25 settembre 2014. In dottrina cfr. F.Buffa, Responsabilità del gestore di sito Internet, in Questione giustizia, 9 gennaio 2017; G. Scorza, *Anonimato in rete e responsabilità del provider*, in www.interlex.it; F. Di Ciommo, *Internet (responsabilità civile)*, in Enc. giur. Treccani, Agg. 2002; G. M. Riccio, *Anonimato e responsabilità in internet*, in *Dir. inf. e inf.*, 2000, 314 ss..

o meno liberamente circolare in rete, riflette una logica paternalistica, se non autoritaria, estranea al nostro modello costituzionale.

La regolamentazione in materia di Intelligenza artificiale, robot, automazione a che punto siamo

Cecilia Trevisi

Sommario

1. Il tentativo di una definizione univoca di robot e intelligenza artificiale. - 2. Riconoscere una soggettività alle creazioni di AI. - 3. La quarta rivoluzione industriale e il dibattito collettivo. - 4. L'impulso alla regolamentazione europea dato dalla Risoluzione di febbraio. - 5. Il copyright

Keywords: AI, Automazione, Intelligenza artificiale, Robot, Robotica

1. Il tentativo di una definizione univoca di robot e intelligenza artificiale.

Il 2017 ha gettato le basi per la regolamentazione globale dell'Intelligenza Artificiale (AI) ma il primo aspetto, verrebbe da dire il più banale ma non il più scontato, è cercare di definire la robotica e l'intelligenza artificiale.

Una nozione univoca non esiste né di robot[1] (o bot) né di AI[2]. Probabilmente potrebbe essere più utile partire *a contrario* e, cioè, individuare cosa non rientri nel novero dell'AI e della robotica. Quando parliamo di AI non dobbiamo cadere nello stereotipo di un umanoide simile in tutto e per tutto all'essere umano, non si tratta del cervello umano

[1] La parola "robot" ha origine dal dramma di K. Čapek del 1921, intitolato, *RUR* (*Rossum's Universal Robots*), dal termine ceco "robota" che letteralmente significa "lavoro forzato" (cfr. nota n. 23 M.C. Carrozza, *I Robot e noi*, Bologna, 2017).

[2] J. Kaplan, *Intelligenza artificiale Guida al futuro prossimo*, Roma, 2017, 31 «L'uso originario dell'espressione "intelligenza artificiale" può essere attribuito a un individuo specifico, John McCarthy, che nel 1956 era un assistente universitario di matematica al Dartmouth College di Hanover, New Hamphsire. Insieme a altri tre ricercatori […], McCarthy organizzò a Dartmouth un convegno estivo sull'argomento […] La richiesta di fondi originale […] affermava che "Lo studio procederà sulla base della congettura che tutti gli aspetti dell'apprendimento o qualsiasi altra caratteristica dell'intelligenza possa essere di principio descritta in modo così preciso che una macchina la possa simulare […] McCarthy scelse per la conferenza l'espressione intelligenza artificiale, in parte per distinguere il lavoro suoi e dei suoi colleghi dal più consolidato campo della cibernetica – "lo studio scientifico del controllo e della comunicazione nell'animale e nella macchina" […]».

o di un succedaneo[3] ma di algoritmi in grado di elaborare milioni di dati e fornire, sostanzialmente su basi statistiche, risposte. AI, sulla base di tale inquadramento, si riduce ad una serie di calcoli matematici, ancorché elaborati, indipendenti dalla fisicità della macchina; non necessariamente le applicazioni di AI si percepiscono pertanto nella loro materialità[45].

Non è dunque il *corpus mechanicum* a definire e qualificare l'AI bensì un processo totalmente automatizzato basato sull'acquisizione e l'elaborazione di informazioni in grado di fornire un risultato, di correggerlo e implementarlo. L'*input* resta quello umano: è quest'ultimo che sceglie l'obiettivo che l'applicazione di AI deve perseguire.

La difficoltà concreta iniziale, cercare una definizione di AI, è data dalla scelta del sostantivo "intelligenza" e dalla sua declinazione "apprendimento automatico".

Gli algoritmi, i calcoli statistici non sono dotati di intelletto e non apprendono, tuttavia sono in grado, tramite elaborazioni complesse di ottenere effetti capaci di modificare la realtà, interagendo con l'essere umano, arrivando addirittura a sostituirne il processo volitivo ma limitato – almeno allo stato attuale – alla scelta iniziale del suo ideatore e utilizzatore.

Un'applicazione di AI nel campo di riabilitazione medica non è in grado di calcolare un premio assicurativo, di effettuare transazioni finanziarie di concedere o rifiutare un mutuo, di predisporre il miglior contratto di *merger and acquisition* e viceversa, nessuna di queste attività generate da un'elaborazione matematica è interscambiabile l'una con le altre. Dunque l'AI e le sue (attuali) applicazioni, seppure eccezionali, sono settoriali e necessitano comunque di un impulso iniziale esterno nella fase di programmazione.

Nonostante la Risoluzione del Parlamento europeo del 16 febbraio 2017 recante le "raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica"[6] tratti di robotica e intelligenza artificiale citandoli separatamente come vi fosse una consapevolezza tecnica, oltre che sostanziale, circa la loro distintività, solo l'allegato alla citata risoluzione dedica il primo punto alla «Definizione e classificazione dei "robot intelligenti"» fornendo gli indici per la loro futura individuazione a livello europeo:

«È opportuno stabilire una definizione comune europea di robot autonomo intelligente, comprese eventualmente le definizioni delle sue sottocategorie, tenendo conto delle seguenti caratteristiche:

–la capacità di acquisire autonomia grazie a sensori e/o mediante lo scambio di dati con il proprio ambiente (interconnettività) e l'analisi di tali dati;

–la capacità di apprendimento attraverso l'esperienza e l'interazione;

[3] J. Kaplan, *Intelligenza artificiale Guida al futuro prossimo*, cit., 15 «Ecco una domanda a cui è sia facile che difficile rispondere, per due ragioni: la prima è che non c'è comune accordo su cos'è l'intelligenza artificiale. La seconda è che ci sono poche ragioni, almeno al momento, per ritenere che l'intelligenza delle macchine abbia molto in comune con quella umana», 21 «La mia opinione personale sul significato dell'IA è la seguente: l'essenza dell'IA – in effetti, l'essenza dell'intelligenza – è la capacità di fare generalizzazioni appropriate in m odo tempestivo e su basi dati limitata».

[4] M.C. Carrozza, *op. cit.*

[5] Le Monde Hors Série, *Futur les avancées technologiques* , Février, 2013.

[6] Disponibile online.

–la forma del supporto fisico del robot;
–la capacità di adeguare il suo comportamento e le sue azioni all'ambiente».
Da una prima lettura sembrerebbe che vi sia una coincidenza tra il robot e il *corpum mecanicum*, quindi con la fisicità della macchina senza che tuttavia sia posto in secondo piano l'aspetto dell'autoapprendimento e dell'interazione del dispositivo con l'ambiente esterno in grado di produrre degli effetti automatici indipendentemente dalla fisicità del dispositivo.
Facendo un passo indietro, nell'indagine Eurobarometro del settembre 2012 dedicata alle inclinazioni del pubblico verso i robot, questi venivano definiti come macchine autonome capaci di aiutare gli esseri umani nelle attività quotidiane, come una specie di collaboratori, di aiutanti nei lavori in fabbrica o nelle attività di pulizia o per tutte quelle attività che possono essere pericolose per gli esseri umani, come la ricerca e il salvataggio in caso di disastri. Veniva altresì precisato che i robot avrebbero potuto essere di varie forme o dimensioni, inclusi quelli umani con l'ulteriore indicazione che gli apparecchi da cucina tradizionali, come un frullatore o un caffettiera, non erano annoverabili tra i robot[7].
Azzardando una semplificazione potremmo allora dire che il robot è un dispositivo automatico o semi-automatico in grado di assumere un comportamento dopo l'analisi e l'elaborazione dei dati ottenuti grazie a sistemi di AI. L'intelligenza artificiale è un *software* programmato e altamente elaborato capace di processare enormi quantità di dati e di auto-migliorare. I robot possono usare l'intelligenza artificiale per perfezionare le loro funzioni auto-correggendosi e implementando le proprie funzioni.

2. Riconoscere una soggettività alle creazioni di AI

Lo sviluppo della robotica e dell'intelligenza artificiale solleva importanti sfide sociali che devono essere affrontate in modo da assicurare che ai benefici di queste nuove tecnologie - percepite come un miglioramento del processo decisionale umano - si accompagni il rispetto dei diritti fondamentali.
Ed è in questa direzione che nel corso del 2017 vi sono stati i primi tentativi di regolamentazione non solo a livello europeo.
Il 28 febbraio del 2017 il comitato etico della Società Giapponese per l'Intelligenza Artificiale (Japanese Society for Artificial Intelligence - JSAI), costituito all'interno di JSAI nel mese di settembre del 2014, ha approvato le linee guida sull'intelligenza artificiale che dovranno essere osservate dai membri di JSAI.
Si tratta di nove articoli che riflettono la relazione tra AI, tecnologia e società in cui nel preambolo si afferma che:
«L'AI assumerà un ruolo significativo nel futuro dell'umanità in una vasta gamma di settori, come l'industria, la medicina, l'istruzione, la cultura, l'economia, la politica, il governo, ecc. Tuttavia, è innegabile che le tecnologie AI possano diventare dannose per la società umana o entrare in conflitto con interessi pubblici a causa di un loro abuso o uso improprio.

[7] Special Eurobarometer 382, *Public attituedes towards robots*, September 2012

Per garantire che la ricerca e lo sviluppo dell'AI rimangano a beneficio della società, i ricercatori dell'AI, in quanto professionisti altamente specializzati, devono agire in modo etico e secondo la propria coscienza e acume. I ricercatori di AI devono ascoltare attentamente le diverse opini della società e imparare da esse con umiltà. Con l'evolversi della tecnologia e lo sviluppo delle società, i ricercatori di AI dovranno costantemente cercare di sviluppare e approfondire il loro senso etico e di moralità in modo indipendente.

La Società giapponese per l'intelligenza artificiale (JSAI) formalizza le linee guida etiche che devono essere applicate dai suoi membri. Queste linee guida etiche serviranno da fondamento morale per i membri JSAI per diventare più consapevoli delle loro responsabilità sociali e incoraggiare una comunicazione efficace con la società. I membri JSAI si impegnano e rispettano queste linee guida».

Seguono i nove articoli:

«1. (Contributo all'umanità) I membri della JSAI contribuiranno alla pace, alla sicurezza, al benessere e all'interesse pubblico dell'umanità. Proteggeranno i diritti umani fondamentali e rispetteranno la diversità culturale. Come specialisti, i membri della JSAI devono eliminare la minaccia alla sicurezza umana mentre progettano, sviluppano e utilizzano l'intelligenza artificiale.

2. (Rispetto delle leggi e dei regolamenti) I membri del JSAI devono rispettare le leggi e i regolamenti relativi alla ricerca e allo sviluppo, alla proprietà intellettuale così come ogni altro accordo contrattuale. I membri della JSAI non devono arrecare danno agli altri attraverso la violazione di informazioni o proprietà appartenenti ad altri. I membri del JSAI non devono usare l'IA con l'intenzione di danneggiare gli altri, sia direttamente che indirettamente.

3. (Rispetto della privacy degli altri) I membri del JSAI rispetteranno la privacy degli altri per quanto riguarda la loro ricerca e lo sviluppo di AI. I membri della JSAI hanno il dovere di trattare le informazioni personali in modo appropriato e in conformità con le leggi e i regolamenti .

4. (Equità) I membri della JSAI saranno sempre giusti. I membri del JSAI riconosceranno che l'uso dell'IA può comportare ulteriori disuguaglianze e discriminazioni nella società che prima non esistevano e non darà luogo a pregiudizi quando si svilupperà l'intelligenza artificiale. I membri del JSAI, al meglio delle loro capacità, faranno in modo che l'intelligenza artificiale sia sviluppata come una risorsa che possa essere utilizzata dall'umanità in modo equo e imparziale.

5. (Sicurezza) In qualità di specialisti, i membri della JSAI devono riconoscere la necessità che l'intelligenza artificiale sia sicura e riconoscere la propria responsabilità nel mantenere l'IA sotto controllo. Nello sviluppo e nell'uso dell'AI, i membri della JSAI presteranno sempre attenzione alla sicurezza, alla controllabilità e alla riservatezza richiesta assicurando al tempo stesso agli utenti di IA informazioni adeguate e sufficienti.

6. (Agire con integrità) I membri del JSAI devono riconoscere l'impatto significativo che l'AI può avere sulla società. Agiranno quindi con integrità e in un modo che può essere considerato affidabile dalla società. In quanto specialisti, i membri della JSAI non asseriranno affermazioni false o poco chiare e sono obbligati a spiegare le limitazioni tecniche o i problemi dei sistemi AI in modo veritiero e in modo scientificamente

valido.
7. (Responsabilità e responsabilità sociale) I membri della JSAI devono verificare le prestazioni e l'impatto risultante delle tecnologie AI che hanno ricercato e sviluppato. Nel caso in cui venga identificato un potenziale pericolo, devono avvertire tutta la comunità. I membri della JSAI capiranno che la loro ricerca e lo sviluppo possono essere utilizzati contro la loro conoscenza ai fini di danneggiare gli altri, e si impegneranno a prevenire tale abuso. Se l'abuso dell'AI viene scoperto e segnalato, non vi sarà alcuna perdita per coloro che scoprono e segnalano l'abuso.
8. (Comunicazione con la società e lo sviluppo personale) I membri del JSAI devono mirare a migliorare la comprensione della società dell'IA. I membri del JSAI capiscono che ci sono opinioni diverse sull'AI all'interno della società e imparano seriamente da loro. Rafforzeranno la loro comprensione della società e manterranno una comunicazione coerente ed efficace con loro, allo scopo di contribuire alla pace e alla felicità complessive dell'umanità. Come professionisti altamente specializzati, i membri della JSAI cercheranno sempre il miglioramento personale e sosterranno anche gli altri nel perseguire lo stesso obiettivo.
9. (Rispetto delle linee guida etiche dell'AI) AI deve attenersi alle politiche sopra descritte allo stesso modo dei membri della JSAI al fine di diventare un membro o un quasi-membro della società».

La finalità delle Linee guida è quella di riflettere le diverse opinioni riguardo all'impatto positivo e negativo che avrà l'AI nella società giapponese con l'intento di instaurare un dialogo continuo tra il pubblico e i ricercatori sul tema delle tecnologie e, in particolare, dell'AI e del suo riflesso sui temi etici.
Tuttavia mentre i primi otto articoli racchiudono principi e orientamenti generali che dovranno guidare i ricercatori affinché la tecnologia e le applicazioni di AI abbiano un utilizzo positivo volto al miglioramento della società e non alla sua involuzione, l'art. 9 ha un contenuto innovativo: riconoscere una soggettività alle creazioni di AI, un'autonomia ed una distintività così elevata rispetto ai suoi ideatori e programmatori tale da rendere necessario che le stesse applicazioni di AI debbano a loro volta rispettare le Linee Giuda. Non solo quindi i ricercatori ma il prodotto della loro ricerca.
Il contenuto dell'art. 9 non è altro che l'iniziale riconoscimento dell'AI come autonomo membro della società[8].
Una tema, quello del riconoscimento della personalità elettronica sul quale anche l'Unione Europea si sta interrogando.
Riconoscere la personalità giuridica ai robot potrebbe aprire possibilità per la loro capacità di avere una gamma completa di diritti e doveri su base contrattuale, in base alla legge sul *copyright* e persino al diritto di famiglia (si pensi solo al tema dell'affezione al robot, aspetto anch'esso affrontato a livello europeo) questo porterebbe a uno spostamento verso la considerazione dei robot come appartenenti all'area dei "vivi" - un *tertium genus* di soggetti facenti parte di una categoria giuridica autonoma - con la naturale conseguenza che ci troveremmo ad interrogarci su cosa effettivamente significhi

[8] L.B. Solum, *Legal Personhood for Artificial Intelligences* , Illinois Public Law and Legal Theory Research Papers, Series No. 09-13 March 20, 2008.

essere un membro di una società.
In questa direzione (riconoscere autonoma soggettività alle creazioni di AI) si è mossa l'Arabia Saudita che ha concesso la cittadinanza al robot Sophia e a distanza di poche settimane Shibuya Mirai ha ottenuto la residenza di un popoloso distretto di Tokyo. Il primo è un androide, l'unico robot al mondo ad aver ottenuto la cittadinanza, il secondo un *software* o meglio, un *chatterbot*, in grado di dialogare con chiunque ne abbia voglia. Mentre è di questi giorni la notizia del "licenziamento" di Fabio, un robot che "lavorava" in un supermercato di Edimburgo perché non adeguato alle mansioni per cui era stato "assunto".
Il 16 febbraio 2017 il governo sudcoreano ha annunciato che più ministeri e agenzie governative sudcoreane avrebbero presentato nel corso del 2017 nuovi standard legali per definire (i) gli status giuridici, (ii) le responsabilità e (iii) gli standard etici delle nuove industrie basate sull'intelligenza artificiale (AI), auto a guida automatica e così via in modo che la società sudcoreana nel suo insieme possa essere preparata affinché un cambiamento possa essere innescato dalla quarta rivoluzione industriale[9]. Il governo sudcoreano sta conducendo ricerche su come riconoscere e utilizzare il valore dei big data in relazione ai diritti di proprietà, così che film, immagini e simili creati dall'AI possono essere protetti legalmente posto che secondo l'attuale legge sul copyright coreano, i proprietari del copyright sono limitati agli esseri umani.
Ed è nel numero del 27 novembre 2017 del settimanale "TIME" dedicato alle «25 migliori invenzioni del 2017» che si parla di JIBO (il primo robot destinato alle famiglie): la macchina sempre più umana e sempre meno oggetto.
«Jibo is different – it's not just that he – and I use the term he here, because that's how Jibo refers to himself – looks like something straight out of a Pixar movie, with a big, round head and a face that uses animated icons to convey emotion […] Jibo seems downright human in a way that his predecessors do not. "We want people to look at Jibo and realize he's someone and not something", says Matt Revis, the company's vice president of product management. And while that technology may seem merely amusing – or creepy, depending on your point of view – it could fundamentally reshape how we interact with machines» (Jibo è diverso - non è solo che lui - e uso il termine lui qui, perché è così che Jibo si riferisce a se stesso - sembra qualcosa uscito direttamente da un film della Pixar, con una grande testa rotonda e una faccia che usa icone animate per trasmettere emozioni […] Jibo sembra decisamente umano in un modo che i suoi predecessori non fanno. "Vogliamo che le persone guardino Jibo e si rendano conto che sia qualcuno e non qualcosa", afferma Matt Revis, vicepresidente della gestione prodotti dell'azienda. E mentre quella tecnologia può sembrare semplicemente divertente - o inquietante, a seconda dei punti di vista - potrebbe fondamentalmente rimodellare il modo in cui interagiamo con le macchine).
Gli impatti etici, sociali, filosofici e legali saranno molto importanti. La comparsa di agenti autonomi, titolari di autonoma soggettività modificherà sensibilmente il nostro modo di pensare. Questo significa che i principi fondamentali dei diritti nazionali saranno soggetti a sostanziali modifiche, sarà dunque necessario aggiungere ed integrare questi "nuovi agenti" nella teoria generale del diritto.

[9] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

3. La quarta rivoluzione industriale e il dibattito collettivo

In materia di AI si è dunque aperto un dibattito globale concretizzatosi nella predisposizione di una piattaforma online The Future Society at Harvard Kennedy School[10] per facilitare il dialogo e la discussione sull'intelligenza artificiale. Un dibattito, iniziato nel settembre del 2017 e che si concluderà il 31 marzo 2018 (attualmente nella sua seconda fase), in cui si può contribuire in inglese, francese e giapponese e che coinvolge attivamente cittadini, professionisti, esperti mondiali e ricercatori che lavorano sull'intelligenza artificiale, robotica, affari informatici, politica pubblica, relazioni internazionali ed economia.

L'obiettivo è di innescare un dialogo sulle dinamiche e sulle conseguenze dell'aumento dell'AI e di come governare l'attuale rivoluzione tecnologica. La piattaforma di *intelligence* collettiva sintetizzerà le idee e le proposte principali, che a loro volta saranno utilizzate per fornire soluzioni e strumenti politici attuabili per la *governance* internazionale dell'AI.

Nella stessa direzione si sta muovendo l'Unione europea che dopo la risoluzione del Parlamento europeo del 16 febbraio 2017 in cui i membri del Parlamento hanno invitato la Commissione europea a presentare, sulla base dell'art. 114 del TFUE, una proposta di direttiva sulle norme di diritto civile in materia di robotica, la Commissione giuridica (JURI) del Parlamento ha deciso di organizzare una consultazione pubblica sul futuro della robotica e dell'intelligenza artificiale che si è conclusa il 1 giugno 2017. Sono state ricevute 298 risposte e tutti i risultati della consultazione, si legge nel comunicato pubblicato l'8 dicembre 2017 sul sito del parlamento europeo, «confluiranno nella relazione del Servizio Ricerca del Parlamento europeo intitolata "Cost of Non-Europe on Robotics and Artificial Intelligence Report" (relazione sul costo della non Europa in materia di robotica e intelligenza artificiale), di prossima pubblicazione, e saranno d'aiuto al Parlamento europeo nell'affrontare le questioni etiche, economiche, giuridiche e sociali che si pongono nel settore della robotica e dell'intelligenza artificiale per uso civile».

4. L'impulso alla regolamentazione europea dato dalla Risoluzione di febbraio

Quattro i temi fondamentali affrontati nella Risoluzione del 16 febbraio 2017: (i) la responsabilità per eventuali danni, (ii) uno status giuridico dei robot come "persone elettroniche", (iii) l'affezione e le possibili dipendenze emotive degli esseri umani rispetto ai robot dotati di una autonoma capacità di apprendimento e (iv) la problematica della disoccupazione quale conseguenza della robotizzazione.

Il Parlamento ritiene in primo luogo che le manifestazioni di AI rappresentino una nuova rivoluzione industriale «rendendo imprescindibile che la legislazione ne conside-

[10] V. Il relativo sito Internet (http://assembl-civic.bluenove.com)

ri le implicazioni e le conseguenze legali» per cui è di fondamentale importanza «creare una definizione generalmente accettata di robot e di intelligenza artificiale» flessibile e che non sia di ostacolo all'innovazione (considerando B. e C.).
Considera di fondamentale importanza che gli esseri umani abbiano il controllo sulle macchine intelligenti in ogni momento («[...] gli sviluppi nel capo della robotica e dell'intelligenza artificiale possono e dovrebbero essere pensati in modo tale da preservare la dignità, l'autonomia e l'autodeterminazione degli individui [...]» considerando O.) soprattutto nella prospettiva che nel lungo termine l'AI superi «la capacità intellettuale umana» (considerando P.).
Ritiene che nell'attuale quadro giuridico vi sia un vuoto normativo che neppure la normativa sulla responsabilità da prodotto difettoso è in grado di colmare, riguardante i danni causati da un robot laddove quest'ultimo abbia preso decisioni autonome, ragion per cui considera essenziale una regolamentazione sugli aspetti legati alla responsabilità giuridica «derivante dall'azione nociva di un robot» posto che «più i robot sono autonomi, meno possono essere considerati come meri strumenti nelle mani di altri attori (quali il fabbricante, l'operatore, il proprietario, l'utilizzatore, ecc.)» (considerando Z., AA., AD, AE).
Sulla scorta di tale assunto reputa opportuno che debba sussistere un sistema generale per la registrazione dei robot (principi generali – art. 2) così come una "scatola nera" in dotazione ai robot più sofisticati in grado di registrare i dati su ogni operazione, «compresi i passaggi logici che hanno contribuito alle sue decisioni» (principi etici – art. 12.). Parimenti ravvisa che un sistema di assicurazione obbligatoria integrato da un fondo per garantire la possibilità di risarcire i danni in caso di assenza di copertura assicurativa, come avviene per le auto, possa essere una soluzione concreta al tema della responsabilità civile (responsabilità – artt. 57, 58).
Invita inoltre la Commissione a valutare la possibilità di istituire uno status giuridico specifico «per i robot [...] in modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendano decisioni autonome o che interagiscano un modo indipendente con terzi» (responsabilità – art. 59f)). Avremo quindi una "capacità giuridica" ed una "capacità d'agire" di nuova generazione, poi sarà interessante capire come i robot in via autonoma siano in grado di un risarcimento in forma specifica o di un'obbligazione di fare o non fare.
Si è altresì sottolineata l'importanza di affrontare la possibilità che nasca un attaccamento emotivo tra gli uomini e i robot soprattutto per le categorie più vulnerabili (bambini, anziani e disabili) con le connesse questioni aperte riguardo all'impatto «emotivo e fisico che un tale attaccamento potrebbe avere sugli uomini» (principi generali – art. 3). La connessione emotiva tra umani e robot è un aspetto già attuale: si pensi al robot Jibo, di cui si è accennato, creato per interagire con l'ambiente familiare e diventarne un componente.
Rispetto all'invecchiamento generale della popolazione (per cui si stima che nel 2025 oltre il 20% dei cittadini europei avrà un età uguale o superiore a 65 anni e si assisterà ad un aumento particolarmente rapido di coloro che avranno più di 80 anni), si ritiene

che l'uso dei robot per l'assistenza agli anziani sarà sempre più diffuso e più mirato nel campo della riabilitazione (anche cognitiva). Ciò comporterà una ulteriore integrazione tra essere umano e robot laddove ai primi viene in ogni caso riconosciuto un ruolo principale e non completamente sostituibile dagli assistenti robotizzati.
Si è osservato che l'uso dei robot consentirebbe «di liberare le persone dalla monotonia del lavoro manuale, consentendo loro di avvicinarsi a mansioni più creative e significative» e, allo stesso tempo, potrebbe comportare una maggiore automazione per le mansioni meno qualificate con una conseguente trasformazione del mercato del lavoro delle politiche sociali[11]. Sulle questioni lavoristiche c'è ancora molta incertezza, recentemente Neil Jacobstein - professore di intelligenza artificiale della Singularity University - ha parlato di reddito universale, ritenendo che si dovrà usare «la ricchezza creata dall'intelligenza artificiale e redistribuirla a chi perde il lavoro».

5. Il copyright[12]

Con riguardo al campo della proprietà intellettuale e di quanto l'AI sia in grado di creare in via autonoma, i membri hanno invitato la Commissione a sostenere un approccio orizzontale e tecnologicamente neutrale nei confronti della proprietà intellettuale applicabili ai vari settori in cui la robotica potrebbe essere impiegata.
In campo medico si suggerisce espressamente di introdurre l'obbligo per i produttori di avanzati dispositivi salvavita di fornire ad appositi enti di fiducia indipendenti oltre alle istruzioni relative alla progettazione dei dispositivi i codici sorgente, come accade per il deposito legale di una pubblicazione presso la biblioteca nazionale. Anche per le protesi robotiche deve essere garantito l'accesso continuo e sostenibile alle manutenzioni, migliorie e agli aggiornamenti *software*.
La possibilità di accedere liberamente ai codici sorgente è altresì esplicitato nell'allegato alla Risoluzione riguardo ad eventuali incidenti e danni causati dai robot intelligenti per garantirne il funzionamento ininterrotto, la disponibilità, l'affidabilità e la sicurezza di tali sistemi.
L'orientamento, quindi, non limitato al capo biomedico, sembrerebbe propendere per nuove eccezioni ai monopoli industrialistici, nel più ampio solco secondo cui formule, principi, piani terapeutici etc. non possono essere oggetto di privativa autorale o brevettuale.
Come sappiamo, la creatività computazionale consente al computer di produrre opere

[11] M. Ford, *Il futuro senza lavoro. Accelerazione tecnologica e macchine intelligenti. Come prepararsi alla rivoluzione economica in arrivo,* Milano, 2017.

[12] A. Levendowski, *How copyright Law can fix Artificial Intelligence's implicit bias problem*, 2017 in *Technology Law and Policy Clinical Teaching Fellow*, New York University School of Law and Research Fellow, NYU Information Law Institute; *L'Intelligence artificielle et le droit d'auteur* , 2017, OMPI Magazine.

d'arte originali[13], ma la domanda ancora in sospeso è la seguente: chi può essere considerato come l'autore di esso? L'umano che ha creato la macchina, il proprietario della macchina o la macchina stessa?[14]

Attualmente le macchine sono cose, non hanno diritti quindi, almeno con riguardo alle norme nazionali, non sono autori e non dispongono dei relativi diritti sulle opere eventualmente realizzate. Né esiste un principio codificato per cui il proprietario della macchina acquista a titolo derivativo ma in via immediata e diretta i diritti di sfruttamento economico della creazione "intellettuale". Nel sistema interno autore, quindi titolare della paternità dell'opera e dei relativi diritti morali, è solo una persona fisica; questo significa che le creazioni realizzate esclusivamente da una macchina non hanno i requisiti per essere assoggettate alla legge sul diritto d'autore[15].

Potremmo arrivare a sostenere che nel nostro ordinamento le opere create esclusivamente da AI, trattandosi di opere prive di una paternità, sono liberamente utilizzabili da chiunque[16] oppure sono equiparabili alla opere orfane e quindi, attraverso un'interpretazione estensiva, farle rientrare nel novero del d.lgs. 10 novembre 2014, n. 163, in attesa non tanto che il titolare del diritto d'autore si palesi e rivendichi l'opera considerata orfana, bensì che la legge colmi il vuoto normativo relativo all'individuazione del titolare dei diritti delle opere create direttamente ed esclusivamente da AI.

Ancora diverso è il caso di interazione tra macchina e persona fisica, laddove l'ope-

[13] Si pensi all'opera intitolata "The Next Rembrandt". Si tratta di un dipinto 3D generato dal computer che utilizza un algoritmo di riconoscimento facciale. Sono stati necessari diciotto mesi di lavoro per produrre questo quadro dopo che sono state scansionate 346 opere conosciute del pittore olandese. É un'opera formata da 148 milioni di pixel, il ritratto è stato realizzato con 168.263 frammenti presi dal lavoro dell'artista e conservati in un database progettato per questo scopo. Il progetto ha beneficiato della sponsorizzazione del gruppo bancario olandese *ING*, in collaborazione con *Microsoft*, della società di consulenza marketing J. Walter Thompson e dei consulenti della Delft University of Technology, della Mauritshuis e del Rembrandt House Museum. Nello stesso modo, sempre nel 2016, una breve storia scritta da un programma per computer giapponese ha superato la prima fase della selezione di un premio letterario nazionale. Infine, la società di intelligence artificiale *Deep Mind*, acquistata da *Google,* ha creato un software in grado di produrre musica partendo dall'ascolto delle registrazioni.

[14] Artificial Intelligence and the Law.

[15] *L'Intelligence artificielle et le droit d'auteur*, cit.: «[…] *Il semblerait cependant que, dans de nombreux pays, la législation ne soit pas disposée à protéger par le droit d'auteur des œuvres qui n'auraient pas été créées par un être humain. Aux États-Unis d'Amérique par exemple, le bureau national du droit d'auteur a déclaré que seules des œuvres originales créées par un être humain pourraient prétendre à une protection par le droit d'auteur. Cette position découle de la jurisprudence (affaire Feist Publications c. Rural Telephone Service Company, Inc. 499 U.S. 340 (1991)) aux termes de laquelle le droit d'auteur protège uniquement le fruit d'un travail intellectuel fondé sur le pouvoir créateur de l'esprit. De manière analogue, dans une récente affaire se déroulant en Australie (Acohs Pty Ltd c. Ucorp Pty Ltd), un tribunal a déclaré qu'une œuvre créée au moyen d'un ordinateur ne pouvait faire l'objet d'une protection par le droit d'auteur car elle n'avait pas été réalisée par un humain. En Europe, la Cour de justice de l'Union européenne a également affirmé à plusieurs reprises, notamment dans un arrêt historique rendu dans l'affaire Infopaq (C-5/08 Infopaq International A/Sc. Danske Dagbaldes Forening), que le droit d'auteur ne s'appliquait qu'à des œuvres originales et que l'originalité allait de pair avec "une création intellectuelle propre à son auteur." Cette décision est généralement interprétée comme signifiant qu'une œuvre originale doit être le reflet de la personnalité de son auteur, ce qui signifie qu'une intervention humaine est indispensable pour qu'une œuvre puisse être protégée par le droit d'auteur*».

[16] *L'Intelligence artificielle et le droit d'auteur*, cit.: «*[…] En théorie, on pourrait considérer que ces créations ne sont pas visées par le droit d'auteur puisqu'elles n'ont pas un être humain pour auteur. Tout le monde pourrait alors les utiliser et les réutiliser en toute liberté, ce qui serait une très mauvaise nouvelle pour les sociétés qui les commercialisent. Imaginez avoir investi des millions dans un système capable de créer de la musique pour jeux vidéo pour vous rendre compte au final que cette musique ne peut être protégée par le droit d'auteur et que n'importe qui dans le monde peut l'exploiter gratuitement […]*».

ra sia il risultato, indipendentemente dalla sua casualità, della "collaborazione" tra la macchina e il suo proprietario. Si pensi al caso che ha fatto tanto discutere gli Stati Uniti (il *selfie* del macaco che ben potrebbe essere un esempio concreto delle problematiche connesse al *copyright* creato da AI se al posto della scimmia ci fosse stato un robot[17]). Molti sostengono che sarebbe ragionevole che il proprietario della macchina fosse anche il titolare della creazione dell'opera intellettuale[18] (una declinazione del principio "possesso vale titolo" disciplinato dall'art. 1153 cod. civ.)[19] – almeno per i diritti patrimoniali di sfruttamento dell'opera - soprattutto nei casi in cui il contributo dell'essere umano sia eziologicamente connesso alla creazione intellettuale, tuttavia escludere a priori dal novero dei titolari dei diritti di sfruttamento economico delle suddette creazioni i progettisti della macchina potrebbe essere penalizzante per coloro che supportano e investono sulla valorizzazione delle creazioni intellettuali. In ogni caso, in materia autorale, l'acquisto a titolo originario può avvenire unicamente al momento della creazione dell'opera e solo da parte di una persona fisica, regola che collide con la previsione contemplata nella citata norma civilistica che presuppone che per l'acqui-

[17] «Nel 2011 il fotografo David Slater, durante un viaggio in Indonesia per un servizio fotografico sui macachi cinopitechi (Macaca nigra), decise di lasciare la propria macchina fotografica su un treppiedi lasciando il comando a distanza dello scatto inserito, a disposizione dei macachi. Una femmina schiacciò più volte il dispositivo scattando diverse fotografie: molte risultarono non utilizzabili, ma alcune presentavano invece chiare inquadrature del macaco, che Slater distribuì chiamandole "autoscatto del macaco". Il fotografo vendette le foto all'agenzia di stampa Caters, rivendicandone il copyright sul presupposto di aver manipolato le fotografie e di aver pertanto avuto "l'idea di lasciare i macachi giocare con la macchina fotografica, sapendo che sarebbe stato verosimile che le scimmie lo avrebbero fatto e prevedendo che alla fine avrebbero fatto degli scatti". Le fotografie vennero successivamente caricate nell'archivio multimediale di Wikimedia Commons, un sito che accetta solo file multimediali disponibili con licenza libera, di pubblico dominio o altrimenti con diritto d'autore ineleggibile. Sul sito le fotografie vennero taggate con licenza di pubblico dominio, sul presupposto che erano state create da un animale, e non dall'uomo. l fotografo Slater chiese allora alla Wikimedia Foundation, proprietaria di Wikimedia Commons, di pagare per mantenere le fotografie o di rimuoverle dal sito, rivendicando il copyright sulle fotografie stesse. La richiesta venne respinta dall'organizzazione, la quale affermava che le fotografie non avessero alcuna proprietà del copyright, dal momento che il creatore delle fotografie era una scimmia.» (Wikipedia – autoscatto del macaco). Peta – People for the Ethical Treatment of Animals – al fine di chiedere l'assegnazione del copyright alla scimmia e l'amministrazione del diritto d'autore ad essa stessa, decise fare causa al fotografo nel 2015. Nel 2016 una corte federale della California diede ragione al fotografo con la motivazione che le leggi americane sul copyright non prevedono di essere applicate a una scimmia. Alla fine Slater ha patteggiato di donare il 25% dei futuri guadagni derivanti dalla vendita della foto – il cui copyright gli rimane in appannaggio – ad associazioni protezioniste del Macaco.

[18] Principio applicabile in base al diritto d'autore anglosassone, difatti l'art. 9.3 del Copyright Designs and Patents Act 1988 prevede espressamente che «*In the case of a literary, dramatic, musical or artistic work which is computer – generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken*» e nel successivo art. 178 è esplicitato che «*'computer-generated' means the work is generated by computer in circumstances such that there is no human author of the work*».

[19] *Contra* Cass. civ., sez. I, 3 gennaio 2017, n. 39 la Corte di legittimità ha ritenuto impossibile nel diritto d'autore la consegna fisica dell'opera posto che laddove questa vi sia si riferisce esclusivamente al supporto materiale su cui la creazione è estrinsecata. «Non è configurabile l'acquisto a titolo originario di un'opera immateriale dell'ingegno, nella specie cinematografica, in base ad un titolo astrattamente idoneo per effetto del possesso di buona fede, ai sensi dell'art. 1153 c.c., a ciò ostando il carattere particolare del diritto d'autore, che trova fondamento unicamente nell'atto creativo e realizzativo dell'idea, per il trasferimento del quale non si richiede una consegna, perché questa, anche ove ricorra, si riferisce all'oggetto materiale in cui l'opera si estrinseca, senza però mai immedesimarsi in essa» (commentata in *Il diritto industriale, 1, 2018, 59*). In senso conforme: Cass. civ., sez. I, 29 dicembre 2011, n. 30082.

rente *a non domino* l'acquisto è a titolo originario[20].

La questione rileva anche dal punto di vista delle invenzioni brevettabili, può una macchina essere titolare di un brevetto o quest'ultimo compete di diritto al suo proprietario? Pur non esistendo un divieto espresso di non brevettabilità delle invenzioni create dall'AI, l'individuo resta l'unico soggetto al quale è riconosciuto il diritto morale sull'invenzione.

Rendere liberamente accessibili opere realizzate in tutto o in parte dai sistemi di AI se da un lato comporterebbe una ancora più massiva fruibilità di tali creazioni con la conseguente limitazione di un controllo monopolistico da parte dei produttori, dall'altro lato riconoscere e consolidare la protezione autorale permetterebbe uno stimolo a tali creazioni; temi alla base di un dibattito molto più ampio in materia di copyright tanto da richiedere un approfondimento specifico.

[20] M. Fabiani, *Esecuzione forzata e sequestro delle opere dell'ingegno* , Milano, 1958.

A proposito del volume "Civiltà giuridica della comunicazione"

Carlo Melzi d'Eril

La questione di come soddisfare la pretesa di giustizia dei consociati si è sempre posta in ogni società; in quelle che si fondano su principi democratici, in particolare, tale pretesa assume se possibile ancora maggior importanza, poiché proprio nell'assicurare l'effettivo rispetto delle proprie norme un ordinamento trova una sua irrinunciabile forma di legittimazione.

Non può stupire, pertanto, che alcuni casi di delitti efferati o comunque di gravi episodi di criminalità divengano un tema centrale della divulgazione mediatica: poiché le norme penali presidiano gli aspetti basilari della vita comune di una società, la loro violazione colpisce spesso l'opinione pubblica che matura l'aspettativa di una risposta sanzionatrice adeguata, che assicuri l'effettività di tali norme. L'appagamento di questa aspettativa, tuttavia, richiede non solo un processo e una sentenza definitiva che assicurino il rispetto della legge mediante la ricostruzione della verità, ma anche che l'esito di tale attività processuale sia percepibile e sia effettivamente percepito come "giusto" da parte dei consociati, cioè di una generalità di cittadini che nel complesso è priva di competenze tecnico-giuridiche ed è pertanto incline a valutare l'esito concreto del processo con criteri di tipo schiettamente sostanziale.

I temi della ricostruzione della realtà in sede giudiziale e della sua efficace e corretta comunicazione all'opinione pubblica sono il fulcro del volume di Giovanni Paolo Accinni "*Civiltà giuridica della comunicazione*" (Milano, Giuffrè, 2018), giunto ora alla seconda edizione e arricchito da tre preziose appendici, relative rispettivamente al segreto istruttorio e la pubblicazione di atti d'indagine; al delitto di diffamazione; infine – aggiunta di questa edizione – all'attualissimo tema della responsabilità penale dell'*hosting provider "attivo"*.

Accinni propone un giudizio fortemente critico rispetto al c.d. "circo mediatico giudiziario" che i media tendono a creare in relazione a eclatanti vicende giudiziarie. Le premesse del ragionamento muovono da una riflessione di ampio respiro circa le possibilità umane di giungere alla verità, di cui l'autore non può che proporre un concetto relativo. Come noto, infatti, anche nell'ambito delle scienze esatte le teorie che sono considerate validate devono comunque essere intese come relative, sempre aperte alla confutazione sulla base di prove che le smentiscano; a maggior ragione, negli altri ambiti di indagine – quale quello giuridico – l'uomo può aspirare alla ricerca non di una verità assoluta, ma di quella che più possibilmente le si avvicina. Ciò non implica, però, un atteggiamento rinunciatario o di puro scettiscismo; anzi, la piena consapevolezza dei limiti della conoscenza deve stimolare la ricerca del vero nel modo più accurato possibile, rendendo decisiva la scelta di un metodo rigoroso di indagine idoneo a verificare la plausibilità di un assunto.

Accinni sottolinea con intelligenza come il processo penale sia «lo "scontro" tra diver-

se narrazioni attraverso la dialettica legale con cui ciascuna delle parti cerca di ottenere il risultato sperato attraverso lo strumento retorico della persuasione». In questo senso l'autore propone un recupero dei concetti di retorica e persuasione, restituendo a essi il loro significato originario depurato dalle connotazioni negative che possono assumere nel linguaggio comune: rispettivamente, la retorica si distingue quale «forma di comprensione razionale di realtà […] non pienamente conoscibili attraverso le c.d. "scienze esatte"» e la persuasione è l'esito di un efficace esercizio di retorica, consistendo nella ragionata adesione a una delle tesi esposte in ragione dell'attendibilità delle prove offerte.

Il processo dovrebbe porsi quale la sede in cui il giudicante, anche mediante i mezzi retorici a cui ricorrono accusa e difesa, si convince di quale delle ricostruzioni proposte sia più attendibile e in questo modo determina quale debba essere considerata sul piano giuridico la verità: un procedimento, pertanto, che si deve fondare sul rigore del metodo e sull'esclusione della plausibilità delle ricostruzioni diverse da quella prescelta, ma sempre nella consapevolezza che la certezza in termini assoluti non è umanamente possibile. Proprio questa consapevolezza, lungi dall'impedire di giungere a una verità processuale, giustifica la previsione di un elevato standard per cui una condanna può essere pronunciata solo qualora la colpevolezza risulti al di là di ogni *ragionevole* dubbio: deve cioè escludersi che, con gli strumenti della ragionevolezza, un'ipotesi diversa da quella accusatoria sia plausibile.

L'autore pone il problema del metodo rigoroso per giungere a una verità accettabile, tuttavia, non solo all'interno del processo penale, ma anche e soprattutto al di fuori, nell'ambito della comunicazione massmediatica che sempre più ossessivamente si concentra sui casi di "cronaca nera": è proprio quest'ultimo l'aspetto oggi più critico per due motivi strettamente legati tra loro.

Da un lato, l'informazione veicolata dai media sui delitti e sui relativi processi si rivela sempre più spesso contraddistinta sia dall'assenza di una minima cultura garantista, sia da una desolante povertà metodologica nella ricostruzione dei fatti; la conseguenza è che si assiste, con i tempi rapidi imposti dalle forme di comunicazione contemporanea, all'imbastimento di veri e propri processi mediatici che si consumano in parallelo e preventivamente rispetto a quelli nelle aule dei tribunali, giungendo a individuare una sorta di verità mediatica che si fonda su processi emozionali e sensazionalistici, sulla base di elementi parziali, spesso travisati o estranei alla vicenda del reato.

Dall'altro lato, non è affatto remota la possibilità che i soggetti giudicanti, rispetto alla formazione della verità processuale, subiscano il condizionamento esterno derivante dalle aspettative che sono così sorte nell'opinione pubblica. I processi conoscitivi, infatti, restano sempre condizionati dal contesto culturale e sociale del soggetto che ricerca la verità; Accinni ricorda come questo sia valido persino quando si osservi un fenomeno con gli strumenti delle scienze esatte e, a maggior ragione, ciò valga soprattutto nelle scienze umanistiche (fra cui quella giuridica).

Il giurista che si occupa di informazione troverà dunque di notevole interesse le riflessioni proposte sulla comunicazione della realtà e la distanza fra la ricostruzione giudiziale e quella giornalistica e radiotelevisiva, che evidenziano gli enormi rischi derivanti dalla celebrazione di veri e propri "riti mediatici". Nel momento corrente, in cui tanto

si discute di *fake news* e post-verità, si rivelano di estrema attualità le considerazioni sulla fascinazione collettiva per teorie e ricostruzioni ascientifiche, che contrastano con consolidate e provate evidenze fattuali – come nell'esempio, più volte evocato dall'autore, delle pseudo teorie antivacciniste che incredibilmente stanno avendo diffusione. Il volume sottolinea con efficacia come sia proprio la propensione ad analisi immotivate e superficiali, incoraggiata dalle modalità della comunicazione massmediatica, a fondare nell'opinione pubblica il convincimento di avere tutti gli strumenti necessari per stabilire quale sia la corretta ricostruzione dei fatti oggetto di un giudizio penale che ha avuto gli onori della cronaca, come – se non meglio – degli stessi organi giurisdizionali deputati a farlo.

L'impressione diffusa dagli stessi organi di informazione, infatti, è che i mezzi legali a cui si deve ricorrere nel processo per l'accertamento dei fatti siano farraginosi e lenti, inidonei a fotografare davvero la realtà delle cose; nella collettività difficilmente matura il dubbio circa l'attendibilità della ricostruzione grossolana che trapela attraverso i canali di comunicazione di massa, né circa la ragionevolezza delle conclusioni a cui si giunge, spesso dettate dal dato emotivo e dalla volontà di trovare a tutti i costi un colpevole. In questo modo, le decisioni giudiziali che non assecondano il sentire popolare – caso non infrequente, viste le modalità con cui quest'ultimo si forma – determinano una crescente sfiducia verso il sistema giudiziario, percepito a torto come incapace di rendere davvero giustizia. Accinni presenta approfonditamente alcuni casi noti che evidenziano lo iato fra accertamento giudiziale e comunicazione giornalistica e radiotelevisiva, in particolare descrivendo alcuni aspetti dei processi per l'omicidio di Yara Gambirasio e di Meredith Kercher (richiamando proprio come in tale vicenda la Cassazione abbia pesantemente stigmatizzato i mass media per aver a tal punto esercitato un condizionamento da pregiudicare il corretto svolgimento delle indagini preliminari), nonché del processo contro O.J. Simpson; ma la sua ragionata e profonda critica al sistema massmediatico va oltre.

L'autore presenta infatti anche il caso del processo di Norimberga nei confronti dei gerarchi nazisti, evidenziando come la stampa dell'epoca (persino quella tedesca) fosse stata totalmente acritica nei confronti di un tribunale istituito dai vincitori per giudicare gli sconfitti sulla base di illeciti non codificati nel momento in cui erano stati commessi, in violazione del principio di legalità penale – nonché in contrasto con la stessa promessa di giudicare tutti i crimini di guerra, poiché non furono mai oggetto di processo le condotte poste in essere dai vincitori. Il processo di Norimberga fu presentato con successo all'opinione pubblica quale il trionfo del diritto e della giustizia, evidenziando ancora una volta sia il peso che la comunicazione mediatica ha nel modellare le opinioni delle masse, sia la sua scarsa familiarità con alcune delle più elementari istanze garantiste che pure formano una parte essenziale del patrimonio giuridico occidentale. Infine il caso di "Tangentopoli" è presentato quale esempio paradigmatico della deriva "oracolare" che può essere provocata dalla comunicazione mediatica quando essa non sia in contrasto con lo svolgimento o le conclusioni di un processo, bensì aderisca a indagini o a tesi accusatorie proposte dagli inquirenti o dalla pubblica accusa e che per qualche motivo godano di ampio riscontro sociale. La serrata critica dell'autore alle modalità proprie dell'odierno sistema di comunicazione di massa sembra così cogliere

perfettamente nel segno quando individua nella sua velocità e approssimazione l'idoneità ad assecondare forme di esercizio del potere di natura "carismatica".
Uno dei pregi del volume è dunque quello di illustrare i procedimenti perversi di comunicazione, demistificandone i presupposti ed evidenziandone le nefaste conseguenze. È forse poco probabile che nel prossimo futuro si assista nell'arena del dibattito pubblico al recupero delle virtù della retorica e della persuasione (nei termini sopra chiariti), soluzione che l'autore propone per colmare positivamente lo iato fra decisioni processuali e sentire popolare; tuttavia, non si può che condividere l'appello affinché la comunicazione mediatica sia più responsabile e si fondi su un autentico dialogo fra saperi specialistici nel tentativo di veicolarne i contenuti in forme comprensibili per un pubblico indistinto, senza tradirne il contenuto, mediante «rinnovati percorsi di addestramento culturale».

Civiltà giuridica della comunicazione
Autore: Giovanni Paolo Accinni
Anno di edizione: 2018
Pagine: VIII – 232
Codice Prodotto: 024201628
ISBN: 9788814226762

Elenco autori

Apa, Ernesto
avvocato in Roma
Arpetti, Jacopo
dottorando di ricerca in ingegneria dell'impresa, Università degli studi di Roma "Tor Vergata"
Basile, Fabio
professore ordinario di diritto penale, Università degli studi di Milano
Bellezza, Marco
avvocato in Roma
Buzzelli, Silvia
professore associato di diritto processuale penale, Università degli studi di Milano Bicocca
Caggiano, Giandonato
professore ordinario di diritto dell'Unione europea, Università degli studi Roma Tre
Campolo, Iolanda
avvocato in Milano
Castellaneta, Marina
professore ordinario di diritto internazionale, Università degli studi di Bari "Aldo Moro"
De Gregorio, Giovanni
dottorando di ricerca in scienze giuridiche, Università degli studi di Milano Bicocca
De Vivo, Jessica
dottoressa di ricerca in scienze giuridiche, Università degli studi di Milano Bicocca
D'Ippolito, Guido
dottorando di ricerca in diritto dell'economia e dei consumatori, Università degli studi Roma Tre
Donati, Filippo
professore ordinario di diritto costituzionale, Università degli studi di Firenze
Frigerio, Filippo
cultore della materia di diritto dell'informazione, Università Commerciale "L. Bocconi"
Gorassini, Attilio
professore ordinario di diritto privato, Università "Mediterranea" di Reggio Calabria
Indovina, Barbara
avvocato in Milano
Lazzaro, Anna
ricercatrice di diritto amministrativo, Università degli studi Messina
Martinelli, Claudio
professore associato di diritto pubblico comparato, Università degli studi di Milano Bicocca
Martines, Francesco
ricercatore di diritto amministrativo, Università degli studi di Messina
Masseno, Manuel David
professor adjunto do IPBeja, Instituto Politécnico de Beja
Melzi d'Eril, Carlo
avvocato in Milano
Ninni, Laura
dottoranda di ricerca in studi sulla criminalità organizzata, Università degli studi di Milano

Orofino, Marco
professore associato di diritto costituzionale, Università degli studi di Milano
Paruzzo, Francesca
dottoressa di ricerca in diritto costituzionale, Università degli studi di Torino
Peron, Sabrina
avvocato in Milano
Pezza, Federica
IP Junior Associate
Pollicino, Oreste
professore ordinario di diritto costituzionale, Università Commerciale "L. Bocconi"
Ranghino, Andrea
avvocato in Milano
Riccio, Giovanni Maria
professore associato di diritto privato comparato, Università degli studi di Salerno
Ruggeri, Antonio
professore ordinario di diritto costituzionale, Università degli studi di Messina
Santos, Cristiana
Institute of Law and Technology, UAB. Law Science
Seminara, Sergio
professore ordinario di diritto penale, Università degli studi di Pavia
Trevisi, Cecilia
avvocato in Milano
Urso, Egle
LL.M. Candidate, Law of Internet Technology, Università Commerciale "L. Bocconi"
Vesto, Aurora
ricercatrice in diritto privato, Università per stranieri "Dante Alighieri" di Reggio Calabria
Vigevani, Giulio Enea
professore associato di diritto costituzionale, Università degli studi di Milano Bicocca
Vimercati, Silvia
dottoranda di ricerca in scienze giuridiche, Università degli studi di Milano Bicocca
Visco Comandini, Vincenzo
docente a contratto di economia politica, Università di Roma Tor Vergata
Zeno Zencovich, Vincenzo
professore ordinario di diritto privato comparato, Università degli studi Roma Tre

CODICE ETICO

La **Rivista di diritto dei media** intende garantire la qualità dei contributi scientifici ivi pubblicati. A questo scopo, la direzione, il Comitato degli esperti per la valutazione e gli autori devono agire nel rispetto degli standard internazionali editoriali di carattere etico.

Autori: in sede di invio di un contributo, gli autori sono tenuti a fornire ogni informazione richiesta in base alla policy relativa alle submissions. Fornire informazioni fraudolente o dolosamente false o inesatte costituisce un comportamento contrario a etica. Gli autori garantiscono che i contributi costituiscono interamente opere originali, dando adeguatamente conto dei casi in cui il lavoro o i lavori di terzi sia/siano stati utilizzati. Qualsiasi forma di plagio deve ritenersi inaccettabile. Costituisce parimenti una condotta contraria a etica, oltre che una violazione della policy relativa alle submission, l'invio concomitante dello stesso manoscritto ad altre riviste. Eventuali co-autori devono essere al corrente della submission e approvare la versione finale del contributo prima della sua pubblicazione. Le rassegne di dottrina e giurisprudenza devono dare esaustivamente e accuratamente conto dello stato dell'arte.

Direzione: la direzione (ivi compresi direttori e vice-direttori) si impegna a effettuare la selezione dei contributi esclusivamente in base al relativo valore scientifico. I membri della direzione (ivi compresi direttori e vice-direttori) non potranno fare uso di alcuna delle informazioni acquisite per effetto del loro ruolo in assenza di un'esplicita autorizzazione da parte dell'autore o degli autori. La direzione è tenuta ad attivarsi prontamente nel caso qualsiasi questione etica sia portata alla sua attenzione o emerga in relazione a un contributo inviato per la valutazione ovvero pubblicato.

Comitato degli esperti della valutazione: i contributi sottoposti a valutazione costituiscono documentazione a carattere confidenziale per l'intera durata del processo. Le informazioni o idee acquisite confidenzialmente dai valutatori per effetto del processo di revisione non possono pertanto essere utilizzate per conseguire un vantaggio personale. Le valutazioni devono essere effettuate con profondità di analisi, fornendo commenti e suggerimenti che consentano agli autori di migliorare la qualità delle loro ricerche e dei rispettivi contributi. I revisori dovranno astenersi dal prendere in carico la valutazione di contributi relativi ad argomenti o questioni con i quali sono privi di familiarità e dovranno rispettare la tempistica del processo di valutazione. I revisori dovranno informare la direzione ed evitare di procedere alla valutazione nel caso di conflitto di interessi, derivante per esempio dall'esistenza di perduranti rapporti professionali con l'autore o la relativa istituzione accademica di affiliazione.

media LAWS

ANNO 2018 - CODICE ISSN 2532-9146