mediaLAWS

Rivista di diritto dei media
1/2023 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)
Marina Castellaneta (Università di Bari)
Marco Bassini (Tilburg University)

VICEDIRETTORI
VICE-EDITORS
Marco Cuniberti (Università di Milano)
Giovanni Maria Riccio (Università di Salerno)
Marco Orofino (Università di Milano)
Ernesto Apa (Avvocato in Roma)

REDAZIONE
EDITORIAL BOARD
Marco Bassini (*coordinatore*) (Tilburg University)
Flavia Bavetta (*vice coordinatore*) (Università Bocconi)
Redazione di Bari
Teresa Catalano, Giuseppe Gallo, Stefania Rutigliano
Redazione di Milano-Bicocca
Maria Galbusera, Giacomo Mingardo, Giulia Napoli
Redazione di Milano-Bocconi
Pietro Dunn, Giuseppe Muto, Federica Paolucci

SEDE
CONTACTS
ACCMS Studio Legale
Via Podgora 13 – 20122 Milano

Università Bocconi - Dipartimento di Studi Giuridici
Via Roentgen 1 - 20136 Milano
e-mail: submissions@medialaws.eu

COMITATO SCIENTIFICO- STEERING COMMITTEE

Shulamit Almog *(University of Haifa),* Fabio Basile *(Università di Milano),* Mirzia Bianca *(La Sapienza – Università di Roma),* Elda Brogi *(European University Institute),* Giuseppe Busia *(Autorità Nazionale Anticorruzione),* Licia Califano *(Università di Urbino, già Garante per la protezione dei dati personali),* Angelo Marcello Cardani *(Università Bocconi, già Autorità per le garazie nelle comunicazioni),* Marta Cartabia *(Università Bocconi, Presidente emerito della Corte costituzionale),* Massimo Ceresa-Gastaldo *(Università Bocconi),* Pasquale Costanzo *(Università di Genova),* Marilisa D'Amico *(Università di Milano),* Filippo Donati *(Consiglio Superiore della Magistratura),* Mario Esposito *(Università del Salento),* Giusella Finocchiaro *(Università di Bologna)*, Tommaso Edoardo Frosini *(Università Suor Orsola Benincasa),* Maurizio Fumo *(Suprema Corte di Cassazione),* Alberto Maria Gambino *(Università Europea – Roma),* Michale 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),* Simone Lonati *(Università Bocconi),* Fiona Macmillan *(University of London),* Vittorio Manes *(Università di Bologna),* Michela Manetti *(Università di Siena),* Christopher Mardsen *(University of Sussex),* Manuel D. Masseno *(Instituto Politécnico de Beja),* Roberto Mastroianni *(Tribunale UE),* Luigi Montuori *(Garante per la protezione dei dati personali),* Antonio Nicita *(LUMSA, già Autorità per le garanzie nelle comunicazioni),* Monica Palmirani *(Università di Bologna)*, Miquel Pequera *(Universitat Oberta de Catalunya),* Vincenzo Pezzella *(Suprema Corte di Cassazione),* Laura Pineschi *(Università di Parma),* Giovanni Pitruzzella *(Corte di giustizia UE),* Francesco Pizzetti *(Università di Torino),* Andrea Pugiotto *(Università di Ferrara),* Margherita Ramajoli *(Università di Milano),* Gianpaolo Maria Ruotolo *(Università di Foggia),* Sergio Seminara *(Università di Pavia),* Salvatore Sica *(Consiglio di Presidenza della Giustizia Amministrativa),* Pietro Sirena *(Università Bocconi),* Francesco Viganò *(Corte costituzionale),* Luciano Violante *(Fondazione Leonardo - Civiltà delle Macchine)*, Lorenza Violini *(Università di Milano),* Roberto Zaccaria *(Università di Firenze),* Nicolò Zanon *(Corte costituzionale),* Vincenzo Zeno-Zencovich *(Università di Roma Tre)*

COMITATO DEGLI ESPERTI PER LA VALUTAZIONE - ADVISORY BOARD

Maria Romana Allegri, Giulio Allevato, Benedetta Barbisan, Marco Bellezza, Daniela Bifulco, Elena Bindi, Carlo Blengino, Monica Bonini, Manfredi Bontempelli, Fernando Bruno, Daniele Butturini, Irene Calboli, Simone Calzolaio, Quirino Camerlengo, Gianluca Campus, Nicola Canzian, Marina Caporale, Andrea Cardone, Corrado Caruso, Stefano Catalano, Adolfo Ceretti, Francesco Clementi, Roberto Cornelli, Giovanna Corrias Lucente, Filippo Danovi, Monica Delsignore, Giovanni De Gregorio, Giovanna De Minico, Gabriele Della Morte, Marius Dragomir, Fernanda Faini, Fabio Ferrari, Roberto Flor, Federico Furlan, Giovanni Battista Gallus, Marco Gambaro, Gianluca Gardini, Ottavio Grandinetti, Antonino Gullo, Erik Longo, Valerio Lubello, Federico Lubian, Nicola Lupo, Paola Marsocci, Claudio Martinelli, Alberto Mattiacci, Alessandro Melchionda, Massimiliano Mezzanotte, Francesco Paolo Micozzi, Donatella Morana, Piergiuseppe Otranto, Omar Makimov Pallotta, Anna Papa, Paolo Passaglia, Irene Pellizzone, Sabrina Peron, Bilyana Petkova, Davide Petrini, Marina Pietrangelo, Federico Gustavo Pizzetti, Augusto Preta, Giorgio Resta, Francesca Rosa, Andrej Savin, Salvatore Scuto, Monica Alessia Senor, Stefania Stefanelli, Giulia Tiberi, Bruno Tonoletti, Emilio Tosi, Lara Trucco, Luca Vanoni, Gianluca Varraso, Silvia Vimercati, Thomas Wischmeyer, Paolo Zicchittu

ANNO 2023 - 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 (rivista.medialaws.eu). 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 comparata"), "Cronache e commenti" 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 e commenti" 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.

Indice
Index

Editoriale

11 The EU regulation of speech. A critical view
Vincenzo Zeno-Zencovich

Saggi

20 Il metaverso tra problemi epistemologici, etici e giuridici
Ginevra Cerrina Feroni

35 L'art. 2 della Costituzione e il "Metaverso"
Luca Di Majo

66 Libertà d'impresa e diritto alla protezione dei dati personali
Raffaele Torino

86 European Collective Redress and Data Protection Challenges and Opportunities
Marina Federico

104 Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo
Andrea Vigorito

128 Le modifiche e l'aggiornamento del contenuto digitale e dei servizi digitali nella disciplina di attuazione delle direttive (UE) 770 e 771 del 2019
Giovanna Capilli

150 Contrastare l'astensionismo e favorire la partecipazione: il voto elettronico basato sulle tecnologie *Blockchain* e *Distributed Ledger*
Marco Ladu

170 Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai *deepfakes*
Martina Cazzaniga

188 Trasformazione digitale del settore finanziario e *Open Finance*: quali prospettive per un credito "sostenibile"? Prime riflessioni
Maria-Teresa Paracampo

207 Dalla Decisione per il rafforzamento della protezione delle informazioni su internet alla Legge sulla tutela delle informazioni personali della RPC "con caratteristiche cinesi"
Enrico Toti

Note a sentenza

252 Le azioni collettive tra *data protection* e tutela consumeristica al vaglio della Corte di giustizia
Lavinia Vizzoni

267 Diritto alla deindicizzazione e notizie false: la Corte di giustizia precisa i confini tra oblio e libertà di espressione
Giulia Napoli

282 Sul diritto all'oblio e obblighi di deindicizzazione globale
Sabrina Peron

291 Il contrasto europeo alla disinformazione nel contesto della guerra in Ucraina: riflessioni a margine del caso *RT France*
Pietro Dunn

302 La Corte costituzionale dichiara l'illegittimità costituzionale del divieto, imponibile dal Questore, di possedere ed utilizzare il telefono mobile e riapre il dibattito sulle misure di prevenzione personali
Davide Galliani e Marco Orofino

326 Algoritmo, provvedimento amministrativo e autotutela
Armando Lorusso

Cronache

343 The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations
Elena Kaiser

358 La tutela dei minori nel cyberspazio. Parental Control di Stato e libera circolazione dei contenuti: un delicato equilibrio
Nicolò Biligotti

366 Pubblicità tradizionale e *digital advertising*: profili di valutazione economica
Roberto Moro-Visconti

Indice
Index

Editorial

11 The EU regulation of speech. A critical view
Vincenzo Zeno-Zencovich

Essays

20 The metaverse: philosophical, ethical and legal dilemmas
Ginevra Cerrina Feroni

35 Art. 2 of the Italian Constitution and "Metaverse"
Luca Di Majo

66 Freedom to conduct business and protection of personal data
Raffaele Torino

86 European Collective Redress and Data Protection Challenges and Opportunities
Marina Federico

104 On the edge between data altruism and social scoring: practical applications of the data-algorithm pattern within the new European regulatory context.
Andrea Vigorito

128 The Italian transposition of EU directives no. 770/2019 and 771/2019 on the modifications and update of digital content and services
Giovanna Capilli

150 Against abstentionism, supporting voters' participation: e-voting and the use of the Blockchain technology and Distributed Ledger
Marco Ladu

170 A new technique (also) to convey disinformation: the European approach to deepfakes
Martina Cazzaniga

188 Digital transformation of the financial sector and Open Finance: what prospects for 'sustainable' credit? First thoughts
Maria-Teresa Paracampo

207 From the Resolution to strengthen the protection of information on the internet to the Personal information protection law with "Chinese charateristcs"
Enrico Toti

Case notes

252 European Court of Justice ruling on collective redress, data protection and consumer protection
Lavinia Vizzoni

266 Right to delisting and fake news: the European Court of Justice on the balance between right to be forgotten and freedom of expression
Giulia Napoli

281 On the right to be forgotten and global de-indexing obligations
Sabrina Peron

290 The European strategy against disinformation in the context of the war in Ukraine: a comment to the *RT France* decision
Pietro Dunn

301 Italian Constitutional Court invalidates the administrative ban on the possession and use of mobile phones and reopens debate on precautionary measures
Davide Galliani e Marco Orofino

325 Algorithmic administrative decision and its withdrawal
Armando Lorusso

Comments

342 The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations
Elena Kaiser

357 The protection of minors in cyberspace. Parental control and free speech: a delicate balance
Nicolò Biligotti

368 Traditional versus digital advertising: an economic evaluation
Roberto Moro-Visconti

Sono stati sottoposti a referaggio anonimo a doppio cieco i saggi di Ginevra Cerrina Feroni, Giovanna Capilli, Martina Cazzaniga, Luca Di Majo, Marina Federico, Marco Ladu, Maria-Teresa Paracampo, Raffaele Torino, Enrico Toti, Andrea Vigorito. Su determinazione della Direzione, ai sensi dell'art. 15 del Regolamento, sono stati altresì sottoposti a referaggio anonimo i contributi di Pietro Dunn, Giulia Napoli, Lavinia Vizzoni, Nicolò Biligotti ed Elena Kaiser.

Editoriale

The EU regulation of speech. A critical view

Vincenzo Zeno-Zencovich

Abstract

The article challenges a series of recent acts, proposals and decisions by EU institutions which progressively limit freedom of speech by individuals, entrusting it to the algorithmic regulation of online platforms and to self-proclaimed guardians of a safe Internet.

Summary

1. Introduction. – 2. The "Digital Services Act". – 3. The "Strengthened Code of Practice on Disinformation". – 4. The "European Media Freedom Act". – 5. The "*Russia Today*" decision. – 6. A few conclusions

Keywords

freedom of speech – content regulation – online platforms – Digital Services Act – disinformation

1. Introduction

As the Latin saying goes, "*mala tempora currunt*" for freedom of expression in the European Union.

And "bad times" are really running (and not simply walking) if one looks at the sequence and timing of a series of acts and documents issued in the last year by the EU:

a) the Digital Services Act (Regulation (EU) 2022/2065 issued in October 2022);
b) the "Strengthened Code of Practice on Disinformation 2022" (published in June 2022);
c) the proposal for a Regulation called the "European Media Freedom Act" presented in September 2022;
d) the decision by EU Tribunal July 27,2022 in the T-125/22 Case (*Russia Today France v. Commission*).

In these few pages I wish to point out that the EU institutions, both at their executive and judicial level, have a deformed notion of what freedom of expression is and what are its functions in a democratic society. In a nutshell, expression is seen not as a freedom – in the sense we have forged this notion over the centuries, and in particular over the last two centuries – but a regulated activity, similar to the production of

goods or the provision of services. This view is repugnant to the European liberal tradition and as a result will increase even more the cleavage between the EU as a whole and its citizens it should – and must – represent[1].
I will try to present my arguments combing through the four texts I have mentioned before, referring also to previous EU normative materials.

2. The "Digital Services Act"

Regulation (EU) 2022/2065 on a "Single Market for Digital Services", commonly called "Digital Service Act" (DSA) replaces the, by now, obsolete directive 2000/31/EC.
The DSA however does not limit itself to regulate the activities that are conducted in a digital environment through public telecommunication networks, but disciplines in depth speech through these networks.
The novel four letter words that are targeted are "hate" [speech] and "fake" [news] which must be banned. The declared objective is that of «ensuring a safe, predictable and trustworthy online environment» by adopting a broad notion of illegal content (Recital 12).
Normative provisions on "hate speech" have been issued over the last years by EU institutions, generally through a "fruit salad" approach which puts together terrorism, child pornography, copyright infringement, deceitful consumer information and «illegal hate speech» (see *e.g.* the Commission Recommendation 2018/334 "on measures to tackle illegal content online").
The first striking feature is putting within the same framework («illegal content») completely different phenomena from a political, economic and social point of view. In a non-digital environment copyright infringement is countered by copyright laws; unfair commercial practices by consumer protection laws; terrorist promotion and abetting and child pornography by provisions in penal codes.
One can legitimately doubt the wisdom of clustering such different conducts simply because they are all put into place through the Internet.
However, the most troubling aspect is the repeated – throughout the DSA and other EU legal instruments – expression «illegal hate speech». Although an experienced lawyer has been trained to face fuzzy EU legal notions, here the ambiguity of the terms is astounding.
In the first place because speaking of «illegal hate speech», makes one think that there are forms of "hate speech" which are "legal". But paramount to this basic logical distinction, the notion of "hate speech" is a portmanteau expression that can be filled with any content: from verbal aggression towards an ethnical or religious group; to the frequent banners or choruses one sees or hears at the football stadium addressed towards the other team and its supporters; the political party or movement one despises;

[1] For similar criticisms see A. Koltay, *Freedom of expression and the regulation of disinformation in the European Union*, Discussion paper for the 2023 Free Speech Discussion Forum - University of Luxembourg - June 2023 (forthcoming)

and the list could be endless.

Not only the notion of "hate speech" is without a reasonably clear definition[2], but a lawyer should react strongly against the attempt to import in the legal arena – in which each word has, and must have, one and only one meaning – terminology picked up from social and press jargon. And the attempt to norm "hate" – an inherent psychological state – appears as fruitless as the attempt to norm its opposite "love". To express the idea with a literary expression, most often "hate" is "in the eyes of the beholder", rather than in the words or acts themselves. An individual or a group vocally complains that it is being "hated", and this self-proclamation is sufficient to ban the speech and shame the author.

All these objections are brushed aways by the DSA through a simple *jeu-de-mots*. What needs to be countered is not "illegal" content but "harmful" content.

Any continental lawyer who has learnt – in his first-year courses – the basic notions of extracontractual obligations has very clear the distinction between "harmful" and "illegal". In the non-digital world, we encounter every minute millions of harmful acts which in no way can be legally prevented or sanctioned because they do not violate some law or regulation or another person's rights. On the Internet, instead, speech must be curtailed because it is «illegal or otherwise harmful» (recital 68) and it is necessary to prevent the «spread of unlawful or otherwise harmful information» (recital 5).

The equalizing – from an effects point of view – of "illegal" and "harmful" not only demolishes basic legal principles (which have never been very much considered in the EU functionalist approach: norms are simply tools *bons-à-tout-faire* to reach a purpose) but entails immediate and vast reaching consequences on speech.

This is because the DSA – faced with the impossibility of monitoring «illegal or otherwise harmful» speech – has outsourced its control and contrast to "Internet intermediary providers" and to the "very large online platforms".

The first technique adopted is that of establishing a principle, but subsequently emptying it through an exception. Art. 6 of DSA – following the E-Commerce Directive of 2000 – states that an information society service provider is not liable for information stored provided that it «does not have actual knowledge of illegal content» and «is not aware of facts or circumstances from which the illegal content is apparent».

This principle is strengthened by the confirmation of the e-commerce rule that providers of intermediary services are not under an obligation to monitor or actively verify illegal content. However, these rules are set aside by the subsequent art. 16 which mimics the "notice and take-down" procedures common to online copyright infringement. When an individual or an entity notifies a provider of hosting services the presence of information that they «consider to be illegal content», such notices «shall be considered to give rise to actual knowledge or awareness» with the consequent loss of the immunity laid out in art. 6.

The shift of liability on internet providers is completed – in a radical way – towards what are qualified as «very large online platforms», which are easily identifiable in Google, Meta, Twitter, Instagram and Tik-Tok, at least for what concerns the dissemination of information and, more in general, speech.

[2] For the multiple notions see I. Spigno, *Discorsi d'odio: modelli costituzionali a confronto*, Milan, 2018.

To make short the very long normative provision contained in arts. 34, 35 and 36, the «very large online platforms» will have to put into place – and more than a legal obligation it is economically based decision – algorithmic systems which will prevent *ab initio* «the dissemination of illegal content through their services».

One has already experimented the results – often ludicrous – of such algorithmic screening that have erased from the Internet breast-feeding Madonnas, putti, paintings and sculptures of Venus, towns and people whose name fell into the politically incorrect primitive vocabulary of Facebook. And the frequent suspension of email or other personal communication services through the detection of messages and photographs which the algorithm considers inappropriate.

The «very large online platforms» are therefore entrusted with a policing role that public authorities are not able to perform. In substance, a fundamental right such as that of expression that in our technological environment can be put into practice only through the Internet and intermediary services and platforms will be subject to algorithmic preventive censorship[3].

But the DSA does not limit itself to vesting «very large online platforms» with such public roles – which in most European Constitution are under a double – legal and judicial – reserve, but adds to them what one could call – using a Wild West expression – a "private posse", to ensure compliance with the Regulation and its contrast to «illegal or otherwise harmful» content.

With this objective the DSA creates the figure of «trusted flaggers».

Again, there is no definition of such completely novel entity apart from the fact that it should have «particular expertise and competence for the purpose of detecting. identifying and notifying illegal content» (art. 22, para. 2, a).

The objective of the creation of such semi-public entities (because the status is conferred by the national "Digital Services Coordinator") is that «action against illegal content can be taken more quickly and reliably where providers of online platform take the necessary measures to ensure that notices submitted by trusted flaggers […] are treated with priority» (recital 61).

If one considers the freezing effects of art. 16 which has been previously mentioned, it is reasonable to expect that the "notice and take-down" requests presented by such «trusted flaggers» shall be automatically processed.

Again, the Regulation puts together extremely different phenomena: terrorist content, child pornography, «illegal racist and xenophobic expressions». But if one extends the scope to the vast area of «discriminatory speech» – which falls within the «otherwise harmful» category – one can already see the multitude of organizations which, purporting the defense of minoritarian groups, ask for the removal of speech or other forms of expression which they consider offensive. It is sufficient to look at the aggressive campaigns conducted under the flags of trans-Atlantic movements ("Me-Too", "Cancel Culture", "Black Lives Matter", "Last Generation", LBGT+whatever, etc.) to understand what the effects of such private internet militia can be on freedom

[3] The point is thoroughly examined and challenged by G.E. Vigevani, *Piattaforme digitali private, potere pubblico e libertà di espressione*, in *Rivista di diritto costituzionale*, 61(1), 2023, 41 ss.

of expression[4].

3. The "Strengthened Code of Practice on Disinformation"

The second four-letter word targeted by the EU institutions is "fake" news. Again, the EU transfers in the legal vocabulary journalistic jargon which is completely undetermined. When it comes to news the ample case-law uses precise parameters such as the falsity or the partiality of a news, or its unsubstantiated source. At any rate such news is sanctioned if it violates somebody's right (typically, reputation).
The EU's attempt is, instead, all encompassing: news, just as the environment or a drug, must comply with certain requirements normatively set.
The perspective does not change if one uses the more educated term of "disinformation", which is the object of innumerous EU interventions since 2016[5].
In this case, however, there is an attempt to define what "disinformation" is: «Disinformation is understood as verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens' health[6], the environment or security».
It should be noted that the "Strengthened Code of Practice on Disinformation 2022", although substantially drafted under the supervision of the EU Commission is presented as a text which is attributed to the Signatories and to which they voluntarily agree. A voluntary acceptance which reminds of the often-quoted phrase from "The Godfather": «An offer which one cannot refuse».
Most of the Code concerns practices put into place in commercial advertising and in clearly deceptive practices, such as fake accounts, impersonation, BOT amplification, use of influencers.
However, the forty pages Code inevitably spills over in the field of individual speech, in particular in the case in which an individual or a group of individuals advocate unconventional ideas which clash with majoritarian views. The bottom line is the question on what content «may cause public harm».

---

[4] Obviously there are authors who, quite at the opposite, welcome the DSA for imposing on the "very large platforms" the respect of fundamental rights. This would enhance speech by "minority and marginalized groups" (J. P. Quintais - N. Appelman - R. Fahy, *Using Terms and Conditions to Apply Fundamental Rights to Content Moderation,* in *German Law Journal,* 24, 2023).

[5] See The Communication by the Commission "Tackling online disinformation: a European Approach" (COM 2018/236); the Joint Communication of the Commission and the High Representative "Action Plan against Disinformation" (Join 2018-36) and the ERGA 2019 "Report on Disinformation: Assessment of the Implementation of the Code of Practice". All these texts are amply commented by G. Pitruzzella - O. Pollicino, *Disinformation and Hate Speech. A European Constitutional Perspective*, Milan, 2020.

[6] During the COVID-19 pandemic the dissemination of misleading information has been of general concern on both sides of the Atlantic, albeit with diverging decisions. See the cases decided by the Italian Telecommunications Authority and administrative tribunal, and by the FCC published in *Diritto dell'informazione e dell'informatica,* 2020, 520 ss., with a critical comment by V. Zeno-Zencovich, *La disciplina della comunicazione in base al suo contenuto. Una proposta di inquadramento sistematico.*

Clearly this hypothetical question to some, limited, degree can find an answer when one is faced with a product or a material activity, but it is practically impossible (with maybe a few exceptions, such as financial markets) to predict the adverse consequences of news, information or ideas.
The problem is that this uncertainty is resolved by entrusting the "verification" of the content to a self-proclaimed «fact-checking community» which, incidentally, should be financed by the providers of intermediary online information-services.
To sum all this up, the dissemination by individuals of content through the Internet is once again subject to scrutiny and censorship by private groups. One must insist on the fact that speech is not a consumer product whose functionality can be ascertained. And while control over a product is aimed at protecting health and wealth of consumers and promoting competition, regulation of speech encroaches a fundamental right. Further, one should add that the fact-checking militia which is "empowered" by the Code adds itself to the "*trusted flaggers*" instated by the DSA.

4. The "European Media Freedom Act"

The summit of Commission's invasion of the field of freedom of expression is represented by its proposal for a regulation «establishing a common framework for media services in the internal services», laudatorily called the "European Media Freedom Act".
From an institutional point of view, one witnesses how the Commission subverts the subsidiarity exception set in art. 5 of the Treaty, turning it in a *carte blanche* to regulate areas that in no way are of the competence of the EU.
To be even more clear, the fact that the EU Charter on Fundamental Rights affirms at its art. 11 the fundamental right of freedom of expression cannot be read in the sense that it implies the right of the Commission to regulate such freedom[7].
While it is obvious that the European tradition has never been that of the First Amendment to the US Constitution ("Congress shall make no law abridging freedom of speech, or of the Press") and has always pointed in a different direction (suffice it to mention the contemporary art. 11 of the French Declaration of the Rights of Men and Citizens), the proposed regulation goes well beyond.
The proposal aims at creating a "European Board for Media Services" which replaces the Regulators Group (ERGA) established by the AudioVisual Media Services Directive (2010/13/EU) and extends its control to the press. Following a common tendency, the Board is a centralized body under the substantial and formal control of the Commission. Although the proposal proclaims the "independence" of the Board from any institution or body, when one goes through the text one finds multiples cases in which the Board can act only if "in agreement" with the Commission.
Further, the Commission shall define "Key performance indicators" to measure the compliance of the European media services to the regulation and set Guidelines.

[7] In the contrary sense, see G. Muto, *European Media Freedom Act: la tutela europea della libertà dei media*, in *Rivista di diritto dei media,* 3, 2022, 209 ss. (at 225).

Member States will have to submit to the Commission "*any legislative, regulatory or administrative measure*" in the field of media services providers.
It is clear that media companies are businesses like any other business and therefore are aiming at making a profit. Therefore they should not be granted any privilege – such as the mystifying appellative of "watch-dogs" – but, at the same time, in an age in which every communication has an informational content, the intention of regulating "media services providers" is simply a way of extending – completely *ultra vires* – the competences of the Commission, which at the end of the day, would be the final decision maker in all events concerning this vital sector.

5. The "*Russia Today*" decision

Following the Russian invasion of Ukraine, the EU has adopted a number of sanctions against Russia, its enterprises and several prominent officials and businessmen. These measures were coupled with significant embargoes of Russian products and services.
Among these measures is decision 2022/350 of the EU Council which has prohibited the broadcast and the dissemination of programs by Russian controlled media outlets present in Europe ("Russia Today" in its English, French, German, Spanish versions, and "Sputnik").
The activities of these outlets are qualified as «hybrid threats» to the Union and its member States under the form of «disinformation», «systematic, intentional campaigns of media manipulation and distortion of facts to enhance [the Russian] strategy of destabilization» «targeted at civil society in the Union». This activity «constitutes a significant and direct threat to the Union's public order and security».
The Regulation was challenged by "Russia Today France" in front of the EU General Court which in a lengthy decision by the Grand Chamber (27 July 2022, in case T 125/22) rejected the claim and confirmed the Regulation.
One hundred of the 250 paragraphs of the decision are devoted to the question raised by RT France of the infringement of freedom of expression and information.
According to the Tribunal the activities of RT France constitute «propaganda actions against the Union and its Member States» which «are capable of undermining the foundations of democratic societies and are an integral part of the arsenal of modern warfare».
The Tribunal further enters in a textual analysis of several broadcasts by RT France, concluding that they were not "balanced" and therefore would have produced «a significant harmful effect on public opinion in the EU, by its operations involving manipulation and hostile influence».
One does not wish to enter into further details of the decision (which has been appealed in front of the Court of Justice)[8]. However, one cannot avoid noting that the decision is argued as if there were a war between the EU and Russia.
The point one wishes to make is different. The decision instead of being founded sim-

[8] For a broader critical comment see S. Sassi, *La soft war dell'Unione Europea: il caso RT-France vs. Consiglio*, in *Diritto dell'informazione e dell'informatica,* 2022, 1265 ss.

ply on the application of art. 20 of New York Covenant on Civil and Political Rights which States that «any propaganda for war shall be prohibited by law» (to which the decision devotes only three paragraphs, from 208 to 210) sets out an impressive array of *rationes decidendi* which will inevitably constitute a precedent in the future in completely different cases.

In particular, the fuzzy notions of «propaganda», «manipulation», «harmful effects», the lack of «balance» can be easily applied in other circumstances, completely different from the Russian aggression of Ukraine. Doing so the Tribunal has paved the way to further significant restrictions of public speech by the EU institutions.

6. A few conclusions

We live totally immersed in information societies, and every minute of our lives we produce and consume information. This is possible because of the existence of telecommunication networks and of the thousands of enterprises that operate on it. Over 25 years ago the US Supreme Court in its landmark decision *Reno v. ACLU* [9] quoted approvingly the statement made by District Judge Dalzell: Internet is «the most participatory form of mass speech yet developed».

In this eco-system there are surely actual and clear risks and dangers, such as our modern societies faced when electricity became the energy for everybody, when railways, motorcars, and aircrafts allowed forms of large-scale transportation, when the whole economy shifted from self-production and self-subsistence to consumerism.

Being aware of such risks and dangers, however, does not vouchsafe responses that, in the present case, impinge on freedom of thought and of expression.

The texts one has analysed in the previous pages present a common intellectual flaw *viz.* the idea that risks and dangers of the information society can be prevented, curbed and eventually repressed, through the authority of the law.

But as it is impossible to control the immense information eco-system by human activity, the only way to enforce the mastodontic legislation issued is by resorting to automated processes governed by Al, which notoriously does not operate on a case-by-case basis but via inferential logic, which is completely insensitive towards diversity.

And freedom of expression by individuals is – in our democratic societies – a question of diversity which cannot, and should not, be curtailed by majoritarian opinions on what is good and what is bad (in the EU words "harmful") for our minds, our feelings, our intellectual well-being.

[9] 521 U.S. 844 (1997).

Saggi

Il metaverso tra problemi epistemologici, etici e giuridici*

Ginevra Cerrina Feroni

Abstract

Metaverso è un termine utilizzato per descrivere uno spazio virtuale collettivo condiviso, creato dalla convergenza di una realtà virtuale immersiva e di una realtà fisica migliorata virtualmente. Le prospettive di applicazione e di sviluppo di tale realtà sono enormi e in massima parte, ad oggi, non prevedibili. Ciononostante è possibile e necessario interrogarsi, con le categorie filosofiche e giuridiche attuali, sulla natura e il significato di questo spazio, sulle relazioni tra i soggetti che ne fanno parte o che lo controllano e, infine, su alcune fondamentali implicazioni per la tutela dei dati personali.

It is known that new technologies affect not only private life, but also have a vast influence on people's status and orientations and, thus, on their constitutional freedoms. Talking about the metaverse means taking a step even forward: functions and structure of this digital "mundus novus" are still unclear. Nevertheless, the present article aims to investigate the potential legal issues in the metaverse, with a focus on the ones of public nature: from the redesigned relations between the actors (Nation-states, platforms and citizen-users) to the alteration/adaptation of the users' rights and freedoms.

Sommario

1. *La vida es*… metaverso. - 2. La natura di un *luogo* "sintetico". - 3. Le funzioni e le prospettive d'indagine del metaverso. - 4. Diritti fondamentali e possibili criticità nella protezione dei dati personali. - 5. Un problema di *governance*: il "medioeverso" come ordinamento giuridico neo-feudale?. - 5. Un tentativo di conclusione tra seduzioni, rischi e opportunità

Keywords

metaverso - privacy - diritti fondamentali - piattaforme – regolazione

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1. *La vida es...* metaverso

L'idea della realtà come simulazione è antica e allo stesso tempo rappresenta una scoperta recentissima. Che il nostro mondo e tutto ciò che esso contiene sia illusione è stato ampiamente affrontato dalla letteratura e, prima ancora, dal mito:

- per Platone la maggior parte degli uomini vivono nell'illusione di considerare le ombre delle cose le cose stesse[1];
- per Pedro Calderon de la Barca la vita è sogno[2];
- per le Upanishadas è lo stesso processo cosmico ad essere il sogno di un Dio e per il Buddismo viviamo in un universo illusorio creato da una forza magica di nome Maya[3]. L'intuizione fondamentale fu poi ripresa da una parte della filosofia occidentale ottocentesca, come ad esempio Arthur Schopenhauer, secondo il quale il mondo che ci circonda esiste solo come rappresentazione[4].

La possibilità di accedere materialmente a "realtà virtuali" create dalla nostra mente, a mondi illusori in cui l'operatore-osservatore si trasforma in attore, è un'ipotesi che anche la filosofia della scienza ha iniziato a indagare verso l'inizio degli anni '80 del Novecento[5], anche in forza di riflessioni preparatorie forniteci da scienziati come Konrad Zuse, che fece notare la corrispondenza tra la realtà fisica e il computer (in particolare tra il comportamento delle particelle digitali, dei *bit* e quello delle particelle subatomiche) giustificando, più in generale, la progressiva coincidenza tra la teoria dell'informazione e quella della fisica[6].

Alla base di queste riflessioni c'è dunque l'idea che la realtà non sia totalmente obiettiva e che i nostri cervelli siano in realtà degli enormi simulatori. La conferma scientifica

---

* Il presente contributo è destinato, in versione ridotta, al *Liber Amicorum* per Guerino D'Ignazio.

[1] È G. Salmeri, *Il metaverso come la caverna di Platone? Il vero mondo è altrove*, in *agendadigitale.it,* 20 gennaio 2022, ad aver notato un'analogia tra il progetto del metaverso e la caverna di Platone, non per considerare l'esperimento un passo ulteriore verso l'annebbiamento del senso della realtà (come molti affermano), ma per sostenere che noi ci troviamo già ora in un mondo illusorio come gli uomini incatenati nella caverna, mentre il digitale rappresenta solo uno *medium*, un catalizzatore del rapporto con il sé, con gli altri e con il mondo.

[2] P. Calderón de la Barca, *La vida es sueño* (1635).

[3] J.L. Borges, *Cos'è il buddismo*, Roma, 1995, ricorda che nel nichilismo buddista dietro il sogno e sotto il sogno non c'è nulla se non il Nirvana che, però, rappresenta anch'esso un mondo senza coscienza.

[4] A. Schopenhauer, *Il mondo come volontà e rappresentazione* (*Die Welt als Wille und Vorstellung*), Leipzig, 1819.

[5] Si pensi a T. Maldonado, *Reale e virtuale*, Milano, 1992, che iniziò a studiare la virtualità nel contesto del sistema delle rappresentazioni visive della nostra civiltà a partire dalle sue radici storiche, facendo confluire molteplici contributi disciplinari, dalla filosofia della scienza, alla storia dei mezzi di comunicazione fino alle scienze cognitive.

[6] K. Zuse, *The Computing Universe,* in *International Journal of Theoretical Physics,* 21(6-7), June, 1982, 589 ss. e, successivamente, E. Fredkin, *Digital Mechanics: An Informational Process Based on Reversible Universal Cellular Automata*, in *Physica*, 45, 1990, 254 ss., dalle cui riflessioni si ricava che l'informazione è il principio ultimo e definitivo della realtà, che il *bit* è il suo elemento costitutivo, l'*arché* immateriale alla sua base. Lo ricordano anche G.O. Longo - A. Vaccaro, *La nascita della filosofia digitale*, in *Mondo Digitale*, luglio 2014, n. 4, che aggiungono: «Al termine del convegno [dove Zuse presentò la sua teoria] erano tutti molto più convinti che l'asserzione "il Cosmo è un Grande Computer" non fosse da intendere come una semplice metafora, bensì come un valido strumento euristico». Cfr., anche N. Negroponte, *Being Digital*, New York, 1995.

delle millenarie tradizioni spirituali e delle intuizioni dei fisici teorici come Zuse ci giunge solo assai recentemente: esperimenti neuro scientifici sono arrivati alla conclusione che la comprensione del mondo non è oggettiva e integrale, ma soggettiva e parziale: i nostri cervelli si stabilizzano su una frequenza della realtà ed escludono le altre[7], sublimano la realtà oggettiva e la filtrano attraverso i propri parametri. In breve, i nostri cervelli creano un metaverso in cui vivere.

Oggi il termine metaverso[8] è utilizzato per descrivere uno spazio virtuale collettivo condiviso, creato dalla convergenza di una realtà virtuale immersiva e di una realtà fisica migliorata virtualmente. Si tratta di una scelta lessicale felice, nella misura in cui la preposizione greca «dopo», «oltre», «al di là», si inserisce perfettamente nell'ottica di promuovere l'idea di un mondo parallelo, cioè di una metafisica del reale. Metaverso, dunque, come "meta-realtà", ma non nel senso di un al-di-là della materia, quanto di al-di-là del modo in cui la nostra mente, collegata al cervello, intende la materia.

Il concetto è assurto alla ribalta in riferimento ad una specifica operazione, prima di tutto commerciale, di Meta appunto. Ed è grazie a questa azienda – e al suo impressionante investimento economico – che il metaverso è diventato un argomento di studio. L'azienda statunitense è forse stata la prima a puntare sul metaverso come prospettiva alternativa plausibile, una visione della realtà virtuale immersiva integrata alla realtà fisica, aspirando a rendere il metaverso un "Internet incarnato"[9] o un "Internet a tre dimensioni", come è stato definito, cioè uno strumento parte della realtà quotidiana degli individui, delle pubbliche amministrazioni e delle aziende.

2. La natura di un *luogo* "sintetico"

Chiunque tratti il tema del metaverso non può preliminarmente fare a meno di notare quanto poco si sappia della sua strutturazione e, tanto meno, della sua possibile evoluzione, dello sviluppo delle sue infrastrutture tecnologiche e delle futuribili interazioni tra beni e transazioni digitali. Parlare del metaverso significa, insomma, procedere per lo più attraverso speculazioni e forse è proprio questo che rende il tema così affascinante, in particolare per chi si interessi di ingegneria giuridica e costituzionale.

Il punto di vista migliore per capire ciò che sta avvenendo è costituito da quelli che sono presentati come gli elementi fondamentali dei metaversi, di ciò che lo deve "costruire". Così, ancor prima di comprendere le funzioni di questo "*mundus novus*" digitale, è utile capire che cos'è, come si struttura.

---

[7] Una conferma ci deriva peraltro proprio dall'utilizzo dei *bias* cognitivi e dalle euristiche, ovvero quei costrutti mentali fondati su una comprensione pregiudiziale della realtà che, pur rischiando di indurci in errore, sono attributi che ci consentono di arrivare a conclusioni rapide e prendere delle scelte. Per una ricognizione dei vari studi che hanno permesso di arrivare a questa conclusione l'editoriale *"Reality" is constructed by your brain. Here's what that means, and why it matters*, pubblicato sul sito del Wu Tsai Neuroscience Institute della Standford University.

[8] Il termine, riportato *in auge* dall'operazione commerciale di Meta si riconduce al romanzo cyberpunk *Snow Crash* di Neil Stephenson uscito nel 1992.

[9] Mark Zuckerberg, durante la conferenza *Connect*, che ha avuto luogo in diretta streaming il 28 ottobre 2021, ma prima ancora in un'intervista su *theverge.com* del 22 luglio 2021 che così continua: «il Metaverso è un Internet dove i contenuti, invece di essere visualizzati, sono vissuti».

Per metaverso possono aversi due diversi significati distinti: da un lato, ci si può riferire all'interfaccia, cioè all'impalcatura strutturale governata da protocolli di sistema e da standard tecnici che garantiscono l'interazione tra le varie tecnologie, vale a dire la loro interoperabilità. Qualcosa di molto simile a quello che avviene oggi per l'*http* di Internet e per il browser di accesso al Web (www)[10]. Questa impalcatura strutturale, sviluppata e fornita nella maggior parte dei casi da tre principali aziende[11], rappresenta il supporto "neutro" di trasferimento, lo scheletro sul quale si può sviluppare il secondo significato di metaverso, ovvero le varie stanze, i vari mondi accessibili. All'interno di ogni stanza, di ogni metaverso, i rispettivi *provider*, come avviene ora per i *social* e le altre applicazioni, potranno gestire la propria realtà immersiva. Dunque, proprio come per Internet, anche nella realtà immersiva ci troviamo davanti tanto ad un metaverso-struttura (l'*http*) quanto a siti-metaversi.

Visivamente, può essere utile immaginare il metaverso come il *desktop* del nostro *smartphone*: una stanza in cui, a propria volta, ci sono delle *app*, degli spazi dove possiamo entrare. Sullo *smartphone* ogni *app* rappresenta un "metaverso bidimensionale", mentre sul metaverso queste *app* saranno tridimensionali, "abitabili".

Ad oggi il metaverso, sebbene in costante progresso, ci offre ancora una risposta decisamente povera in termini grafici e di esperienza immersiva: l'assenza di tre dei cinque sensi è (ancora) senza dubbio vistosa[12] e l'interconnessione tra il nostro sistema vestibolare, che produce il senso dell'equilibrio e la realtà virtuale è (ancora) da perfezionare, stante il senso di nausea e di malessere che può cogliere chi ne faccia esperienza per più di un certo tempo.

In effetti, se l'esperienza della presenza nel metaverso si evolvesse fino al punto da potere essere percepita nella sua pienezza, come identica a quella reale – come sembra potrà essere possibile nel lungo termine – alcuni studi indicano che generalmente sarebbe espressa una preferenza per la realtà simulata rispetto a quella analogica[13], fino

[10] L'architettura *client-server*, cioè il sistema per la trasmissione d'informazioni, del grande metaverso che si prospetta unico ed interoperabile, dovrebbe adottare a livello applicativo, un protocollo "neutro" sulla falsariga di quello che avviene già ora per Internet con l'Hypertext Transfert Protocol (http), nucleo base del World Wide Web (www) adottato fin dagli anni Novanta dagli enti normatori di Internet.

[11] Secondo un recente studio dell'Osservatorio sulle realtà immersive del Politecnico di Milano l'84% delle 141 realtà immersive ed aumentate ad oggi esistenti è sviluppato su tre piattaforme: The Sandbox, Decentraland e Roblox. Sempre secondo lo studio dei 141 mondi virtuali esistenti solo il 44% (circa 62 piattaforme) è già Metaverse Ready, ossia è liberamente accessibile da chiunque, persistente (continua cioè a esistere in maniera indipendente dalla presenza o meno di un soggetto), economicamente attivo, dotato di grafica 3D, con componenti di interoperabilità che permetterebbero di utilizzare gli asset digitali in maniera *cross-platform*. Cfr. *ilsole24ore.com*.

[12] Nel 2014 Facebook ha comprato l'azienda Scentsitive per 3,6 miliardi di dollari, una società che progetta e produce tecnologie per il profumo digitale attraverso sofisticati sistemi di stampa sintetica di odori. Lo sviluppo e l'applicazione dell'esperienza olfattiva sembra dovrebbe essere parte dei visori per il metaverso che sono in progettazione per la fine del decennio. Chi ragiona in termini di evoluzione tecnologica, infatti, non può fare a meno di mettere in conto che essa, prima o poi, sarà in grado di mettere l'uomo nelle condizioni di interagire tanto con la realtà virtuale, quanto con il mondo fisico "virtualizzato".

[13] La più celebre teoria sul punto è l'esperimento mentale di Robert Nozick (*Anarchia, Stato e utopia*, Firenze, 1974) sulla c.d. "Macchina dell'esperienza". Secondo Nozick, se la vita in un simulatore potesse garantire all'individuo la possibilità di vivere qualsiasi esperienza nello stesso grado di quella reale,

a portare, nel lunghissimo periodo, persino alla rinuncia di quello specifico *hardware* che oggi ne permette il concreto accesso, ovvero il corpo fisico. A quel punto ci dovremmo chiedere quale sia la vera realtà, se quella vegetale-materiale o quella sintetica-simulata. Ma per far ciò è innanzitutto necessaria una piena interazione tra stimoli fisici e vita digitale, in modo tale che il cervello – come avviene nel test di Turing per le IA - non possa più distinguere se siamo di fronte ad una simulazione o ad una realtà.
Già oggi, tuttavia, la vita quotidiana non immersiva *onlife*, per riprende una espressione ormai nota ai teorici del digitale[14], ha affiancato la dimensione corporea alla dimensione virtuale, "informatizzando" il mondo e di conseguenza "de-materializzando" il reale. Il filosofo coreano-tedesco Byung-Chul Han ben coglie questa duplice conseguenza, quando scrive che con la digitalizzazione abbandoniamo l'ordine terreno: «Oggi non abitiamo più il cielo e la terra, bensì il Cloud e Google Earth». E ancora: «la digitalizzazione conduce a una povertà di presenza e quindi di mondo, fino ad arrivare a non percepirlo più se sotto forma di informazioni e di dati»[15]. Le «non-cose», dunque, cioè le informazioni digitalizzate, «scacciano le cose»[16], cioè privano dell'esperienza della presenza, nella misura in cui attraverso è le cose che si sviluppa una porzione della identità dell'individuo e si rafforza la percezione di stare al mondo.
Il metaverso costituisce forse un passaggio ulteriore nella comprensione della linea di sviluppo dello spazio, fisico o digitale, che circonda l'utente e supera gli schemi tradizionali il mondo immersivo-digitale, ma non per il fatto che il mondo sia cambiato, quanto perché la realtà digitale incide diversamente sui processi cerebrali di adatta-

nessuno sceglierebbe di viverla, sapendo che si tratta di una vita simulata. Tale tesi risulta confermata da uno studio del 2014 (D. Weijers, *Nozick's experience machine is dead, long life the experience machine!*, in *Philosophical Psychology*, 27(4), 2014, 513 ss.), in cui è stato chiesto ai partecipanti se avrebbero accettato di vivere il resto della loro vita connessi ad una macchina in una simulazione che permettesse di esaudire ogni desiderio: il rifiuto della grande maggioranza delle persone coinvolte (84%) ha dimostrato che in genere l'essere umano dà più valore al rapporto effettivo con la realtà rispetto alle sensazioni delle esperienze. Tuttavia, già nel 1994, in "*Mental Statism and the Experience Machine*", Adam J. Kolber (*Mental Statism and the Experience Machine*, in *Bard J. of Social Science - San Diego Legal Studies Paper*, 3, 1994-1995, 10 ss.) avanzò l'intuizione per cui le conclusioni dell'esperimento mentale di Nozick potessero risultare ingannevole a causa del c.d. "pregiudizio dello *status quo*" - un fenomeno ormai consolidato in psicologia, secondo il quale le persone tendono irrazionalmente a preferire lasciare le cose come stanno. Questa idea è stata poi ripresa da Filipe De Brigard nel 2010 in un saggio a valle di una ricerca da lui condotta, nella quale ha avanzato l'idea della "macchina dell'esperienza inversa" (Cfr. F. De Brigard, *If you like it, does it matter if it is real?*, in *Philosophical Psychology*, 23(1), 2010, 43 ss.). Descrivendo un suo esperimento mentale, De Brigard ha chiesto ai partecipanti allo studio di immaginare di scoprire di essere stati collegati a una macchina dell'esperienza fino ad ora. A questo punto viene offerta loro la possibilità di uscire dal mondo virtuale a cui sono abituati, sapendo che la realtà sarà molto meno piacevole. Di fronte a questo scenario, solo il 13% dei partecipanti ha dichiarato che lascerebbe il mondo virtuale. Lo studio di De Brigard ha indicato che i rifiuti dell'offerta originale della macchina dell'esperienza di Nozick sono in gran parte determinati dal pregiudizio dello *status quo* piuttosto che dalla nostra valutazione della realtà. Infatti, la maggior parte delle persone dichiara di preferire la realtà quando pensa di essere nel mondo reale, ma sembra preferire la simulazione quando immagina di essere già nel mondo virtuale.

[14] L. Floridi, *The Onlife Manifesto: Being Human in a Hyperconnected Era*, New York, 2014.

[15] B-C. Han, *Le non cose*, Torino, 2022, 6, poi ribadito anche nell'intervista al Corriere della Sera, *Byung-Chul Han, la natura, i vaccini, le vite virtuali*, 27 febbraio 2022.

[16] Cosi V. Flusser, *Dinge und Undinge. Phänomenilogische Skizzen*, München, 1993, 81.

mento alla realtà[17]: le funzioni dei neuroni specchio, dei neuroni GPS, delle reti di auto-attenzione e delle oscillazioni neuronali *interbrain* sono, per così dire, in massima parte "normalizzate" attraverso l'esperienza immersiva, perché percepiscono quella dimensione come "luogo"[18]. Le realtà immersive o aumentate[19], dunque, non sono semplicemente mondi accessori a quello analogico – come avviene durante una conferenza su *Meet*, in cui l'utente rimane nel mondo reale e comunica attraverso il mondo digitale –, sono piuttosto luoghi sostitutivi.

Per parafrasare Han, nel metaverso ci troviamo nel crinale di passaggio tra l'èra delle cose e l'èra delle non-cose, dal momento che le informazioni, a mano a mano che la tecnologia grafica e simulativa si evolve, verranno sempre più percepite dal nostro io come veri e propri luoghi, come "cose", dunque, parte del mondo in cui l'uomo abita. La rivoluzione del metaverso sta nella sua capacità di alterare il modo con cui si percepisce la realtà poiché in esso, diversamente dall'Internet a due dimensioni, il nostro io dovrebbe ritornare a percepire le "cose".

Questo nuovo contesto ci richiede insieme pragmatismo e visione, cioè la capacità di contemperare quel che *è utile* con quel che *ha senso*. E le risposte sul senso e la ragione delle cose possono arrivare solo da una nuova filosofia delle forme – non è un caso che per gestire le implicazioni dell'informatica già verso la fine degli anni '80 IBM assumeva anche laureati in filosofia –, che nella realtà virtuale prendono vita come forme sintetiche, forme simili o addirittura identiche a quelle fisiche, ma frutto di processi di riproduzione[20], tanto che non è soltanto un'operazione meramente suggestiva parlare, parafrasando Walter Benjamin, di realtà "nell'epoca della sua riproducibilità tecnica".

3. Le funzioni e le prospettive d'indagine del metaverso

Accanto all'indagine sul "come" la realtà immersiva possa essere concepita e disci-

[17] È ciò che ricorda anche M. Gancitano, *I nuovi Dei*, Milano, 2021, 100.

[18] Come afferma D. Grimaldi, *Il metaverso come viaggio dentro noi stessi*, in *agendadigitale.it*, 4 gennaio 2022: «Il potere della presenza […] è dato dalla capacità della realtà virtuale di prevedere i meccanismi simulativi della mente umana; così, applicando il concetto di presenza al funzionamento dei neuroni specchio, siamo in grado di distinguere tra noi e l'altro e generare delle interazioni sociali credibili».

[19] La realtà aumentata è una tecnologia in cui il mondo reale viene "aumentato" attraverso l'aggiunta di elementi virtuali ed è utilizzata per arricchire l'esperienza utente aggiungendo elementi virtuali al mondo reale. Ad esempio, gli utenti potrebbero vedere informazioni aggiuntive su oggetti virtuali o interagire con oggetti virtuali in modo più realistico grazie alla tecnologia di realtà aumentata. Per un approfondimento, R. Moro Visconti - A. Cesaretti, A., *Il metaverso tra realtà digitale e aumentata: innovazione tecnologica e catena del valore*, in *Diritto di Internet*, 3, 2022, 627 ss., secondo i quali il metaverso costituirebbe l'ideale estensione di Internet, cioè il suo potenziamento.

[20] Della capacità del digitale di ri-creare il mondo sinteticamente, come si fa con gli aromi che del sapore o dell'odore delle cose ne sono una riproduzione chimica, C. Accoto, *Il mondo in sintesi. Cinque brevi lezioni di filosofia della simulazione*, Milano, 2022, spec. 10: «Chiari e continui sono oramai i segni che annunciano l'era della simulazione», avverte l'A. che elenca le future meraviglie: volti artificiali e carni coltivate, gemelli digitali e monete virtuali, creature biosintetiche e metaversi saturanti fino ad arrivare alle macchine quantistiche e agli impianti neuroproteisici, accostando la simulazione a quella che considera una nuova "terraformazione".

plinata (gli aspetti tecnologici e giuridico-organizzativi, appunto), è importante anche comprendere "perché" tale realtà stia prendendo piede e quale rivoluzionaria concezione della vita digitale stia alla sua base.

Anche senza considerare le numerose realtà prettamente ludiche (si pensi a programmi di *gaming* come *Fortnite* o alle piattaforme di socialità come *Second Life*) che ad oggi costituiscono le applicazioni di gran lunga prevalenti nei metaversi, gli attuali e i futuri utilizzi sono destinati per lo più ad attività integrative e migliorative dell'esperienza digitale non immersiva. Accanto all'accoglienza aziendale e lo svolgimento di conferenze[21], sono già in via di sperimentazione progetti di straordinaria utilità pratica: il riconoscimento di oggetti, la formazione di specialisti nel campo meccanico (BMW ha già realizzato il primo corso nel metaverso destinato agli apprendisti meccanici per insegnare a smontare e rimontare i propri motori, con evidente risparmio di denaro e di tempo per l'azienda e per gli apprendisti), oppure nel campo medico, con la possibilità di simulare interventi chirurgici per impratichire gli specializzandi senza rischi per i pazienti[22]. Sempre in campo sanitario, studi recenti hanno anche osservato che la realtà virtuale potrà essere impiegata per aiutare gli individui affetti da patologie da relazione (come autismo e agorafobia)[23] o da *ictus*[24].

L'obiettivo ultimo sembra però quello di sostituire larga parte della realtà analogica con quella digitale.

A fronte di queste prospettive di sviluppo, sono due le domande fondamentali da porsi.

Ci si deve chiedere se sia legittimo dare per scontato che alla base del metaverso vi sia un'evoluzione lineare, basata sull'ottimizzazione dei processi e delle realtà che già conosciamo, o se invece questa esperienza apra un capitolo nuovo del nostro rapporto non solo con il digitale, ma con l'intera realtà analogica; ci si deve domandare, cioè, se siano da mettere in conto innovazioni non prevedibili, applicazioni e opportunità inimmaginabili, come è stato per la rivoluzione digitale prodotta da Internet, che mutino il mondo per come lo conosciamo.

La seconda questione è un precipitato della prima: se il metaverso è destinato a seguire lo stesso percorso di Internet, allora l'ordinamento può ragionare attraverso le categorie giuridico-concettuali attuali, ma se invece la sua evoluzione è imprevedibile, come

---

[21] E. Dincelli - A. Yayla, *Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective*, in *The Journal of Strategic Information Systems*, 31(2), (101717), 2022.

[22] K. Bhugaonkar - R. Bhugaonkar - N. Masne, *The Trend of Metaverse and Augmented & Virtual Reality Extending to the Healthcare System*, in *Cureus – J. Med. Science*, 14(9), settembre 2022.

[23] W. Jarrold - P. Mundy - M. Gwaltney - J.N. Bailenson - N. Hatt - N., McInyre - K. Kim - M. Solomon - S. Novotny - L. Swain, *Social Attention in a Virtual Public Speaking Task in Higher Functioning Children with Autism*, in *Autism Research*, 6(5), 2013, 393 ss. D. Freeman - S. Lambe - T. Kabir - A. Petit - L. Rosebrock - Y. Ly-Mee - R. Dudley - K. Chapman - A. Morrison - E. O'Regan, *Automated virtual reality therapy to treat agoraphobic avoidance and distress in patients with psychosis (gameChange): A multicentre, parallel-group, single-blind, randomised, controlled trial in England with mediation and moderation analyses*, in *The Lancet Psychiatry*, 9(5), 2022, 375 ss.

[24] È la sperimentazione promossa dall'Azienda Ospedaliero-Universitaria di Parma e coordinata dal Centro Cardinal Ferrari – Santo Stefano Riabilitazione (Gruppo Kos) e dall'istituto Clinico Quarenghi di San Pellegrino Terme, che permetterà di valutare i tempi di reazione, ma anche di stimolare la loro mobilità.

possiamo impostarne di nuove? A fronte di questi rischi, sono da costruirsi nuovi e specifici diritti (e doveri) per i metaversi? E in caso affermativo, chi creerà le regole? Chi dovrà farle rispettare? Qualcosa di simile – come riporta Carl Schmitt – a quello che successe quando emerse l'esigenza di regolare il diritto del mare e ci si rese conto che era impossibile farlo con il semplice *nomos* della terra[25].

4. Diritti fondamentali e possibili criticità nella protezione dei dati personali

Come si è già accennato, uno dei vantaggi principali del metaverso sarà l'aumentata possibilità di interconnessione tra persone e tra esperienze: ciò avverrà attraverso la capacità di rendere i suoi spazi interoperabili[26]. Tale interoperabilità permette sempre più a questa realtà di trasformarsi in una sorta di serbatoio di sperimentazione e applicazione di moltissime tecnologie di lungo periodo, dalla *blockchain*[27] alle criptovalute, dagli NFT (*Non-Fungible Tokens*) alla DeFi (*Decentralised Finance*) e persino di alcune DAO (*Decentralised Autonomous Organization*)[28]. È *nella* e *grazie alla* realtà immersiva che queste ed altre innovazioni digitali trovano l'ambiente migliore per prosperare ed evolversi, non da ultimo per il fatto che il loro funzionamento prescinde dalla presenza dello Stato[29].

L'impiego di tali processi tecnologici è connesso con innumerevoli profili giuridici di stampo privatistico o pubblicistico. Tra i primi ci sono quelli legati alla contrattualizzazione delle relazioni di mercato che la rete infrastrutturale del metaverso, allo stesso

---

[25] C. Schmitt, *Il nomos della terra nel diritto internazionale dello "jus publicum europaeum"* 1950; ed. it., Milano, 1991. Riporta molto correttamente l'analogia A. Celotto, *Il "metaverso" e delle sue implicazioni per l'ordinamento giuridico*, audizione presso la Commissione Affari Costituzionali del Senato della Repubblica, in *senato.it,* 6 luglio 2022.

[26] L. Floridi, *Metaverse, a Matter of Experience*, in *Philosophy & Technology*, 35(73), 2022, spec. 4, anche se – come spiega lo stesso Floridi - è possibile che ad oggi tale scelta risulti ancora antieconomica, perché ogni azienda che opera nel suo metaverso cerca di attrarre più utenti possibili nel suo luogo, escludendo gli altri.

[27] Sulla perfetta adattabilità della *blockchain* al funzionamento del metaverso, in particolare alla tecnologia *peer-to-peer* e alle strutture di database che favoriscono l'*autogovernance*, l'accessibilità e l'interoperabilità, v. B. Ryskeldiev et al., Distributed Metaverse: *Creating Decentralized Blockchain-based Model for Peer-to-peer Sharing of Virtual Spaces for Mixed Reality Applications*, in *AH2018: The 9th Augmented Human International Conference, February 7–9 2018*, Seoul. Ciò che rende il metaverso un fenomeno completamente nuovo rispetto alle altre esperienze di realtà aumentata è proprio l'utilizzo della tecnologia *blockchain* che garantisce non più la semplice interconnessione tra mondo digitale e mondo reale, ma consente la creazione di un vero e proprio mondo alternativo, qualitativamente diverso da ogni esperienza di realtà aumentata precedentemente conosciuta. La *blockchain*, infatti, consente la decentralizzazione dei dati e l'interoperabilità: la prima permette di custodire su un registro decentralizzato le caratteristiche del nostro avatar e i nostri beni; la seconda permette il trasferimento dei dati e la loro interazione, dando così prova della proprietà digitale e consentendo la loro utilizzazione in qualsiasi metaverso si decida di frequentare. Cfr. C. Galli, *Blockchain, NFT e metaverso, tra tecnica e innovazione giuridica*, in *Altalex.com*, 11 luglio 2022.

[28] Sulle implicazioni giuridico-economiche del metaverso, R. Moro Visconti - A. Cesaretti, *Il metaverso tra realtà digitale e aumentata: innovazione tecnologica e catena del valore*, cit.

[29] In proposito si v. A. Monti, *Metaverso e convergenza tecnologica: aspetti (geo)politici, giuridici e regolamentari*, in G. Cassano - G. Scorza (a cura di), *Metaverso*, Roma, 2023, 65 ss.

tempo, consente e richiede, anche al fine di rendere negoziabili e opponibili a terzi i beni della vita che vengono in esso creati: si aprono così una serie di sotto-problemi legati alla proprietà intellettuale, alle transazioni[30] (e dunque all'uso di *token* non-fungibili) e alle obbligazioni non contrattuali[31]. Tra i profili pubblicistici, invece, vanno menzionati l'individuazione e la punibilità dei reati, l'imposizione fiscale, la garanzia del funzionamento dell'*e-governance* della pubblica amministrazione, la sicurezza nazionale e, soprattutto, la tutela delle libertà e dei diritti, tra cui primariamente la libertà d'espressione e la tutela dei dati personali. Raccolta e trattamento di dati (personali e non) è forse l'aspetto più problematico e più cruciale della vita *del* e *nel* metaverso.

Un metaverso interconnesso e ordinario (cioè non legato soltanto al tempo che l'uomo dedica al suo *divertissement*), dove si conduce parte delle normali attività quotidiane, comporta la raccolta di quantità massicce di dati, tra cui il monitoraggio delle abitudini di consumo, delle opinioni e dei gusti e persino delle emozioni attraverso l'analisi di dati comportamentali e biometrici[32]. Un ossimoro, dunque, sostenere il concetto di *privacy* nella meta-realtà. Nel metaverso ci sarà protezione dei dati personali, ma non *privacy* intesa nel senso originario del termine, come *right to be let alone*: il problema che si pone non è più *come avere accesso* ai dati personali degli abitatori di questa realtà, ma solo di *come gestire* il loro trattamento.

Da questo punto di vista i rischi sono reali e richiedono un'attenzione particolare su moltissime questioni. Tre in particolare.

Innanzitutto c'è il problema della portabilità dei dati: l'interoperabilità porterà una condivisione automatica dei dati tra metaversi. Come stabilire il bilanciamento tra diritti di proprietà sui dati e diritti degli utenti? E ancora: i dispositivi di accesso sono integrati con i contenuti dei servizi e ciò riduce notevolmente la capacità degli utenti di evitare la raccolta di dati personali: come sarà dunque possibile assicurare che la corrispondenza personale venga protetta sia dagli interessi commerciali delle aziende sia, in Paesi come la Cina, dalle interferenze dello Stato? Infine, sempre con riferimento all'organizzazione dell'infrastruttura, dovranno essere affrontate anche la conservazione, la gestione, la salvaguardia (nonché la responsabilità per il furto o l'uso improprio dei dati) e il

[30] Tra queste, forse le più rilevanti, riguardano, da una parte, il problema dei marchi (i diritti sui marchi di una azienda di moda, in particolar modo laddove questa non sia presente sul metaverso, si estendono anche al mondo virtuale?); dall'altra parte il problema del tipo di proprietà che segue una transizione in una realtà immersiva (l'opera d'arte acquistata nel metaverso è pienamente nella disponibilità dell'acquirente o si tratta di una forma di licenza?). In proposito, cfr. J. Bick, *Legal Issues Around Tangible Asset NFT's,* in *Law Journal newsletters*, ottobre 2021. V. anche C. Beckett - D. Geoffrey, *The Metaverse: a Virtual World with Real World Legal Consequences*, in *Rutgers Computer & Technology Law Journal*, 49(1), 2023, 1 ss.

[31] Molti sono gli esempi di incidenti e persino delle morti causate nella realtà fisica dai giochi a realtà aumentata. È il caso, ad esempio, di Pokemon Go: sebbene il tentativo del suo sviluppatore di esentarsi dalla responsabilità attraverso la sottoscrizione di clausole contenute nei termini di utilizzo, negli ultimi anni la società ha raggiunto numerosi accordi transattivi con i danneggiati. Per quanto riguarda la realtà virtuale, invece, non sembra ancora chiaro se esiste una personalità giuridica degli avatar e dunque se siano ad essi imputabili eventuali responsabilità. Il problema si pone con più forza laddove si comprenderà se l'avatar può agire indipendentemente dalla persona umana a cui si riferisce (processo forse reso possibile attraverso lo sviluppo del *deep learning*). Cfr. F. Sarzana di S. Ippolito - M. G. Pierro - I. Epicoco, *Il diritto del metaverso*, Torino, 2022, 32 ss.

[32] Come affermano anche F. Sarzana di S. Ippolito - M. G. Pierro - I. Epicoco, *Il diritto del metaverso*, cit., 38.

trasferimento dei dati utilizzati nel metaverso, tutto questo all'interno della cornice normativa e giurisprudenziale di derivazione europea[33].

C'è poi l'aspetto che riguarda direttamente le attività compiute *sugli* utenti attraverso il trattamento dei loro dati: si tratta ad esempio della soppressione o diminuzione della capacità di autodeterminazione degli individui, a vantaggio della formattazione su un unico standard dominante per la costruzione di ulteriori mercati. La prevalenza della realtà virtuale potrebbe facilmente condurre ad un nuovo assalto silente alla vulnerabilità umana esposta alla modulazione comportamentale degli utenti/consumatori, aprendo a diverse questioni di giustizia sociale, di mercificazione dei dati personali e di pratiche predatorie e aggressivamente profilatorie[34], senza contare che alla perdita di autonomia segue la perdita di libertà, la disintegrazione dell'identità personale[35] e, quindi, la violazione della dignità. Già oggi, a fronte di metaversi non ancora interoperabili, rimane fondamentale garantire l'utilizzo delle più aggiornate misure di sicurezza e di una metodologia certa nell'ambito della gestione dei *data breach*, considerato altresì che la realtà virtuale immersiva potrebbe generare nuove fonti di illeciti.

C'è infine l'aspetto dell'*accountability* che si riflette sia nel concetto di trasparenza delle condizioni contrattuali, sia soprattutto nel concetto di sicurezza come valutazione del rischio informatico, ovvero il rischio di danni diretti ed indiretti che possono derivare dall'uso delle tecnologie per il trattamento di dati, ai sensi dell'art. 32 GDPR. E questo spinge a porre l'attenzione fin dalla fase della progettazione (*by-design*), nel senso che il titolare deve avere in mente, sin da quando inizia a concepire di trattare dati di terzi, le misure specifiche da adottare per ovviare a specifici rischi. Il problema sta nella difficoltà di identificare tali rischi e, di conseguenza, la possibile strategia di un loro contenimento: stante l'imprevedibile evoluzione dei processi tecnologici e dei bisogni, una regolamentazione frettolosa può, da una parte, soffocare l'innovazione, dall'altra, paradossalmente, non essere efficace per la risoluzione dei problemi che potranno sorgere[36]. Al di là dell'imprevedibilità connessa alle innovazioni, tali misure possono

[33] A. Celotto, *Il "metaverso" e delle sue implicazioni per l'ordinamento giuridico*, cit. 4, richiama le sentenze *Schrems* e, in particolare, *Schrems II* della Corte di giustizia sul *Privacy Shield UE-USA*, che ha rilevato come la mancanza della adozione di una valutazione di adeguatezza da parte della Commissione europea continui a far permanere uno stato di incertezza nei traffici internazionali di dati. Essenziale sarò dunque risolvere questo nodo al più presto, pena l'impossibilità di funzionamento del metaverso i cui dati sono raccolti e gestiti automaticamente da sistemi di intelligenza artificiale.

[34] Si rimanda alla fondamentale prolusione conclusiva di S. Rodotà, *Privacy, libertà e dignità*, 26ma Conferenza internazionale sulla protezione dei dati, Wroclaw (Polonia) – 14-16 settembre 2004: «Senza una forte tutela delle informazioni che le riguardano, le persone rischiano sempre più di essere discriminate per le loro opinioni. (…) La *privacy* è strumento necessario per difendere la società della libertà e per opporsi verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale».

[35] G. Alpa, *Il diritto di essere se stessi*, Milano, 2021, spec. 253 ss.

[36] Sull'importanza di progettare tecnologie e spazi responsabili fin dall'inizio ha scritto, tra gli altri, con riferimento ad alcune prudenti interlocuzioni informali a livello di Unione europea, M. Pollet, *Métavers: les régulateurs face à la difficulté d'un nouvel espace encor à inventer*, in *Euractiv.fr*, 21 giugno 2022. La Commissione infatti, fino ad oggi, per quanto «non intenda aspettare che ci siano danni prima di intervenire» (così il Commissario per il Mercato interno Thierry Breton all'Assemblea digitale organizzata dalla Presidenza della Repubblica francese a Tolosa nel giugno 2022), non riesce ancora ad identificare le sfide che potranno sorgere. Quest'anno, tuttavia, si attende un primo libro bianco specifico sul metaverso da parte della Commissione.

e devono sicuramente ad oggi comprendere la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità, la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento[37].
La moltitudine di entità presenti nel metaverso e i loro ruoli intrecciati e sovrapposti creerà, infatti, una rete di relazioni che renderà molto difficile determinare le rispettive responsabilità e oneri. Ad esempio, definire la distinzione tra responsabile e incaricato del trattamento dei dati, cioè definire chi fa cosa per conto di chi, nel metaverso potrebbe diventare quasi impossibile. La raccolta dei dati sarà, poi, molto spesso involontaria e continua, rendendo quasi impossibile la raccolta del consenso, almeno per come lo si intende ad oggi alla luce delle regole del GDPR, esplicito e specifico: dove e fino a che punto si deve raccogliere il consenso dell'utente? E come concretamente adempiere all'obbligo di pubblicare le informative sulla *privacy*: esso deve valere per un particolare metaverso o per ogni entità a prescindere dal metaverso che essa abita?
Sebbene ad oggi, come ricordato anche dal Parlamento europeo[38], il quadro applicabile è quello delineato con il GDPR, sono sempre crescenti le voci di chi chiede di aggiornare questo fondamentale atto normativo, in particolare sotto l'aspetto della regolamentazione dei dati raccolti durante i comportamenti inconsapevoli o durante l'interazione con l'intelligenza artificiale (il recente caso ChatGPT che il Garante si è trovato a decidere dimostra la complessità, ma anche la necessità di un tale intervento).

5. Un problema di *governance*: il "medioeverso" come ordinamento giuridico neo-feudale

Tanto le prospettive pratiche, quanto quelle metafisiche ed epistemologiche alla base del metaverso sono importanti per comprendere il progressivo e inevitabile affiancamento e, forse, nel lunghissimo tempo, anche sostituzione del nostro mondo con il "*mundus novus*" digitale e immersivo, sebbene appaia difficile, ad oggi, immaginarci le ripercussioni che questa realtà avrà sull'ordinamento giuridico. In quanto esperienza sociale, benché digitale, la vita nel metaverso non può esistere senza un accordo su un sistema normativo condiviso.
Lo stesso ordine digitale-immersivo non è un ordine trascendente, ma è storicamente dato. È un ordine costruito e gestito artificialmente. Così come il mercato di cui è parte[39], il metaverso è un fenomeno creato dall'uomo e, dunque, nel bene e nel male, un

[37] Si tratta di garanzie previste nella bozza del nuovo regolamento sull'intelligenza artificiale, stante la interconnessione tra i due temi.

[38] Cfr. Risoluzione del Parlamento europeo del 5 maggio 2022 sulla competizione politica – report annuale 2021.

[39] Già alla fine degli anni Novanta, Natalino Irti nel suo *L'ordine giuridico del mercato* sottolineava come un certo mercato volesse impedire che il diritto conformasse in modo diverso lo scambio delle merci, adducendo come ragione che il mercato si regolasse da solo e dunque dal mercato provenisse anche, naturalmente, un modo di intendere l'uomo, i suoi spazi di libertà e i suoi diritti. N. Irti, *L'ordine giuridico*

ordine plasmabile.

I temi prioritari che le istituzioni della società analogica – comprese le imprese che investono sul metaverso – debbono affrontare per conto di quella virtuale sono quelli delle responsabilità e dei doveri. E perciò, accanto alla questione a quali valori la sua impalcatura e il suo funzionamento dovranno fare riferimento, resta una seconda domanda fondamentale: chi deve formulare le leggi valide nel metaverso? Accanto alla questione dei diritti, dunque, vi è quella ugualmente importante, della loro *governance*.

Il metaverso potrebbe essere davvero qualcosa di interessante se potesse essere disegnato, democraticamente, da tutti gli attori del mercato, tuttavia dobbiamo riconoscere che l'organizzazione della Rete non si è mai basata, nemmeno alla sua origine, su un discorso democratico, ma su una fragile dialettica di posizioni in contrasto tra loro[40]. Invero, alcuni tentativi di aprirsi in questa direzione sono stati avanzati negli ultimi anni: si pensi al *Metaverse Standards Forum*[41], il cui scopo dovrebbe essere quello di fornire ai diversi attori coinvolti l'opportunità di cooperare a livello industriale sugli standard di interoperabilità necessari per la sua costruzione. Ma per loro stessa natura l'interoperabilità tra standard, sistemi e applicazioni, che pure consentiranno agli utenti di spostarsi facilmente tra spazi e servizi diversi e, dunque, evitare la frammentazione tra i mondi che lo compongono, non risponde direttamente agli interrogativi che riguardano il rispetto dei diritti fondamentali degli utenti/cittadini del metaverso e, in particolare, della protezione dei loro dati personali.

Ad oggi non sembra ancora molto chiaro che ruolo eserciteranno le potentissime aziende proprietarie della maggior parte dei futuri luoghi che abiteremo[42]. Difficile non pensare che i demiurghi tecnologici - aziende il cui obiettivo è quello di aumentare il proprio fatturato - non coglierebbero l'occasione per prevedere, disciplinare e, probabilmente, influenzare le nostre emozioni, insicurezze, desideri, interessi.

La vera questione da affrontare riguarderà, dunque, il rapporto tra *contenuto* e *supporto*, cioè tra il bene comune che rappresenterà il mondo digitale e la proprietà privata che rappresenterà il terreno sul quale questa realtà si innesta.

La questione più seria è quella dell'*Ordnung ohne Ortung* per riprendere un'espressione di Carl Schmitt, poiché la deterritorializzazione pone la questione della sottrazione al diritto di quelle situazioni in cui un potere può imporre la propria supremazia di fatto[43].

Sembra ormai passato molto tempo, ma l'ambizione originaria degli operatori della Rete era riscoprire e riadattare i fondamenti assiologici dello Stato minimo ottocentesco: un ordine proto-liberale che salvaguardasse le libertà del singolo, lasciando ogni forma di sovranità ai margini della sua regolazione.

Ad oggi, invece, il rischio che si prospetta sempre più reale di fronte all'assenza dei

del mercato, Roma-Bari, 2003.

[40] Di questo accenna anche G.L. Conti, *La* lex informatica, in *Osservatorio sulle fonti*, 1, 2021, 318 ss., spec. 334.

[41] Cfr. *Metaverse Standard Forum*.

[42] Sul problema che comporta per la *net neutrality* la centralizzazione della *governance* del metaverso in capo ad alcune imprese private A.C. Nazzaro, *La natura giuridica del metaverso tra Stato,* essential facility *e giardino privato*, in G. Cassano - G. Scorza (a cura di), *Metaverso*, cit., 55 ss.

[43] C. Schmitt, *Il nomos della terra*, Milano, 1991 (ed. orig. *Der Nomos der Erde im Völkerrecht des Jus Publicum Europaeum*, Berlin, 1950).

poteri pubblici nel metaverso è quello del ritorno ad una sorta di forma di stato patrimoniale di stampo (neo)feudale, un *medioeverso* in cui i grandi proprietari (dei metaversi) sovrintendono e regolano l'interazione dei sudditi (gli utenti) stabilendo le regole e la loro applicazione[44]. In questo ordinamento di natura patrimoniale-pubblicistica c'è totale coincidenza tra la persona del Signore (la grande Big Tech) e la proprietà privata della terra (lo spazio digitale dove si costruisce il metaverso)[45]. La stessa natura contrattuale disuguale che assumeva il rapporto tra il feudatario e la comunità contadina si articola oggi nel rapporto tra piattaforma e utente, con la fondamentale differenza che a fronte di un diritto sostanzialmente consuetudinario tipico del mondo medievale (e quindi intrinsecamente antiassolutistico), nel mondo virtuale si assiste sempre più all'imposizione unilaterale dei principi fondativi e delle regole di comportamento della società.

La trasformazione dell'ordine "spontaneo", come era originariamente quello digitale, in un "assolutismo empirico" caratterizzato da un intreccio tra fine pubblicistico e fine privatistico, è determinata anche dalla montante privatizzazione della sfera pubblica che ha già imposto un ripensamento degli stessi presupposti alla base del nostro costituzionalismo[46]. Ad oggi, come avviene anche per lo spazio digitale non immersivo, i metaversi continuano nella direzione di ridurre lo spazio pubblico a beneficio del privato ancorché quest'ultimo è chiamato a pubblicizzarsi. Per usare una metafora che evidenzi la riconduzione a uno spazio giuridico definito diritto (con regole e giudici distinti) si può evocare la Platea Magna delle città medievali o il Foro di Roma antica. Le *Big Tech* occupano lo spazio corrispondente di incontro, confronto, commercio.

A fronte di ciò, come possono essere ridisegnati i rapporti non solo tra Stati-nazione e piattaforme, ma anche tra queste ultime e i cittadini-utenti, dal momento che le piattaforme sono soggetti formalmente privati che assumono, su una base contrattuale asimmetrica, un potere sostanzialmente pubblicistico in relazione alla libertà di espres-

[44] Sulla *governance* neo-feudale dei poteri private della Rete, v. J. Kotkin, *The Coming of Neo feudalism: a warning to the global middle-class*, New York, 2020. Ma anche A. Venanzoni, *Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*, in questa *Rivista*, 3, 2020, 178 ss.

[45] In realtà le tipiche caratteristiche dello Stato patrimoniale di stampo feudale emergono anche in relazione ad altri aspetti: la presenza di una monarchia o di un impero senza poteri effettivi e diretti sulle terre dei propri feudatari ricorda la difficoltà che incontrano, rispettivamente, gli Stati-nazione e gli ordinamenti sovranazionali nell'implementare il proprio *hard law* in rete. Esiste un vero e proprio trasferimento ai feudatari (le piattaforme) degli assetti produttivi e persino culturali della realtà, dal momento che sono le piattaforme a plasmare in larga parte le dinamiche di interazione sociale. Come ricorda G. Sartor, *Il diritto della rete globale*, in *Ciberspazio e Diritto*, 1, 2003, 47 ss., ciò è avvenuto attraverso la loro capacità di incidere sulla fisionomia e sulla modulazione dell'architettura-codice della Rete.

[46] Senza considerare che a fronte del penetrante controllo in relazione alle libertà di espressione dell'utente esercitato col concedere o negare l'accesso alla "loro" piattaforma o regolando i contenuti caricati su di essa, l'utente è di regola non adeguatamente informato riguardo alle funzionalità e ai meccanismi della piattaforma e tantomeno riguardo al trattamento dei suoi dati, così introducendo, a loro autonoma e non negoziabile discrezione, limitazioni e procedure ulteriori rispetto a quelli poste per tutti con la garanzia democratica e paritaria della legge. È chiaro, infatti, che data la multidimensionalità verticale e orizzontale del fenomeno, la regolazione sarà in larga parte autoregolazione. Ma per far ciò, sarà necessario stabilire, attraverso atti di *soft law*, rigidi protocolli e codici di condotta che guidino la progettazione del sistema e l'*enforcement* dei diritti. Sul punto A. Gatti, *Istituzioni e anarchia nella Rete. I paradigmi tradizionali della sovranità alla prova di Internet*, in *Diritto dell'Informazione e dell'Informatica*, 3, 2019, 711 ss.

sione del pensiero, alla gestione dei dati, alla libera iniziativa economica e, in generale, alle varie dimensioni della vita del contraente debole?
In questo senso, la "forma di Stato" del metaverso si differenzia rispetto all'attuale "forma di stato" della Rete, cioè della dimensione digitale non immersiva, per il fatto che questi rapporti si compiono in un *luogo* che è uno spazio omnicomprensivo. Nel *Medioeverso*, a differenza dell'Internet bidimensionale, i signori neo-feudali oltre ad essere "padroni della terra", cioè del nuovo spazio pubblico[47], – e dunque arbitri delle regole sociali e delle prospettive ideologiche alla base della vita della comunità (le regole della *community* come grandi costituzioni *ante litteram*)[48] – sono anche i demiurghi delle stesse leggi fisiche che reggono il mondo, veri e propri dei-creatori.
In un siffatto scenario di riduzione dello spazio pubblico a beneficio del privato (ancorché quest'ultimo è chiamato a pubblicizzarsi) la realtà immersiva richiederà uno suo sviluppo "sostenibile" in termini democratici, forse anche attraverso una distribuzione del suo plusvalore o di quote sociali ai suoi partecipanti[49] che potrebbero nel tempo trasformarsi anche in quote di sovranità politica sul metaverso.

6. Un tentativo di conclusione tra seduzioni, rischi e opportunità

Già nel 1973, precorrendo i tempi, Stefano Rodotà sottolineava come le nuove tecnologie avrebbero influito non solo sulla vita privata, ma avrebbero condizionato la stessa vita sociale, incidendo sullo *status* delle persone e sui loro orientamenti e quindi sulle loro libertà costituzionali[50].
I vantaggi – pratici ed esistenziali – che offre un "trasloco" sul metaverso rispetto agli altrove che compongono il nostro mondo (le straordinarie opportunità di vita potenziata, l'aumentata possibilità di interconnessione tra persone e tra esperienze[51], la seduzione della immensa possibilità di archiviazione del nostro "io", così come la possibilità di una vita pianificata) sono sotto gli occhi di tutti. Nondimeno esso dà una enorme *chance* di manipolazione delle nostre interazioni sociali, supportata dal continuo monitoraggio delle abitudini di consumo, delle opinioni e dei gusti e persino delle emozioni attraverso ogni tipo di dato, comportamentale e biometrico. L'esercizio delle nostre libertà in uno spazio digitale immersivo tocca nel profondo l'idea di identità della persona, il nucleo più profondo dell'art. 2 della nostra Costituzione e, più in generale, del principio personalistico sancito e garantito da tutte le costituzioni liberal-demo-

[47] Sia consentito un rinvio a G. Cerrina Feroni, *Come rifondare il diritto nella nuova realtà digitale*, in *Agenda Digitale*, 23 novembre 2020.

[48] G. De Gregorio, *Digital Constitutionalism*, Cambridge, 2022.

[49] Con riferimento allo sfruttamento dei dati da parte delle piattaforme, lo sostiene apertamente M. Ferraris, *Documanità*, Roma-Bari, 2021.

[50] S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973.

[51] Si è già accennato al fatto che obiettivo di medio-lungo termine di molte aziende sviluppatrici del metaverso è quello di rendere i suoi spazi interoperabili.

cratiche; il diritto *ad essere se stessi*[52], con il relativo bagaglio di convinzioni ideologiche, politiche, religiose, morali e sociali che differenzia l'individuo, ma allo stesso tempo lo qualifica. Il pieno godimento di questa libertà presuppone che il singolo possa determinarsi nella sua identità, che sia libero di compiere azioni e che la realtà circostante non lo influenzi oltre un certo grado. Ma l'individuo digitale, contrariamente a quello analogico, per sua natura indeterminabile, imperfetto e unico, sarà estremamente più determinabile, più "perfetto" e più "ripetibile" e con ciò più portato a seguire regole pre-impostate. Regole pensate dai demiurghi del metaverso che in tal modo possono potenzialmente esercitare una influenza normativa anche sulla libertà di espressione. Si può ad esempio pensare che, in ossequio alla teoria politicamente corretta del determinismo linguistico, per cui la lingua plasmerebbe il modo in cui pensiamo e le parole che utilizziamo definirebbero ciò che siamo[53], sarà possibile per un'*app* di socialità censurare alcuni pensieri o alcune parole che le regole di *community* non permettono, le quali, magari, saranno rese impronunciabili dagli avatar?

Il rischio di affievolimento o contenimento della propria identità rischia di essere aggravato dal controllo centralizzato delle piattaforme "feudatarie" non in quanto l'accesso venga precluso – atteso che, come già detto, i protocolli di sistema dovrebbero funzionare sulla falsariga del "www" –, ma in quanto le regole "fisiche" e sociali delle singole *app*-metaversi sono in mano alle sole piattaforme, senza alcun vero controllo o garanzia democratica. Come si può non concludere che questo non comporti una perdita di controllo degli utenti sui loro dati e persino sulle loro esperienze esistenziali *online*?

Senza dubbio anche su questo aspetto è il momento giusto per iniziare a proporre alcune considerazioni giuridiche più positive e di più ampio respiro sul tema della realtà digitale.

Per il metaverso privatizzato si potrebbe, ad esempio, pensare ad un'amministrazione congiunta di un insieme di organismi, sulla falsariga di ciò che già avviene per Internet (ICANN, W3C, IETF): ognuno di questi enti mostra la propria natura bipolare perché sono società private che orientano le proprie attività in senso pubblicistico. Se tale modello possa rappresentare una direzione anche per il futuro remoto non siamo certi, ma ogni tentativo creativo che avvicini il mondo digitale immersivo alle prassi del costituzionalismo è utile per ricordarci che i problemi che comporta il metaverso non sono inevitabili e possono essere mitigati attraverso tre regole auree che interagiscono tra loro: una maggiore (benché parziale) regolamentazione (da parte delle autorità pubbliche), una maggiore trasparenza (da parte delle piattaforme) e una maggiore consapevolezza (da parte degli utenti).

[52] Per riprendere l'evocativa espressione di G. Alpa, *Il diritto di essere se stessi*, cit., 253 ss.

[53] Tra i più recenti contributi sul tema, B. Cristalli, *Parla bene, pensa bene*, Milano, 2022.

L'art. 2 della Costituzione e il "Metaverso"*

Luca Di Majo

Abstract

Il contributo affronta una delle frontiere del progresso tecnologico-digitale: il Metaverso. A partire da una rilettura dell'art. 2 della Costituzione, sembra emergere la consapevolezza delle difficoltà di praticare gli strumenti del costituzionalismo classico sul terreno di nuove e inedite prospettive digitali ma, allo stesso tempo, di dover comunque individuare percorsi giuridici che possano, anche su questo terreno impervio, mettere "sotto diritto" e garantire quelle tutele che ci si è tanto sforzati di offrire alla persona umana almeno nelle Carte dei diritti e nella giurisprudenza delle Corti.
Le principali criticità connesse alla progressiva affermazione di tecnologie digitali sempre più "immersive" e alla conseguente smaterializzazione e decostruzione della stessa nozione di persona sembrano confermare la convinzione di trovarci in una fase di transizione dalla soglia antropologica che rischia di cedere davanti a meri interessi economici.

This paper addresses the one of the frontiers of technological-digital progress: the Metaverse. Reading the Article 2 of the Constitution, seems to emerge an awareness of the difficulties of practising the tools of classical constitutionalism on the terrain of new and unprecedented digital perspectives. At the same time, we need to identify new legal protections that can put "under the law" and guarantee those protections that we have striven so hard to offer the human person at least in the Charters of Rights and in the jurisprudence of the Courts, even on this impervious ground.
The main critical issues related to the progressive affirmation of increasingly "immersive" digital technologies and the consequent dematerialisation and deconstruction of the very notion of the person, seem to confirm the conviction that we are in a phase of transition from the anthropological threshold that risks yielding before mere economic interests.

Sommario

1. Premessa. - 2. Il Metaverso. - 3. L'art. 2 Cost., tra lettura classica e rilettura tecnologica. - 3.1. L'inviolabilità. - 3.2. La solidarietà. - 3.3. Il Metaverso come «formazione sociale»? - 4. Un rimedio per l'insostenibilità costituzionale del Metaverso: una Carta dei doveri?

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Keywords

Metaverso – diritti – Costituzione – Intelligenza Artificiale – costituzionalismo digitale

1. Premessa

La diffusione dei computer, l'accesso al *world wide web*, la progressiva affermazione dei social network, hanno scandito diverse fasi di rivoluzioni digitali (web, web 2.0 e web 3.0)[1], amplificando le relazioni tra l'uomo e il virtuale, agevolando il passaggio dalla *home computing* al *mobile computing*, fino all'affermazione di smartphone considerati vere e proprie estensione del corpo.

La successiva rivoluzione del *web 4.0* sarà, anzi, è già lo *space computing*, in cui la potenza computazionale è rappresentata da uno spazio immateriale ove l'uomo sarà in grado, meglio di come lo faccia oggi, di vivere un'esperienza virtuale, c.d. immersiva[2]: un "ambiente parallelo", nel quale la corporeità di un soggetto è invasa, condizionata e ricostruita attraverso elementi tratti da un «passaggio epocale»[3] in cui le tecnologie tenderanno a conformare il corpo della persona non soltanto nella sfera più direttamente percepibile della fisicità, ma anche nei processi cerebrali, nelle modalità di comunicazione e di approccio a un mondo nuovo, vissuto in modalità "*onlife*"[4].

Riecheggia, oggi, la prospettiva di una persona umana diversa, trascendentale, «pioneristica»[5], una sorta di riproposizione millenaristica di uno dei grandi temi di riflessione del '700, l'*homme machine*[6], inquadrato in un ambiente virtuale, in una realtà aumentata (o estesa)[7] definita Metaverso, contrassegnata con un simbolo (∞) divenuto comune ai più grandi sviluppatori di piattaforme nelle quali l'uomo trascende sé stesso e si

[1] B.L. Smith, *The Third Industrial Revolution: Policymaking for the Internet*, in *Science and Technology Law Rev.*, 3, 2019, T.E. Frosini - O. Pollicino - E. Apa - M. Bassini (a cura di), *Diritti e libertà in Internet*, Milano, 2017.

[2] L'approdo definitivo all'«umanesimo digitale», secondo M.I. Leocir Pessini, *Bioetica, umanesimo e post-umanesimo nel XXI secolo*, in *Revista Ecclesiastica Brasileira*, 306, 2017, 330.

[3] E. Mazzarella, *Contro Metaverso. Salvare la presenza*, Sesto San Giovanni, 2022, 109. Una sorta di «post-tutto», come rileva M.I. Leocir Pessini, *Bioetica, umanesimo e post-umanesimo nel XXI secolo: alla ricerca di un nuovo essere umano?*, Roma, 2018, 301.

[4] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, ma anche, dello stesso A., *The Onlife Manifesto, Being Human in a Hyperconnected Era*, Berlino-Heidelberg, 2015.

[5] G. Anders, *L'uomo è antiquato. Considerazioni sull'anima nell'epoca della seconda rivoluzione industriale*, trad. it. a cura di L. Dallapiccola, Torino, 2007: «come un pioniere l'uomo sposta i propri confini sempre più in là, si allontana sempre più da sé stesso, si trascende sempre di più, e anche se non si invola su una regione sovrannaturale, tuttavia, varca i limiti congeniti della sua natura, passa in una sfera che non è più naturale nel regno dell'ibrido e dell'artificiale».

[6] J. Offray de La Mettrie, *L'uomo macchina*, trad. it. a cura di F. Polidori, Sesto San Giovanni, 2015, spec. 56-61, considerava l'uomo come una macchina per essere in grado di riprodurre meccanicamente, a partire da stimoli eteronomi cc.dd. «molle», che generano la «simpatia tra muscoli e immaginazione», le funzioni umane.

[7] Ma, in realtà, anche «filtrata» dal titolare della piattaforma, come rileva E. Pariser, *Il filtro. Quello che Internet ci nasconde*, Milano, 2012.

«invola»[8] in quella regione transumana che Adolf Huxley aveva in qualche modo preconizzato.

Una sorta di simbiosi tra l'uomo e la tecnologia, punto di arrivo (forse?) di un percorso avviato con l'introduzione nell'uomo di corpi estranei (i chiodi per ricomporre le fratture, protesi di silicone per asimmetrie di gambe e bacino, ma non solo), di meccanismi salva vita (i *bypass*, i *pacemaker*), e giunto, con il Metaverso, ad una sorta di equivalenza tra meccanismi cibernetici, prodotti attraverso la scienza, e organismi biologici, sintomo di un passaggio quasi radicale dal regno dell'umano al regno dell'artificialità.

Ci troviamo di fronte non soltanto a un cambiamento del corpo e della persona, ma anche ad una modifica poliedrica dei suoi rapporti con il mondo esterno e con il fatto che si entra in relazione, in modo pressoché irreversibile, con la tecnologia.

Una "personalità download", da qualcuno definita «corpo elettronico», i cui dati sono distribuiti in contenitori collocati in luoghi diversi, dove la «nuova cittadinanza» non è più «il segno di un legame territoriale o di sangue» ma un «fascio di poteri e doveri che appartengono ad ogni persona»[9], alle frontiere di quello che è stato definito «postumanesimo millenarismo»[10], caratterizzato da una spinta in avanti inesauribile verso una molteplicità di specie, con un passaggio dal singolare al plurale, dall'evoluzione tradizionalmente darwiniana a quella guidata da tecnologie che consentono di plasmare o trasformare la forma umana.

Anche nello scenario post-umano, intorno al modo in cui viene costruita una società democratica all'interno della quale i diritti fondamentali delle persone devono essere garantiti in tutte le situazioni create dal mutamento tecnologico, riemerge il tema di come valorizzare i diritti fondamentali che viaggiano verso altre direzioni rispetto a quelle oggi legate alle categorie classiche, con riferimento particolare alla persona umana.

C'è qualcosa di anacronistico in questi principi oppure la continuità, l'universalità e la «permanente vitalità»[11] di straordinari valori, «patrimonio irretrattabile»[12] della persona, sanciti all'esito di un lungo processo[13], consacrati nelle Carte, riaffermati dalla giurisprudenza delle Alte Corti, vanno preservate per chiedersi se è legittimo essere assorbiti totalmente da taluni strumenti tecnologici che incidono significativamente sulla persona? È proporzionato l'uso di un determinato strumento rispetto al fine che si vuole perseguire?

---

[8] A. Huxley, *Religion without Revelation*, New York, 1957.

[9] S. Rodotà, *Relazione 2002. Discorso del Presidente Stefano Rodotà*, Roma, Garante per la protezione dei dati personali, 2003, 7.

[10] H. Jonas, *Dalla fede antica all'uomo tecnologico. Saggi filosofici*, Bologna, 2001. La tecnologia diventa, in sostanza, immanente nel corpo di una persona (in tal senso, R. Pepperell, *The Posthuman Manifesto*, in *Kritikos*, 2, 2005, 1 ss., ma anche U. Galimberti, *Psiche e techne. L'uomo nell'età della tecnica*, Milano, 2021).

[11] G. Zagrebelsky, *Diritto per: valori, principi, regole*, in *Quaderni fiorentini per la storia del pensiero giuridico moderno*, 31(2), 2002, 865.

[12] Corte cost., sent. 11/1956.

[13] P. Ridola, *Le libertà e i diritti nello sviluppo storico del costituzionalismo*, in R. Nania - P. Ridola (a cura di), *I diritti costituzionali*, vol. 1, Torino, 2001, 1 ss., spec. 35, ha posto in evidenza «la volontà [delle Costituzioni del XIX secolo] di opporre alle esperienze disumanizzanti della guerra, della persecuzione e dello sterminio, una immagine dell'uomo costruita su un patrimonio di diritti inviolabili».

Su tali aspetti il diritto ha il compito di costruire un contesto normativo coerente con la novità dei tempi, dove i valori e principi inviolabili del costituzionalismo – primi tra tutti, la dignità e l'eguaglianza sanciti dagli artt. 2 e 3 Cost. – non possono non tracciare il perimetro di una riflessione non più procrastinabile rispetto a cosa il diritto può fare, cosa il diritto deve fare e cosa, invece, deve astenersi dal fare[14], pur governando i rischi congeniti insiti nella tecnologia[15].

2. Il Metaverso

Il Metaverso è uno dei concetti più discussi della tecnologia moderna e non vi è, ad oggi, una definizione condivisa. Coniato nel 1992 da Neal Stephenson[16] nel celebre romanzo *Snow Crash*, veniva rappresentato come un «mondo virtuale che persiste nel tempo e coinvolge quasi ogni ambito dell'esistenza umana, influenzandola e interagendo con essa»[17]. Si trattava di una rappresentazione forse troppo pretenziosa di un ambiente a quei tempi ancora in una fase primordiale di sviluppo, certamente in continua espansione, ma dove «entità quasi nazionali organizzate in franchising […], città-stato con una propria Costituzione, i suoi confini, le sue leggi»[18], il suo popolo, apparivano per lo più affini a quello che è stato successivamente definito "proto-Metaverso", limitato ad una interazione sociale tra avatar e agenti software in un villaggio globale, tridimensionale, immersivo.

Non a caso, le prime forme di "proto-Metaverso" erano sviluppate su piattaforme simili ad un «parco giochi on line»[19], benché la conversione in uno spazio comune e digitalizzato – che ha poi consentito agli utenti di andare oltre la semplice interazione già oggi garantita, in diverse forme, dai social network – mutò da giochi multiplayer come *Fortnite* o *War of Warcraft* in vere e proprie comunità parallele, decentrate e collocate in «una rete di massima scalabilità e interoperabile di mondi virtuali 3D renderizzabili in tempo reale, che possono essere vissuti in modo sincrono e persistente da un numero effettivamente illimitato di utenti, con un senso individuale di presenza al loro interno, e che garantiscono la continuità dei metadati[20] relativi a identità, storia, oggetti, comunicazioni e pagamenti»[21].

---

[14] S. Rodotà, *La vita e le regole. Tra diritto e non diritto*, Milano, 2009.

[15] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995.

[16] Sebbene E. Zuckerman, *"Hey, Facebook, I Made Metaverse 27 Years Ago*, in *The Atlantic*, 29 ottobre 2021, ritenga che «*Stephenson, of course, wasn't being entirely original either. His vision of the metaverse owed a debt to Venor Vinge's 1981 True Names and to a series of Willian Gibson novels form the '80s. Both of those authors owed a debt to Morton Heilig's 1962 Sensorama machine, and on and on we go, back in time to Plato's shadows on a cave wall*».

[17] M. Ball, *MetaVerso. Cosa significa, chi lo controllerà e perché sta rivoluzionando le nostre vite*, trad. it. di G. Mancuso, Milano, 2022.

[18] N. Stephenson, *Snow Crash*, New York, 1992, 7, trad. it. di P. Bertante, Milano, 2022.

[19] S. Grauman Weinbaum, *Pygmalion's Spectacles*, 2, trad. it., *Gli occhiali di Pigmalione*, Firenze, 2013.

[20] Per tali aspetti, cfr. M. Palmirani, *Big Data e conoscenza*, in *Rivista di filosofia del diritto*, 1, 2020, 78 ss.

[21] M. Ball, *MetaVerso. Cosa significa, chi lo controllerà e perché sta rivoluzionando le nostre vite*, cit., 55. La parola Metaverso, composta da "meta-" (oltre, dopo) e "-verso" (universo), descrive «uno spazio digitale

Si tratta di un'esperienza molto complessa, ulteriore conferma della «vocazione liberale di Internet»[22]: un panorama oggi dominato da poche grandi aziende tecnologiche, unici soggetti deputati a definire l'architettura di standard e protocolli tecnici[23] frapposti al godimento di diritti fondamentali subordinati alle condizioni imposte da meri accordi negoziali. Insomma, una prospettiva non troppo rassicurante per il diritto, a fronte di un dilagante entusiasmo[24] dell'universo delle *big techno companies* che continuano a tralasciare, con imbarazzante disinvoltura, profili come il controllo, l'appartenenza, l'apprendimento di dati, la fidelizzazione[25], anzi guardando con favore l'assorbimento quasi totale dell'uomo umano nel virtuale ("il tuo dispositivo ti conosce, sa dove sei e quando"[26]), anche riconducendo il fondamento dell'esercizio di una forma significativamente pervasiva di un potere di soggezione[27] dell'individuo al solo esercizio della libertà di iniziativa economica[28].

Una versione tecnico-giuridica del concetto di Metaverso è contenuta nel documento licenziato dall'European Parliament Research Service, considerato come «*an immersive and constant virtual 3D world where people interact by means of an avatar to carry out a wide range of activities. Such activities can range from leisure and gaming to professional and commercial interac-*

abitato dalla rappresentazione digitale di persone, luoghi e oggetti» o «una nuova versione di Internet con la quale è possibile interagire direttamente» (F. Nasi, *Across the metaverse: un'introduzione al metaverso*, in *Pandora rivista,* 11 luglio 2022). Il Metaverso, così come inteso nella sua accezione più evoluta, deve possedere quattro caratteristiche: 1) realismo: consentire alle persone di immergersi emotivamente nel mondo virtuale; 2) ubiquità: gli spazi virtuali devono essere accessibili attraverso tutti i dispositivi digitali utilizzando l'identità virtuale; 3) interoperabilità consentire a sistemi o piattaforme distinti di scambiare informazioni o interagire senza soluzione di continuità; 4) scalabilità: disporre di una architettura di rete che fornisca una potenza sufficiente per consentire ad un numero massiccio di utenti di occupare il Metaverso senza compromettere l'efficienza del sistema e l'esperienza degli utenti. Sul punto, A. Pescapè, *Facebook diventa Meta. Si va verso la realtà virtuale*, in *Il Mattino*, 20 ottobre 2021, rappresentando la metamorfosi di Facebook, descrive «un ambiente dove le persone possono vivere e lavorare in un complesso mondo di realtà virtuale connessa: non più e non solo foto e video da guardare, bensì mondi virtuali nei quali immergersi. Mondi non più solo osservati attraverso un monitor, piuttosto confini da valicare graie a visori per realtà virtuale. Confini che una volta valicati porteranno l'utente, attraverso il su avatar, a vivere la propria vita nella stessa maniera della vita reale: la fusione di offline e online, la realizzazione dell'*onlife*. Attraverso il nostro avatar faremo acquisti, andremo al teatro o a cena da amici, andremo al lavoro e in vacanza. Il tutto comodamente seduti a casa nostra e semplicemente indossando dei visori per realtà virtuale».

[22] T.E. Frosini, *Internet come ordinamento giuridico*, in M Nisticò - P. Passaglia (a cura di), *Internet e Costituzione*, Torino, 2014, 63 ss.

[23] A. Quarta, *Mercati senza scambi. Le metamorfosi del contratto nel capitalismo della sorveglianza*, Napoli, 2020, 47.

[24] *Contra*, E. Mazzarella, *Contro Metaverso*, cit. In alcuni settori, come la sanità, la difesa, l'industria manufatturiera, l'istruzione o l'intrattenimento vengono già utilizzati applicazioni di "realtà mista" particolarmente interessanti (cfr. sul punto R. Moro Visconti - A. Cesaretti, *Il Metaverso tra realtà digitale e aumentata: innovazione tecnologica e catena del valore*, in *Diritto di internet*, 3, 2022.

[25] Su questi aspetti, ancorché riferiti ad internet in via generale, cfr. G. Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015.

[26] Non è un caso che Tim Sweeney, *Chief Executive Officer* di *Epig Games*, riconosce che «se una società centrale riuscirà ad avere il controllo del *Metaverso*, diventerà più potete di qualsiasi altro governo e sarà una sorta di Dio in terra».

[27] Nella dimensione tratteggiata da N. Bobbio, Il *problema del potere. Introduzione al corso di scienza della politica*, Torino, 2020.

[28] Lo rileva, benché per le piattaforme social, M. Cuniberti, *Potere e libertà nella rete*, in questa *Rivista*, 1, 2018, 39 ss.

tions, financial transactions or even health interventions such as surgery»[29]. Auspici di regolazione manifestati dal Parlamento italiano, ove ancora non è stato depositato alcun progetto di legge avente ad oggetto la regolazione delle nuove piattaforme digitali immersive[30], quantomeno nell'ambito delle competenze statali, si fanno lentamente strada.

Si tratta, purtuttavia, di un approccio non maturo e caratterizzato da una marcata indifferenza della politica (e del diritto) alla regolazione[31] di un aspetto soltanto parziale di un futuro sempre più tecnologico, dove lo Stato sarà chiamato a confrontarsi con le nuove tecnologie, oramai definitivamente entrate in ogni angolo della vita sociale: un ambiente parallelo in cui l'economia, le regole del mercato, la circolazione centralizzata o decentralizzata dei dati personali è ancora incontrollata, sregolata ed esclusivamente governata da grandi società private che hanno assunto un «ruolo infrastrutturale»[32] condizionante nell'accesso a beni e servizi da considerarsi essenziali[33] anche nel Metaverso.

Il Metaverso, fondato attorno ad un'invenzione della post-modernità, il corpo elettronico, è percepito già oggi come un potente strumento politico ed economico che plasma una società virtuale, per certi aspetti molto simile alla società degli stati feudali, corporativa, che inchiodava, in qualche modo, ciascuno alla condizione di nascita, per cui l'artigiano continuava a praticare la propria arte, l'aristocratico conservava i suoi privilegi, il contadino rimaneva ancorato alla sua terra. Una nuova linea di frattura nella quale la sedimentazione di un inedito «doppio standard»[34] caratterizzerà una *virtual reality* organizzata su individui ai quali saranno attribuite funzioni diverse non in base ad una decisione politica o sociale, ma attraverso il condizionamento biologico[35].

Tali considerazioni conducono ad una serie di interrogativi, invero già posti rispetto alla modernità, e che oggi riemergono per i nervi scoperti lasciati dal Metaverso: se siamo animali o siamo «automi»[36], se stiamo mutando progressivamente in schiavi felici delle macchine, perdendo la nostra naturalità[37] oppure resiste qualche elemento che

---

[29] *Metaverse Opportunities, risks and policy implications*, in *europarl.europa.eu*.

[30] La I Commissione affari costituzionali del Senato (XVIII Legislatura), il 31 marzo 2022 ha avviato, di propria iniziativa, 4 audizioni sul tema, i cui resoconti sono disponibili sul sito istituzionale del Senato della Repubblica *senato.it*. Parimenti, la Camera dei Deputati (XVIII Legislatura), l'On. Giulio Dori, ha presentato una interrogazione a risposta scritta indirizzata al Presidente del Consiglio dei Ministri, disponibile sul sito istituzionale della Camera all'indirizzo *camera.it*.

[31] Per gli aspetti normativi legati al digitale, cfr. *ex multis*, O. Pollicino - E. Bertolini - V. Lubello (a cura di), *Internet: regola e tutela dei diritti fondamentali*, Roma, 2013.

[32] F. Paruzzo, *I sovrani della rete. Piattaforme costituzionali e limiti al potere privato*, Napoli, 2022.

[33] Si tratta, infatti, di una struttura multiversante, in cui le piattaforme agiscono da intermediari e i dati individuali assumono un ruolo cruciale sia al momento della loro valorizzazione diretta, sia nella possibilità di rivoluzionare i servizi tradizionali (dal commercio al dettaglio, ai servizi postali, dall'intrattenimento audiovisivo e musicale al settore automobilistico, fino ai nuovi servizi finanziari), sia, infine, nella creazione di nuovi mercati.

[34] J.E. Butler, *The Double Standard of Morality*, in *Friends' Intelligencer and Journal*, XLIII, Philadelphia, Friends Intelligencer Association, 27 novembre 1886, 757–758.,

[35] A. Huxley, *A brave new world*, London, 1994. Più recentemente, M. Betzu, *Regolare Internet. La libertà di informazione nell'era digitale*, Torino, 2012, 15 ss.

[36] W. James, *Siamo automi?*, in W. James, *Alcuni problemi di psicologia*, a cura di M. Bella, Roma, 2002, 43.

[37] S. Butler, *Erewhon*, Milano, 1988.

continuerà a differenziarci dal puro essere e dal puro appartenere al mondo delle macchine. Sono temi che devono essere considerati e sui quali il costituzionalismo deve porsi quale elemento ordinatore di una società nuova, virtuale, tecnologica che chiede limitarsi non tanto – e forse non più – il potere statuale, quanto il potere economico «dominante»[38], manifestato attraverso la soggezione dei corpi virtuali, e con essi dei diritti fondamentali, alle grandi società che gestiscono i Metaversi[39].

Possono coesistere diritti fondamentali nel Metaverso, in assenza di autorità pubbliche legate ad una territorialità indefinita ove esercitare un monopolio della forza legittima volta, da un lato, ad arginare le prevaricazioni di colossi che guardano esclusivamente al profitto[40] e, dall'altro, a tutelare i corpi elettronici, controllare l'accesso alla rete dei minori[41], reprimere la pornografia, le fake news[42], il sexting, il cyberbullismo, l'incitamento all'odio, l'antisemitismo, le intimidazioni? Sono soltanto circostanze oggi penalmente rilevanti nel mondo reale, non facilmente giustiziabili nel Metaverso perché sono gli stessi sviluppatori a guardare con diffidenza controlli eteronomi di un mondo parallelo gelosamente custodito, che si vuole preservare da qualsiasi ingerenza statuale, rendendolo impermeabile al governo delle regole[43].

Se queste sono le premesse, per certi aspetti inquietanti, la riflessione da cui partire per delineare un modello di società virtuale irreversibile nel suo divenire, ma allo stesso tempo incoerente con i principi, i valori e le tradizioni storiche del costituzionalismo, deve essere incentrata su alcuni aspetti preliminari da non tralasciare e ben incastonati nella Costituzione italiana che pone la persona e il suo corpo unitariamente inteso

[38] A. Moazed - N.L. Johnson, *Modern Monopolies. What It Takes to Dominate the 21th Century Economy*, New York, 2016, R. Foroohar, *Release Big Tech's grip on power*, in *Financial Times*, 18 giugno 2017. In tale prospettiva, cfr. Anche M. Rubino de Ritis, *L'espansione economica nel Metaverso: i No Fungible Token*, in *GiustiziaCivile.com*, 16 novembre 2021.

[39] Non a caso, declinato al plurale, in quanto trattasi di «vari mondi digitali […] una somma di spazi interconnessi» (R. Moro Visconti - A. Cesaretti, *Il Metaverso tra realtà digitale e aumentata: innovazione tecnologica e catena del valore*, cit., 627).

[40] Come sostiene E. Mazzarella, *Contro Metaverso*, cit., 53, si tratta di una «pura sovrastruttura della struttura di produzione capitalistica (oggi interdipendenza globale delle economie pseudo-locali retta dalla loro finanziarizzazione), guidata dall'astrattezza del profitto». Già dal 2019, l'Osservatorio sulle piattaforme on line dell'Autorità per le garanzie delle comunicazioni rilevava un «balzo in avanti delle piattaforme on line» (spec. 5), con una crescita pari al 35% rispetto al 2017 e un fatturato globale pari a 632 miliardi di euro.

[41] Non solo, ma anche tutelarli da numerosi e pericolosi rischi, come mette in guardia G. Ziccardi, *Diritti digitali*, cit., *passim*.

[42] A.C. Freschi, *Falsità, manipolazione, intimidazione: le minacce digitali al pluralismo e alla democrazia*, in *Rivista il Mulino*, 4, 2019, F. Pizzetti, *Fake news e allarme sociale: responsabilità, non censura*, in questa *Rivista*, 1, 2017, 48 ss.. Sullo stesso tema, in generale, cfr. *ex multis*, F. Pizzetti (a cura di), *Internet e i diritti della persona. Il caso del motore di ricerca*, Firenze, 2015, M. Bassini - G.E. Vigevani, *Primi appunti su fake news e dintorni*, in questa *Rivista*, 1, 2017, 1 ss., G. Pitruzzella - O. Pollicino - S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, 2017, T.E. Frosini, *No news is fake news*, in *Dir. Pub. Comp. Eur.*, 4, 2017, 5 s., C. Pinelli, *"Postverità", verità e libertà di manifestazione del pensiero*, in questa *Rivista*, 1, 2017, 41 ss., M. Cuniberti, *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, ivi, 26 ss., N. Zanon, *Fake news e diffusione dei social media: abbiamo bisogno di una "Autorità pubblica della verità"?*, in questa *Rivista*, 1, 2018, 12 ss., R. Perrone, *Fake news e libertà di manifestazione del pensiero: brevi coordinate in tema di tutela costituzionale del falso*, in *Nomos*, 2, 2018, 1 ss., E. Lehner, *Fake news e democrazia*, in questa *Rivista*, 1, 2019, 92 ss., G. Donati, *Fake news e libertà di informazione*, ivi, 2, 2018, 440 ss.

[43] Cfr. S. De Vivo, *Viaggio nei metaversi alla ricerca del diritto perduto*, in *Informatica e diritto*, 1, 2019, 191 ss.

(fisico e virtuale) come nucleo centrale dal quale promanano e convivono diritti tradizionali e nuovi diritti.

Benché l'esatta portata e l'impatto sulla società e sull'uomo siano ancora per lo più sconosciuti, il Metaverso comporterà opportunità e rischi[44], pratiche illegali[45], legate per lo più a profili di proprietà intellettuale, di pubblicità ingannevole che, tuttavia, si ripercuotono sulla base di questa struttura verticale, senza la quale il Metaverso non avrebbe ragione di esistere: l'individuo virtuale, un corpo elettronico lasciato vagare in un ambiente immersivo sregolato, in cui le società private non si sono mai preoccupate – e, visti gli ultimi sviluppi, mai lo faranno – di tutelare gli avatar inibendo molestie verbali, incitamento all'odio[46], proiezioni antisemite[47], azioni inappropriate che configurano aggressioni sessuali o contenuti pornografici, diffusione di contenuti diffamatori, truffe, *malware*, *tracking* finalizzati ad accedere illegalmente ai portafogli digitali che memorizzano *No Fungible Token* o *cryptoasset*, attività di riciclaggio, giochi d'azzardo, tutte condotte equipollenti ad atti penalmente rilevanti e vietati nella realtà umana[48]. Diventerà sempre più concreta la possibilità di estrarre informazioni dalla persona umana per poi riversarle in ambienti virtuali, attraverso il trasferimento ad entità esterne artificiali a mezzo di impianti neuronali, visori, strumenti in grado di replicare non soltanto la mobilità sensoriale in ambienti inumani, ma anche le percezioni interiori, le emozioni, le paure[49], il feedback motorio secondo gli input provenienti dal corpo reale[50].

Pur essendo profili importanti da approfondire nel futuro prossimo e immediato, il punto di partenza preliminare per comprendere se e in che modo i diritti fondamentali possano coesistere con il Metaverso, non può che essere l'art. 2 Cost., per certi versi una sintesi dell'intera Carta costituzionale[51] e per tale ragione il nucleo più profondo

---

[44] Per una panoramica su profili legati al diritto costituzionale, cfr. P. Bonini, *Il "metaverso". Questioni e prospettive di diritto costituzionale*, in *Giustamm.it*, 9, 2022.

[45] Per una rassegna, D. Ingarrica, *Metaverso criminale. Quali interazioni nel presente nazionale e quali sfide globali del prossimo futuro*, in *Giurisprudenza penale*, 9, 2022, 1 ss. Benché tracce di orientamenti repressivi di alcune condotte inizino a farsi strada nella giurisprudenza (A. Fonsi, *Commercio dei dati e tutela del consumatore: il Consiglio di Stato rigetta il ricorso di Facebook su una sanzione dell'AGCM*, in *medialaws.eu*, 20 aprile 2021) e nei provvedimenti delle autorità amministrative indipendenti, come in esempio l'Autorità Garante della Concorrenza e del Mercato, che con delibera n. 27432 del 29 novembre 201848, ha sanzionato Facebook per pratiche commerciali scorrette, partendo proprio dal presupposto per cui «il modello commerciale di tale società si basa sulla raccolta e sfruttamento dei dati degli utenti a fini remunerativi».

[46] G. Ziccardi, *L'odio on line. Violenza verbale e ossessioni in rete*, Milano, 2016, G. Pesci, *L'odio on line, forme in continua evoluzione e il dibattito sulle modalità di contrasto*, in *Ciberspazio e diritto*, 69, 2021, 457 ss.

[47] Ed infatti, E. Mazzarella, *Contro Metaverso*, cit., non esclude una "resurrezione" in avatar di neonazisti che rappresentino Hitler.

[48] *Ex multis*, per una ricognizione tecnologica di condotte penalmente rilevanti, S. Canestrari - A. Manna - M. Papa, *Cybercrime*, Milano, 2019.

[49] Per certi versi, ancora più evoluto rispetto allo scenario descritto da K. Ashton, *That 'Internet of Things' Things*, in *RFID Journal*, 22 giugno 2009.

[50] Sulla trasferibilità degli aspetti sensoriali e fisici dall'umano al digitale, cfr. L. Voon Kiong, *Metaverse Made Easy: A Beginner's Guide to the Metaverse. Everything You Need to Know about Metaverse, BFT and GameFi*, pubblicazione indipendente del 9 gennaio 2022.

[51] Così M. Fioravanti, *Costituzione italiana: articolo 2*, Roma, 2017, 1. Tale prospettiva era stata fatta propria dalla Corte costituzionale sin dalle primissime pronunce, affermando che «l'art. 2 della Costituzione eleva a regola fondamentale, per tutto quanto attiene ai rapporti tra la collettività e i singoli,

dei diritti inviolabili, riletto in chiave tecnologica.

3. L'art. 2 Cost., tra lettura classica e rilettura tecnologica

Rispetto alle questioni precedentemente poste, la manifestazione più densa delle garanzie costituzionali resta un punto di partenza imprescindibile per la valutazione di quanto la persona e il proprio corpo virtuale siano effettivamente sovrani delle scelte nel Metaverso, se in tale ambiente immersivo, prospettabile oppure no come una formazione sociale, e in assenza di un'autorità di regolazione, i diritti fondamentali possano essere garantiti in una prospettiva «orizzontale»[52], dunque anche nei confronti «del potere privato, o comunque, come riconosciuto dalla giurisprudenza (Corte costituzionale, sentenza n. 122/1970), nei confronti di altri soggetti privati»[53].
Insomma, si tratta di comprendere, quale sia la porta di accesso alla garanzia e al godimento dei diritti inviolabili attribuiti all'uomo, «sia come singolo, sia nelle formazioni sociali» (art. 2 Cost.), anche nella dimensione dei rigidi schemi virtuali del Metaverso, ove si verifica, come vedremo, una scissione tra persona umana e virtuale, tra corpo e anima, caratterizzata da un'evidente asimmetria dal momento che le prerogative costituzionali incontrano una barriera invalicabile in tale mondo parallelo.
L' art. 2 Cost. segna un'autentica e consapevole rivoluzione copernicana nella concezione della persona: non più subordinazione allo Stato, quanto lo Stato in funzione della persona, di cui sono riconosciuti e garantiti i diritti inviolabili. Se considerato in una prospettiva inscindibile con l'umano, anche il corpo elettronico è persona, certamente diversa da quella reale, ma non per questo slegata dai principi di eguaglianza, autodeterminazione e dignità[54], nati da una lunga elaborazione, persistenti – in teoria – in questa inusuale dimensione, connessi al nuovo ambiente in cui è immerso il corpo.
Sul terreno del ripensamento delle categorie giuridiche, non a caso, uno dei dati più significativi è rappresentato dal processo di «costituzionalizzazione della persona»[55] che possiede un valore teorico molto importante e non si arresta innanzi ad un'ulteriore

il riconoscimento di quei diritti che formano il patrimonio irretrattabile della personalità umana e che appartengono all'uomo inteso come essere libero» (Corte cost., sent. 11/1956). Per la ricostruzione, in chiave più recente, delle posizioni assunte in Assemblea costituente, cfr. A. Barbera - F. Cocozza - G. Corso, *Le situazioni soggettive. Le libertà dei singoli e delle formazioni sociali. Il principio di eguaglianza*, *Le situazioni 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*, Bologna, 1984., spec. 211-213.

[52] Per la distinzione in merito ai destinatari dell'obbligo di riconoscimento e garanzia dei diritti fondamentali posto dall'art. 2 Cost., v. A Apostoli, *La svalutazione del principio di solidarietà. Crisi di un valore fondamentale per la democrazia*, Milano, 2012, *passim.*

[53] A. Barbera, *Art. 2*, in G. Branca (a cura di), *Commentario alla Costituzione*, Roma, 1975, 67.

[54] Secondo R. Mackling, *Dignity is a Useless Concept*, in *British Medical Journal*, 7429, 2033, 1419 ss., elemento recessivo dell'essere umano.

[55] Per una interessante ricostruzione, S. Rossi, *Lungo il percorso di costituzionalizzazione della persona. Riflessioni sull'opera di Stefano Rodotà*, in *BioLaw Journal – Giornale di Biodiritto*, 1, 2018, 147 ss. Sul ruolo della Corte costituzionale, invece, M. Fioravanti, *La Corte e la costruzione della democrazia costituzionale*, Roma, 2016.

rivisitazione di una categoria soggettiva plasmata dalla tecnologia immersiva.

L'art. 2 Cost. attribuisce alla persona un primato sostanziale[56], posizione emersa con forza dalle componenti cattolica e marxista in Assemblea costituente, benché con sfumature diverse, a tratti distanti, certo, ma solo apparentemente inconciliabili[57]. La garanzia dei diritti inviolabili non solo costituisce il limite invalicabile all'intervento dello Stato e dei pubblici poteri nella sfera dell'individuo, ma rappresenta anche la principale finalità dell'azione statuale in una prospettiva verticale che deve farsi carico della loro protezione anche contro le aggressioni provenienti da soggetti privati e, dunque, anche da chi gestisce le piattaforme digitali nei modi e nelle forme precedentemente descritte. È stato infatti già precisato che non è «alla natura pubblica o privata del potere che bisogna guardare per tutelare il sistema democratico o la dignità del singolo, quanto ai suoi effetti, al fine di evitare abusi derivanti da una combinazione di forze che si avvalgono di una libertà (quella di iniziativa economica e di impresa) a discapito di altri»[58].

L'art. 2 Cost. è una disposizione chiave per comprendere se e in che modo il Metaverso possa essere conciliabile con l'affermazione dei diritti costituzionali «inviolabili» che rappresentano, oltre al «vero e proprio fondamento dell'ordine sociale e politico»[59], il presupposto dell'essere *homo dignus*[60].

È singolare come l'art. 2 Cost. adoperi l'enunciato «la Repubblica riconosce e garantisce», *unicum* rispetto ad altre disposizioni, ove il riferimento è limitato talvolta al riconoscimento (artt. 4, 5, 29, 35, 45 e 46 Cost.) talaltra alla garanzia (artt. 32 e 37 Cost.) dei diritti costituzionali. Sono espressioni strettamente legate in un'endiadi per esprimere chiaramente l'idea che i diritti inviolabili connessi alla forma repubblicana[61] sono attratti da una natura costituzionale, non limitata alla sola enunciazione in Costituzione[62], piuttosto a situazioni soggettive connaturate a diritti di carattere fondamentale, «anteriori e precedenti»[63], inviolabili per l'appunto, ricavati da fonti ordinarie,

---

[56] In tal senso, D. Tega, *Articolo 2*, in F. Clementi - L. Cuocolo - G.E. Vigevani - F. Rosa (a cura di), *La Costituzione italiana. Commento articolo per articolo*, Bologna, 2018, 23.

[57] Cfr. *Atti dell'Assemblea costituente*, 307 ss., in particolare le posizioni di Togliatti e Dossetti. Per una ricognizione, anche A. Barbera, *Art. 2*, cit., spec. 50 ss., e M. Fioravanti, spec. 41 ss.

[58] P. Rescigno, *L'abuso del diritto*, in *Riv. Dir. Civ.*, I, 1965, 289.

[59] P. Ridola, *L'evoluzione dei diritti fondamentali e le trasformazioni delle Costituzioni*, in R. Nania - P. Ridola (a cura di), *I diritti costituzionali*, cit., 5.

[60] Secondo la ricostruzione fornita da S. Rodotà, *Antropologia dell'*homo dignus. *Lezione tenuta nell'Aula Magna dell'Università di Macerata il 6 ottobre 2010 in occasione del conferimento della Laurea honoris causa*, in *Storia e memoria*, 2, 2010, 107 ss.

[61] A. Apostoli, *La svalutazione del principio di solidarietà. Crisi di un valore fondamentale per la democrazia*, cit., 7.

[62] Nel senso che l'ordinamento a livello costituzionale individua i diritti fondamentali, per cui gli stessi devono essere riconosciuti dalla Costituzione e nella Costituzione.

[63] P. Ridola, *Le libertà e i diritti nello sviluppo storico del costituzionalismo*, cit., 38. In precedenza, già A. Barbera - F. Cocozza - G. Corso, *Le situazioni soggettive. Le libertà dei singoli e delle formazioni sociali. Il principio di eguaglianza*, cit., 209, rilevavano che «tale formula è stata adottata dall'Assemblea costituente sotto la spinta cattolica per operare un riferimento a diritti naturali propri di un ordine extrastatuale, che l'ordinamento statuale si limiterebbe a riconoscere». Non condivide pienamente questa impostazione E. Rossi, *Art. 2*, in R. Bifulco - A. Celotto - M. Olivetti (a cura di), *Commentario alla Costituzione*, Torino, 2006, spec. 43-44, benché individui un punto di incontro tra le opposte concezioni dei diritti.

canalizzati e consacrati[64] nel nostro ordinamento in atti e convenzioni internazionali, dal cui esame si possono enucleare una serie di diritti ulteriori e moderni che rispondono a queste caratteristiche, sempre che essi ricevano, nell'ordinamento, una effettività di tutela che li eleva al rango di diritti costituzionali.

L'art. 2 Cost. volge la prospettiva di tutela all'uomo, o meglio, alla «persona umana», a testimonianza di come i diritti inviolabili vivano nell'esperienza giuridica perché riferiti alla persona in quanto tale e inscindibili su ogni fronte, a prescindere da qualsivoglia qualificazione relativa alla cittadinanza, alla nazionalità, all'essere straniero, all'essere clandestino, all'immigrato digitale, affinché si attivi quel meccanismo di tutela che fonda la base legittimante di una disciplina più capillare, costituita da norme e dal perimetro interpretativo tracciato da un «uso sapiente»[65] della giurisprudenza, in relazione al «paniere»[66] ove sono collocati tutti quei diritti che concorrono, unitamente, a preservare la dignità della persona, tanto che in assenza o in violazione di uno di essi verrebbe tradito lo spirito costituente, e travolta la Costituzione nella sua più intima vocazione universalizzante dei diritti inalienabili della persona umana, «assunti come suoi principi fondamentali e poi anche supremi»[67].

Il riferimento ai «diritti inviolabili» è forse il più delicato per essere, l'inviolabilità, strettamente legata all'integrità dei diritti, all'impossibilità che essi subiscano un *vulnus* da parte di chiunque, delle autorità pubbliche, dello Stato medesimo, dei privati. Non si tratta di un'inviolabilità in valore assoluto, ma stabilita entro quei limiti in cui la tutela effettiva delle posizioni soggettive può trovare in essa. Anche i diritti fondamentali possono incontrare delle limitazioni che nascono dalle fonti legislative che li disciplinano, ma che, tuttavia, non possono andare ad incidere quello che viene considerato il nucleo fondamentale dei diritti stessi, cioè il nocciolo duro della loro essenza, quel limite che non può essere oltrepassato se non attraverso una rottura dell'elenco.

Tali condizionamenti, esaminati nella concretezza della tutela giuridica attribuita dall'ordinamento, trovano la loro giustificazione nel bilanciamento di una pluralità di interessi, tutti di livello costituzionale. Si tratta di un'apparente contraddizione dovuta ad un imprescindibile contemperamento, in esempio, tra l'interesse sotteso ad un qualsiasi diritto fondamentale (la libertà personale o la libertà di circolazione) e l'interesse statale all'ordine pubblico, alla difesa da attacchi esterni, dal terrorismo, che comporta una serie di possibili limitazioni lecite che i diritti stessi subiscono.

A tal riguardo, emblematica, è l'apparente contraddizione portata dalla disposizione dell'art. 32 Cost., considerato in una duplice prospettiva, come diritto fondamentale dell'individuo tutelato nel suo interesse specifico e nell'interesse della comunità, che rende l'idea delle possibili limitazioni che può subire[68]. Ogni volta che viene imme-

[64] Così A. Barbera, *Art. 2*, cit., 66.

[65] D. Tega, *Articolo 2*, cit., 22.

[66] M. Fioravanti, *Articolo 2*, cit., 69.

[67] Ivi, 110.

[68] Secondo la costante giurisprudenza della Corte costituzionale, il contemperamento del diritto alla salute del singolo (comprensivo del profilo negativo di non essere assoggettato a trattamenti sanitari non richiesti o non accettati) con l'interesse della collettività costituisce il contenuto proprio dell'art. 32 Cost. (sentt. 5/2018, 258/1994 e 307/1990) e rappresenta una specifica concretizzazione dei doveri di solidarietà di cui all'art. 2 Cost., nella quale si manifesta «la base della convivenza sociale normativamente

diatamente in rilievo la «persona umana», emerge con forza l'impostazione colta dai Costituenti di una cultura strettamente legata ai diritti inviolabili dell'uomo. L'art. 32 Cost. è la testimonianza di massima presbiopia del Costituente, di quanta lungimiranza e di quale straordinaria capacità di intuire la realtà, prossima o remota, caratterizzasse le posizioni dei componenti dell'Assemblea costituente. Non è affatto un caso che nel primo comma sia collocato l'aggettivo «fondamentale» accanto al diritto alla salute, considerato (insieme al lavoro) uno degli elementi costitutivi della «persona umana» a presidio della sua dignità.

Nella Costituzione tale termine ricorre non tanto nella logica del c.d. compromesso costituzionale o come una concessione a quella parte del pensiero cattolico che aveva le sue radici nel personalismo di Mounier[69]; non un contributo compromissorio, piuttosto una grande operazione culturale, generata da un confronto certamente vivace che ha spostato l'oggetto della tutela dall'individuo alla «persona» che è persona fisica, quindi "corpo", in qualunque prospettiva la si voglia inquadrare, umana o artificiale.

In una società dell'eguaglianza, democratica, tutte le persone devono essere considerate uguali, facendo astrazione della dimensione naturale nella quale si trovano perché nascono liberi ed eguali secondo le grandi formule delle dichiarazioni di fine '700 e delle convenzioni del '900.

Il confinamento, nel Metaverso, delle libertà nella sfera privata pone sullo sfondo la persona ed evidenzia, allo stesso tempo, alcuni nervi scoperti di una Costituzione forse ancora più, da sola, «insufficiente [e che esige] salde istituzioni di libertà»[70], non limitate alla sola pubblica amministrazione e ad un sistema giurisdizionale che faticano a rincorrere il progresso tecnologico per riattarlo a garanzia dei diritti crocifissi sull'altare di un'incontrollata crescita economica oligopolistica.

Nel contesto virtuale, infatti, i veri detentori del potere, i titolari delle piattaforme (pur essendo anch'essi «soggetti [privati] titolari dei diritti e, per converso, destinatari del vincolo in cui si esprimono i doveri»[71]) ove si svolge la vita degli immigrati digitali agiscono come uno Stato assoluto e così si identificano, dettano le regole, limitano i diritti, concedono o non concedono facoltà agli utenti, stabiliscono cosa può circolare e cosa non può circolare[72]. Insomma, si atteggiano come veri e propri "Meta-Stati" illimitatamente sovrani nel proprio territorio digitale, nel quale non ammettono ingerenze sotto forma di regole eteronome, salvo quelle autostabilite, esercitano la propria forza nei confronti del «popolo in rete»[73] che accetta, quindi legittima, una sorta di autoimposizione illimitata, «sospesa tra auto-regolazione da ordine spontaneo e arbi-

prefigurata dal Costituente» (sent. 75/1992).

[69] Secondo E. Mounier, *Il personalismo*, Roma, 1964, 81, «ogni persona ha un significato tale da non poter essere sostituita nel posto che essa occupa nell'universo delle persone. Tale è la maestosa grandezza della persona che le conferisce la dignità di un universo; e tuttavia la sua piccolezza, in quanto ogni persona è equivalente in questa dignità, e le persone sono più numerose delle stelle».

[70] Barbera, *Art. 2*, cit., 57.

[71] A. Apostoli, *La svalutazione del principio di solidarietà*, cit., 33, lo scritto in parentesi quadro è il mio.

[72] Circostanza mai celata da Mark Zuckerberg, come si legge nell'intervista rilasciata a *The Guardian*, il 19 settembre 2017.

[73] A. Venanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, in *Rivista italiana di informatica e diritto*, 1, 2020, 7.

trio»[74] sulla persona.

La logica dominante imposta da una libertà di iniziativa economica "orfana" dei commi 2 e 3 dell'art. 41 Cost., e la massimizzazione della proprietà privata – estesa finanche al corpo degli immigrati digitali, totalizzanti in un Metaverso caratterizzato dalla tradizionale logica statalista del XIX secolo – non solo pongono in secondo piano la persona e i suoi diritti, quanto l'architettura complessiva del modello costituzionale italiano e del costituzionalismo inteso come limite al potere; un potere certamente diverso da quello statuale e che radica la propria forza attrattiva in un benessere economico senza limiti per i soli signori delle piattaforme, in un ideale di società completamente diverso da quello reale nel quale dominano tutt'oggi – fortunatamente – i pilastri dell'art. 2 Cost.: inviolabilità e solidarietà, architravi dei diritti fondamentali contenuti nella Costituzione e attratti dalla «fattispecie aperta»[75] che consente di plasmarli in funzione di nuovi e inediti scenari, come il Metaverso per l'appunto, nel quale non si tratta tanto di riconoscere nuovi diritti, quanto di irrobustire garanzie diverse, restituirle a quei corpi virtuali che ne perdono la titolarità al momento dell'immersione e già prima dell'esercizio di facoltà "concesse" dai detentori del potere.

La cortina dell'intangibilità della persona e del suo corpo viene già infranta nel momento in cui essa si cala nella vita virtuale e diventa parte di un progetto economico teso a raccogliere una massiccia quantità di dati funzionali a rielaborare gusti, affinità, tendenze, passioni, utili limitatamente ad attrarre la persona digitale in un vortice di relazioni negoziali.

Insomma, i diritti fondamentali divengono strumenti a fini utilitaristici e la solidarietà estromessa a favore di una concorrenza senza regole tra corpi e corpi, tra corpi e piattaforme, tra piattaforme e piattaforme, in un legame profitto-benessere illimitato che non tiene conto – e come potrebbe farlo – «dell'anteriorità e della precedenza dei diritti»[76], della primazia della persona attorno alla quale il costituzionalismo ha costruito, a fatica, il principio dell'*habeas corpus*.

Si tratta, a ben vedere, di una società colma di diseguaglianze, caratterizzata da un gap incolmabile tra il popolo virtuale e le *big techno companies*, tra governanti e governati, per la riottosità di chi detiene potere e mezzi economici di essere limitato, perché alla limitazione della propria azione consegue una limitazione del profitto. I Metaversi sono fondati sulla negazione, in sostanza, del «doppio ruolo»[77] assegnato alla persona dalla Costituzione, come soggetto di diritti e come soggetto attraverso cui lo Stato (il titolare del potere politico reale) realizza la solidarietà tra gli uomini e il benessere della società

[74] Ivi, 6.

[75] A. Barbera, *Art. 2*, cit., *passim*. Tale caratteristica ha consentito alla Corte costituzionale, benché con qualche indugio, di riconoscere, tra gli altri, il diritto alla riservatezza della vita privata (in tutte le sue sfumature. Sul punto, cfr. M. Bellocci - S. Magnanensi - P. Passaglia - E. Rispoli, *Tutela della vita privata: realtà e prospettive costituzionali. Quaderno predisposto in occasione dell'incontro trilaterale delle Corti costituzionali spagnola, portoghese e italiana*, Lisbona, 1°-4 ottobre 2006, disponibile sul sito istituzionale della Corte costituzionale), il diritto all'abitazione (sent. 404/1988), il diritto alla vita (sent. 223/1996) anche del concepito (sent. 27/1975), il diritto degli omosessuali a costituirsi in «forma di comunità» (sent. 138/2010), il diritto all'identità di genere (sent. 221/2015).

[76] P. Ridola, *L'evoluzione dei diritti fondamentali e le trasformazioni delle Costituzioni*, cit., 38.

[77] M. Fioravanti, *Articolo 2*, cit., 58. Per A. Barbera, *Art. 2*, cit., 102, la persona è il «fine del sistema».

per mezzo del lavoro e della libertà di iniziativa economica, volti alla concretizzazione dei diritti sociali che ancora oggi caratterizzano la persona come degna di essere parte attiva di un contesto socio-economico che, allo stesso tempo, non può non reggersi sull'inviolabilità dei diritti e sulla solidarietà, espressi oltre il «temperamento delle ingiustizie»[78], attraverso il contributo offerto da ciascuno «al progresso materiale o spirituale della società» (art. 4, c. 2, Cost.), svolto anche a mezzo dell'iniziativa privata (art. 41 Cost.), ma senza arrendersi alla logica dominante di chi vuole piegare l'esercizio di diritti e libertà ai propri interessi personali, individuali, egoistici[79], in aperto contrasto con i pilastri dell'art. 2 Cost. che si irradiano nel complessivo impianto costituzionale.

3.1. L'inviolabilità

La caratteristica scultorea dell'inviolabilità dei diritti fondamentali è strettamente legata al riconoscimento della natura costituzionale di pretese inalienabili, imprescrittibili, irrinunciabili, indisponibili, assolute[80]. L'obbligo di garanzia posto in capo al legislatore e ai giudici (perché no, anche al Presidente della Repubblica), così come gli istituti della riserva di legge, del principio di legalità, sarebbero privi di significato se non accompagnati dall'inviolabilità.

Che senso avrebbe avuto, per il Costituente, la forte preoccupazione di predisporre un modello così articolato a difesa dei diritti, ivi compresa la rigidità costituzionale, con i suoi limiti ancora meglio declinati dalla Corte (sentt. 1146/1988, 366/1991, 348/2007 e 349/2007), in assenza di una qualità così densa, così limitante per i pubblici poteri, certo, ma anche per i soggetti privati, ai quali non a caso viene chiesto l'adempimento di doveri di solidarietà sociale, politica ed economica?

Insomma, senza l'inviolabilità, la complessiva architettura dei diritti costituzionali, espressi o attratti nella Carta, si sarebbe atteggiata come un principio generale non prescrittivo. Ed invece, l'inviolabilità è posta a presidio da un eventuale esercizio illimitato di prevaricazioni, vero e proprio contropotere collocato come cortina invalicabile del «privato debole, che subisc[e] una serie di condizionamenti tali da essere posto in soggezione nei confronti del potere privato, comunque nei confronti di altri privati posti

[78] C. Colapietro, *La giurisprudenza costituzionale nella crisi dello Stato sociale*, Padova, 1996, 344.

[79] Non a caso, A. Apostoli, *La svalutazione del principio di solidarietà*, cit. 45, fa notare che «basti pensare, a questo proposito, alla libertà economica, alla quale non è solo richiesto di non svolgersi «in modo da recare danno alla sicurezza, alla libertà, alla dignità umana», ma anche che «possa essere indirizzata e coordinata a fini sociali» (art. 41). E ancora, la Costituzione prescrive alla legge di riconoscere e garantire il diritto di proprietà, ma anche di determinarne i modi di acquisto, di godimento e i limiti «allo scopo di assicurarne la funzione sociale» (art. 42, c. 2). A. Barbera, *Art. 2*, cit., 102, rilevava come «attraverso il rinvio alla persona (non come valore astratto ma come persona fisica, nel suo concreto essere), si determina la possibilità di immettere nell'ordinamento costituzionale, con le garanzie ivi previste, tutti quei valori di libertà che il processo di emancipazione dell'uomo e l'evolversi della Costituzione materiale renderanno rilevanti […]. Attraverso la persona, e attraverso i valori che essa esprime, si opererebbe quindi quel processo dinamico di integrazione della Costituzione che in altra epoca Smend basava su altri valori e altri principi».

[80] P. Grossi, *Introduzione ad uno studio sui diritti inviolabili*, Padova, 1972.

in condizione dominante»[81], confermando così la duplice direttrice dell'art. 2 Cost., volta a porre obblighi e limiti nei confronti del potere statale e di soggetti, individuali o collettivi, collocati al di fuori della sfera pubblica.

Al contrario, l'inviolabilità dei diritti fondamentali diventa uno degli elementi sintomatici, forse più pregnanti, della rigidità Costituzionale[82]: promana dall'art. 2 Cost. e qualifica il fondamento dei diritti rendendone il contenuto irretrattabile innanzi ai tentativi di revisionismo delle conquiste più «sanguinose»[83] ereditate dalla resistenza; si afferma come «aspetto più profondo e sostanziale della rigidità costituzionale»[84], fondamento interpretativo preliminare che concretizza e rende permanentemente vitali i diritti fondamentali, senza che possano essere tacciati di anacronismo; si pone come parametro primario per stabilire, con sufficiente grado di certezza, il livello costituzionalmente ammissibile delle pretese dei singoli, delle interferenze esterne da parte dei poteri pubblici e privati, preservando quel «nucleo indefettibile della posizione giuridica del soggetto, che è fattore primario del libero sviluppo della persona nella varietà delle sue espressioni»[85].

L'art. 2 Cost. è la casa dei diritti fondamentali retta su solide fondamenta e su pilastri come l'inviolabilità, la direttrice lungo la quale si snoda il complessivo sistema accolto dalla Carta fondamentale e riconosciuto nelle Costituzioni del dopoguerra che ha consentito di rafforzare il contenuto dei diritti[86], di trasferirne la qualità a quelle situazioni soggettive non qualificate come costituzionalmente rilevanti, ma comunque accoglibili nel giardino dei diritti perché, attraverso la clausola aperta, sono degne di ricevere il crisma dell'inviolabilità (il diritto alla privacy, il diritto alla vita).

Tutto ciò svanisce nel Metaverso. Il consistente volume delle informazioni più intime relative alla persona umana, captate dai modelli di Intelligenza Artificiale, pone già una serie di problemi significativamente complessi relativi alla protezione dei dati, alla cybersicurezza, alla raccolta del consenso degli utenti finalizzata al trattamento dei propri dati sensibili, alla protezione degli avatar dal furto di identità o da un'ampia gamma di comportamenti illegali e dannosi, fino ad incidere su aspetti sensibili e inviolabili della persona umana come la salute, le pari opportunità, la tutela speciale di soggetti più vulnerabili[87].

I sistemi di realtà virtuale sono in grado di acquisire i dati biologici espressi dall'utente attraverso il linguaggio del proprio corpo virtuale come la dilatazione della pupilla, il

[81] A. Barbera, *Art. 2*, cit., 107.

[82] In tal senso anche A. Morrone, *Art. 2 della Costituzione*, in *Codice della famiglia*, 1, 2009. Non a caso, rispetto allo Statuto Albertino, la Costituzione ha "rovesciato il guanto": nello statuto regio, inviolabile era la persona del Re (art. 4), il domicilio (art. 27), la proprietà (art. 29), gli impegni dello Stato verso i creditori (art. 31), la dignità era collegata alla Nazione, la libertà personale era semplicemente «garantita».

[83] È il senso utilizzato da P. Calamandrei, *Discorso sulla Costituzione*, 26 gennaio 1955.

[84] M. Fioravanti, *Articolo 2*, cit., 5.

[85] P. Ridola, *L'evoluzione dei diritti fondamentali e le trasformazioni delle Costituzioni*, cit., 47.

[86] Come rileva E. Rossi, *Art. 2*, cit., 46-47, ha esteso l'inviolabilità ad altri diritti attraverso numerose pronunce, indicate nelle note.

[87] Per comprendere come opera l'Intelligenza Artificiale su questi aspetti, cfr. G. Cerrina Feroni - G. Fontana - E.C. Raffiotta (a cura di), *AI Anthology. Profili giuridici, economici e sociali dell'Intelligenza Artificiale*, Bologna, 2022.

movimento degli occhi, le espressioni facciali, la temperatura della pelle e le risposte emotive agli stimoli[88], trattando la persona non più solo per quel che ha già manifestato di essere, ma per ciò che si ritiene sarà in futuro. Insomma, vivere attraverso avatar e utilizzare attrezzature speciali come i visori di *virtual reality* (*VR*), ovvero ulteriori accessori in grado di trasferire la sensorialità umana nel mondo virtuale, comporta un processo involontario e continuo di raccolta di *Big Data*[89], biometrici, fisiologici cc.dd. «sensibili» ai sensi dell'art. 9, regolamento (UE) 2016/679 e dell'art. 4, c. 1, d.lgs. 196/2003[90], per i quali, in quanto attratti dall'inviolabilità, è richiesta tanto una protezione speciale quanto un consenso esplicito dell'utente per ciascuna finalità per le quali tali dati vengono utilizzati.

Nel momento in cui la persona umana immerge il proprio corpo nel Metaverso, vengono raccolte una quantità di informazioni personali sempre maggiori sui comportamenti assunti, al di là – anzi contro – ogni prospettiva di tutela della privacy, sia per utilizzarli al solo fini di incrementare il profitto dei titolari delle piattaforme virtuali, sia per tracciare i profili individuali, di gruppo, collettivi, che incasellano la persona in logiche di normalità o di utilizzabilità da parte di soggetti economici. Attraverso tecnologie di tipo probabilistico, le aziende governanti il Metaverso «si pongono come arbitri, che pretendono di autolegittimarsi e di gestire, sfruttando l'asimmetria di conoscenza derivante dalla mole di dati a loro disposizione, gli spazi di libertà che essi stessi concedono agli utenti»[91]. Insomma, violandone la sfera più intima, costruiscono sulla persona un profilo distinto e relativizzato: assemblando tutte le informazioni assunte, non solo creano una fotografia della persona, ma sono in grado di ricavare, con un elevato livello di certezza, la possibilità di stabilire quali saranno i comportamenti futuri «cesellati su bisogni, desideri, interessi creati ad arte mediante il continuo sfruttamento dei dati personali [sostituendosi] quasi integralmente al potere pubblico, rendendo la società digitale uno spazio vuoto impermeabile alle garanzie storiche del costituzionalismo»[92].

---

[88] Si può immaginare, in esempio, un utente che vede l'immagine di un'auto rossa e brillante. In un'esperienza VR la sua risposta emotiva può essere analizzata e tracciata, incluso il modo in cui essa cambia nel tempo. La dilatazione della pupilla potrebbe trasmettere l'eccitazione che l'utente prova nel vedere l'auto e le risposte galvaniche della pelle possono dirci quanto intensamente egli provi una particolare emozione.

[89] Secondo la lettera a) dei «Considerando della Risoluzione sulle Implicazioni dei Big data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto», adottata dal Parlamento europeo il 14 marzo 201760, i «Big data si riferiscono alla raccolta, all'analisi, all'accumulo ricorrente di ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di un trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento, che usano sia informazioni memorizzate, sia in streaming, al fine di individuare determinate correlazioni, tendenze e modelli». Secondo la definizione del Gruppo di Lavoro Articolo 29 per la Protezione Dei Dati, invece, tale nozione riguarda «gigantesche banche dati digitali conservate da aziende, governi e altre grandi organizzazioni che vengono analizzate in modo estensivo attraverso algoritmi elettronici». Su questi aspetti, cfr. G. Della Morte, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018.

[90] L'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale, i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.

[91] F. Paruzzo, *I sovrani della rete. Piattaforme costituzionali e limiti al potere privato*, cit., XI.

[92] A. Venanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, cit., 10.

La «psicografia biometrica»[93] consente di infrangere agevolmente la barriera dell'inviolabilità della persona, scissa tra umano e virtuale, di penetrare nel corpo, di raccogliere e utilizzare dati biologici per rilevare dettagli intimi su simpatie, antipatie, preferenze, interessi che possono condurre a metodi ancora più opachi e invadenti di profilare, categorizzare, catturare l'«orientamento economico»[94], manipolare gruppi sensibili e vulnerabili al di là di ogni relazione umana[95]. Si tratta di un *modus operandi* talmente invasivo da rompere la cortina della dignità come «forza di ogni essere umano di dare a sé stesso una qualche identità che egli ha scelto»[96].

Si tratta, a ben vedere, di un metodo standard di *social sorting*[97] significativamente intrusivo da comportare la perdita del controllo di ogni corpo virtuale[98], soggetto continuamente ad attività di «*targeting advertising*»[99] digitale aggressivo, di sorveglianza capillare[100] «preterintenzionale»[101] attraverso le "tracce lasciate in rete"[102]. Insomma, una struttura basata sulla condivisione di questi dati e sulla conseguente profilazione dell'utente che smentisce ancora una volta, alla radice, la pretesa di inviolabilità dei diritti costituzionali del cittadino nella più ampia rete (non soltanto nel Metaverso) «in favore di un modello di mercato in cui il consumatore è portato a scegliere quanto altri hanno già deciso, sulla base di un monitoraggio delle sue attitudini, inclinazioni e bisogni»[103]. Sono aspetti strettamente legati alla natura chiaramente economica di mondi virtuali e alla visione prettamente consumeristica dei dati delle persone[104], ad oggi monopolizzati da grandi aziende digitali molto più sensibili ad incrementare il business, perpetuando

[93] Electronic Frontier Foundation (EFF), *Virtual Worlds, Real People: Human Rights in the Metaverse*, 9 dicembre 2021.

[94] M. Weber, *Economia e società*, Roma-Ivrea, 1974.

[95] Su questi aspetti, cfr. S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004,

[96] G. Pico della Mirandola, *Oratio de hominis dignitate*, 1486.

[97] Vengono utilizzate le tecniche avanzate di *machine learning* e *deep learning*. Su tali aspetti, cfr. The Royal Society, *Machine learning: the power and promise of computers that learn by examples*, 2017, 5, consultabile all'indirizzo *royalsociety.org*, Select committee on artificial intelligence (House of Lords), *AI in the UK: ready, willing and able?*, 2018, consultabile all'indirizzo *publications.parliament.uk,* e M. Fasan, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *Biolaw Journal. Rivista di Biodiritto*, 1, 2019, 101 ss.

[98] Preconizzato, in qualche modo, da S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973.

[99] K. Cukier, *Data, Data everywhere*, in *The Economist*, 25 febbraio 2010.

[100] Parla di «capitalismo della sorveglianza» S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019.

[101] G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in questa *Rivista*, 1, 2018, 25,

[102] F. Paruzzo, *I sovrani della rete. Piattaforme costituzionali e limiti al potere privato*, cit., 6. Parla di «società dei sensori», G. Ziccardi, *Diritti digitali*, cit., 25-66.

[103] M. Cuniberti, *Tecnologie digitali e libertà politiche*, in *Dir. Inf.*, 2, 2015, 300. La stessa direttiva UE recante il Codice europeo delle comunicazioni elettroniche (Dir. UE 2018/1972) segnava il passo di questa mutata prospettiva e rilevava in modo esemplificativo come nell'economia digitale «i partecipanti al mercato sempre piú spesso ritengono che le informazioni sugli utenti abbiano un valore monetario. […] Il concetto di remunerazione dovrebbe pertanto ricomprendere situazioni in cui il fornitore di un servizio chiede all'utente finale dati personali ai sensi del Regolamento UE/2016/679 o di altri dati e questi glieli trasmette consapevolmente in via diretta o indiretta».

[104] G. Giannone Codiglione, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la «consumerizzazione» della privacy*, in *Dir. Inf.*, 2017, 418 ss.

pratiche anticoncorrenziali e autoreferenziali volte a favorire il prodotto *digital home made* attraverso la progettazione di siti web e interfacce applicative per dispositivi mobili, tesi a influenzare il comportamento e il processo decisionale degli utenti[105] attraverso modelli di apprendimento automatico di tracciamento e monitoraggio in tempo reale[106].

Un tale «shock antropologico»[107] apre uno scenario delicato in cui il profilo dell'autodeterminazione della persona, connaturato alla propria libertà e all'inviolabilità degli elementi sintomatici del corpo, impone di preservare la reversibilità della situazione precedente. In esempio, un impianto (come l'*holter* cardiaco) è utile in una fase diagnostica per tenere sotto controllo lo stato di salute e l'evoluzione post-operatoria, ma in un secondo momento deve essere possibile rimuoverlo, ripristinando lo *status quo ante*, altrimenti si mette in discussione l'autonomia di una persona ferma nella condizione di essere controllata dall'esterno da parte di qualcuno che, fino a un certo momento, esercitava un'attività del tutto legittima e nell'interesse della persona medesima, poi violata nella sua più intima essenza. Nel momento in cui tale finalità è venuta meno, il perseverare nello scambio di dati e informazioni attraverso gli impianti collocati nel corpo muta in una condizione diversa dalla tutela del diritto alla salute, piuttosto in una limitazione della propria autonomia, perché ciò che appartiene alla corporeità della persona è condiviso con soggetti esterni, sancendo la definitiva epifania della inviolabilità della persona e della capacità di autodeterminarsi.

L'esperienza della regolazione del fine-vita, dove la legge può intervenire solo per garantire l'effettiva libertà dell'autodeterminazione, non potendosi sostituire integralmente alla scelta soggettiva, ha lasciato uno straordinario insegnamento che fa della prevalenza del rispetto dell'inviolabilità della persona umana e dei diritti fondamentali il centro di gravità permanente di ogni ordinamento, quindi anche digitale, in prospettiva. L'autonomia declinata come autodeterminazione e presidio all'inviolabilità dell'essere umano e dei suoi diritti assume, in questo contesto, un valore fondativo per il godimento dei diritti fondamentali, al fine di evitare la costruzione di Metaversi non democratici e più simili a «non Stat[i]»[108] virtuali, dove la proprietà del territorio digitale e della persona – che ivi dovrebbe (ri)costruire la personalità parallela – è assorbita da un potere economico totalizzante e sregolato, in uno spazio svincolato dai poteri pubblici e connotato da rapporti di poteri privati contro i cui effetti il costituzionalismo contemporaneo è chiamato a elaborare strumenti di tutela equivalenti a quelli costruiti nei confronti del potere politico, per non trovarsi, un domani, a governare nuove forme di diseguaglianza o subordinazione che determinano, sul piano della struttura sociale, un'amplificata asimmetria tra il dover essere costituzionale e l'essere effettivo del diritto, a beneficio della potenza di sovrani globali e contro l'impotenza di con-

[105] Come evidenziato da C. Pinelli, *Pluralismo e democrazia nella società digitale. È tempo di regole?*, Seminario Astrid, 29 gennaio 2021.

[106] Secondo una ricerca condotta dalla società irlandese *Research and market*, sono 55 le società attive nel *Metaverso*, tra cui Meta Platforms Inc., Apple Inc., Google, Tencent Holdings, Microsoft, ByteDance Ltd., Alibaba Cloud, Sony Corporation, Baidu, Binance, Walmart, Nike, Gap. Inc, Netflix, Adidas e Atari.

[107] E. Mazzarella, *Contro Metaverso*, cit., 11.

[108] L'espressione è di N. Bobbio, *Il problema del potere*, cit., 37.

tro-poteri garantisti[109].

3.2. La solidarietà

La solidarietà conferma la primaria importanza della persona «come centro di interessi e valori attorno a cui ruota tutto il sistema delle garanzie costituzionali»[110]. È, dunque, l'uomo il capolinea dei diritti, certo, ma anche dei «doveri inderogabili», «destinati a tradursi […] tramite obblighi puntuali stabiliti»[111] da norme che «impegnano in modo prescrittivo la società nel disegnare il suo futuro»[112], talvolta direttamente dal testo costituzionale (artt. 4, c. 2, 30, 32, c. 2, 34, c. 2, 48, c. 2, 52, c. 1, 53, 54, cc. 1 e 2), talaltra nell'ordinamento statuale, nel quale la solidarietà assume una veste più concreta per essere diretta alla tutela dei diritti di chi si trova in una condizione fisico-giuridica inidonea a garantirli per sé stesso, o ancora per essere riconducibile allo spontaneismo solidaristico delle associazioni di volontariato[113] o del "Terzo settore"[114] impegnate in attività legate alla cura di «individui ovvero di interessi collettivi degni di tutela da parte della comunità»[115], scevre da qualsivoglia «calcolo utilitaristico o imposizione di un'autorità»[116], «non pressati dalla minaccia di una sanzione giuridica o etica»[117].
È un principio in continuo movimento, connaturato allo sviluppo di una società sempre più pregna di "diritti di nuova generazione" e di "nuove generazioni" ai quali non

[109] Così, L. Ferrajoli, *La costruzione della democrazia. Teoria del garantismo costituzionale*, Roma-Bari, 2012, 193.

[110] G. Lombardi, *Potere privato e potere negativo*, in *Autonomia e diritto di residenza*, in *Studi sassaresi*, (serie III), III, 1970-1971, 68.

[111] A. Barbera, *Art. 2*, cit., 99. M. Fioravanti, *Articolo 2*, cit., 117, specifica che la «solidarietà è il principio che caratterizza le Costituzioni del Novecento come costituzioni "politiche", destinate cioè a generare e alimentare un'obbligazione tra i consociati che è comunque più profonda e più solida di quella che sostiene un semplice patto di garanzia, stipulato tra possessori di beni e di diritti, che addivengono alla Costituzione solo ed esclusivamente per acquisire un migliore livello di garanzia di quei beni e di quei diritti. Nella logica della Costituzione democratica non c'è invece una Costituzione se non c'è un patto più esteso, che guarda più avanti nel futuro, e in forma più collettiva, con il disegno della "società giusta", che risulta dalla attuazione della Costituzione». V. Tamburrini, *I doveri costituzionali di solidarietà in campo sociale: profili generali e risvolti applicativi con particolare riferimento alla tutela della salute*, in *Ianus. Diritto e Finanza. Rivista di studi giuridici*, 18, 2018, 29, evidenzia che «la solidarietà non rileva unicamente come sentimento umano, come moto d'animo interiore capace insieme di giustificare e sorreggere la vita del gruppo sociale; né si configura come mero valore costituzionale, privo in quanto tale di forza prescrittiva. Essa è, senz'altro, un sentimento umano e un valore di rilievo costituzionale e può qualificarsi in questi termini». Sul percorso della pari ordinazione tra diritti e doveri, cfr. A. Apostoli, *Il consolidamento della democrazia attraverso la promozione della solidarietà sociale all'interno della Comunità*, in *Costituzionalismo.it*, 1, 2016.

[112] M. Fioravanti, *Articolo 2*, cit., 100.

[113] Sul punto, cfr. F. Rigano, *La solidarietà orizzontale e il ruolo dell'associazionismo*, in B. Pezzini - C. Sacchetto (a cura di), *Il dovere di solidarietà*, Atti del Convegno - Giornate europee di diritto costituzionale tributario, V edizione, Bergamo 14-15 novembre 2003, Milano, 2005.

[114] E. Castorina, *Le formazioni sociali del Terzo settore: la dimensione partecipativa della sussidiarietà*, in *Rivista AIC*, 3, 2020 e G. Tiberi, *La dimensione costituzionale del Terzo settore*, in *Astrid on line*.

[115] Corte cost., sent. 75/1992.

[116] Corte cost., sent. 500/1993.

[117] V. Tondi della Mura, *La solidarietà fra etica ed estetica: Tracce per una ricerca*, in *Rivista AIC*, 4, 2020, 3.

possono che legarsi, in una corrispondenza biunivoca da sempre vitale per il mantenimento della prospettiva solidaristica orizzontale[118], «nuovi orizzonti per una maggiore affermazione di solidarietà»[119] collocata tra «i valori fondanti dell'ordinamento giuridico, tanto da essere solennemente riconosciut[a] e garantit[a], insieme ai diritti inviolabili dell'uomo, dall'art. 2 della Carta costituzionale come base della convivenza sociale normativamente prefigurata dal Costituente»[120].

I doveri di solidarietà hanno attraversato la storia repubblicana progressivamente, rafforzandosi nel contenuto inteso come solidarietà «necessaria ed attuale»[121], «doverosa e cooperativa»[122], nel suo significato più profondo di «reciproco soccorso tra individui»[123], nel quale trovano collocazione non soltanto i doveri strettamente intesi come obblighi, bensì le limitazioni nel godimento di diritti fondamentali nel proprio nucleo più caratterizzante, in nome della salvaguardia di ulteriori che, altrimenti, ne subirebbero una compressione irreversibile. La libertà personale, la libertà di circolazione, la libertà di manifestazione del pensiero, possono subire limitazioni riservate alle fonti legislative, certamente senza incidere sul *nocciolo duro* della loro essenza che non può essere eroso se non attraverso la violazione del diritto medesimo. Sono diritti che vanno esaminati nella concretezza della tutela giuridica che l'ordinamento gli attribuisce e che comportano anche l'esame delle possibili limitazioni lecite che i diritti stessi necessariamente subiscono in nome di una solidarietà che ne circoscrive il contenuto senza sacrificarlo, anzi contribuendo – alle volte anche in maniera determinante – al bilanciamento, come nella legislazione di emergenza che, per sua stessa natura, comporta compressioni ai diritti fondamentali dei cittadini giustificati dal bilanciamento di una pluralità di interessi, tutti di livello costituzionale. Emblematico, a questo riguardo e ancora una volta, può essere considerato l'unico diritto espressamente qualificato come fondamentale in Costituzione, tutelato nell'interesse specifico del singolo e nell'interesse della comunità. La duplice veste assunta dall'art. 32 Cost. fonda il suo condizionamento più forte in quella solidarietà che, da un lato, legittima l'apposizione di limiti da parte di chi esercita la potestà pubblica in materia sanitaria, mentre dall'altro, contiene la riduzione del suo contenuto, paralizzando il rischio di un'estensione fin troppo incisiva del potere statuale tale da degradare la salute a mero interesse legittimo del singolo. È la solidarietà che rende il diritto alla salute intangibile fino ad una certa soglia e non oltre, perché vale il principio secondo il quale essa nasce dalla conformazione che, dei singoli, i diritti ne fanno fondamento costituzionale[124].

Alla luce di quanto ricostruito a partire dagli studi sviluppatisi sul tema, ci si chiede se i

[118] Sulla distinzione (invero che emerge solo su un piano strettamente teorico) tra solidarietà orizzontale e verticale, cfr. S. Galeotti, *Il valore della solidarietà*, in *Diritto e società*, 1996, 10.

[119] Lo aveva previsto, con lungimiranza, A. Barbera, *Art. 2*, cit., 97. Nello stesso senso, A. Pace, *Problematica delle libertà costituzionali. Parte generale*, Padova, 2003. *Contra,* G. Lombardi, *Contributo allo studio dei doveri costituzionali*, Milano, 1967, 40.

[120] Corte cost., sent. 75/1992.

[121] M. Fioravanti, *Articolo 2*, cit., 7.

[122] V. Tondi della Mura, *La solidarietà fra etica ed estetica*, cit., 11.

[123] A. Apostoli, *La svalutazione del principio di solidarietà*, cit., 24.

[124] Su questi temi, cfr. V. Tamburrini, *I doveri costituzionali di solidarietà in campo sociale: profili generali e risvolti applicativi con particolare riferimento alla tutela della salute*, cit., 31 ss.

doveri di solidarietà riconosciuti nella Carta costituzionale siano argini sufficientemente robusti non tanto per allentare la tensione tra profili individualistici e profili solidaristici, piuttosto per frenare il definitivo annientamento del contenuto di diritti già privi, nel Metaverso, di uno dei pilastri ad essi assegnati dall'art. 2 Cost. (l'inviolabilità per l'appunto), ivi registrando la completa assenza di una cultura solidale, né garantita da chi esercita il potere sul popolo virtuale, né assicurata dalla sedimentazione spontanea e volontaria dei singoli corpi virtuali consociati nel Metaverso, in sostanza smentendo il duplice volto del principio solidaristico[125].

Ed invero, le principali preoccupazioni affrontate oggi dai titolari delle piattaforme, dalle imprese tecnologiche «*over the top*»[126], sono volte esclusivamente all'intensificazione delle attività nella realtà aumentata, finalizzate all'esclusivo interesse di consolidare il profitto attraverso trasformazioni, fusioni, acquisizioni. *Blockchain*, criptovalute[127], *Non Fungible Token* (NFT)[128], sviluppo delle tecnologie di natura computazionale (*edge computing*, *quantum computing*, *distributed computing*), pur sollevando questioni oscure nella prospettiva del riconoscimento e della tutela, principalmente, della proprietà industriale e del *know-how*[129], restano ancorate ad una prospettiva strettamente economica, senza tener conto che l'impetuoso uno-due oligopolio/profitto mette all'angolo le residue prospettive di affermazione non soltanto della inviolabilità, quanto della stessa solidarietà che non può trovare spazio in un contesto dove la concorrenza è assorbente rispetto ai doveri imposti se si accoglie (e come non si potrebbe) l'impostazione tradizionale di Augusto Barbera che segna una corrispondenza biunivoca tra il catalogo aperto dei diritti e il catalogo aperto dei doveri[130].

Sono, tuttavia, esclusivamente quelle sopra elencate, ma senza presunzione di esaustività, le principali preoccupazioni di chi governa e opera nel Metaverso, «permeato capillarmente da un nuovo linguaggio produttivo e finanziario, elemento propulsivo della germinazione inarrestabile di organismi societari connessi in rete che attraverso Internet traggono nutrimento, capacità auto-poietica di sviluppo e di facilitazione dei sistemi complessi e degli ordinamenti giuridici»[131], restando sullo sfondo le violazioni

[125] Come rileva V. Onida, *Conclusioni*, in B. Pezzini - C. Sacchetto (a cura di), *Il dovere di solidarietà*, cit., 116, emergono due aspetti del principio di solidarietà: «il primo, nel quale la collettività politica, dunque l'autorità pubblica, configura diritti e assume la responsabilità di definire i modi in cui essi diventano effettivi, cioè vengono garantiti, o comunque definisce prestazioni doverose. Il secondo, in cui, al di là dei diritti garantiti e delle prestazioni doverose, la società è libera di esprimere le proprie energie di solidarietà, e deve essere incentivata a farlo».

[126] L'espressione è di M. Cuniberti, *Potere e libertà nella rete*, cit., 41.

[127] Su tale tecnologia, cfr. G. Gallone, *Blockchain e big data nel settore pubblico: spunti in tema di GDPR compliance*, in *Federalismi.it*, 14, 2022 e A. Nuzzo (a cura di), *Blockchain e autonomia privata*, Roma, 2020, e più recentemente, M. Passaretta, *La valuta virtuale nel sistema dei servizi di pagamento e di investimento*, Torino, 2023.

[128] Sul punto, cfr. R. Moro Visconti - A. Cesaretti, *La valutazione dell'arte digitale*, in *Il diritto industriale*, 5, 2021, 34 ss.

[129] Cfr., *ex multis*, A.C. Nazzaro, *Le regole del metaverso tra legge esistente e progetti futuri. Relazione, Stati Generali del diritto dell'Internet, 18 dicembre 2021, Roma LUISS*, in *Diritto di Internet*, 1, 2022.

[130] Nello stesso senso, anche A. Pace, *Problematica delle libertà costituzionali. Parte generale*, Padova, 1990, 15 ss.

[131] A. Venanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, cit., 8.

più concrete delle norme costituzionali dalle quali possono ricavarsi i diversi aspetti della solidarietà più pregnanti e più solidi per essere, il «dovere di avere doveri»[132], uno dei tratti caratterizzanti una società libera, eguale, solidale, che colloca al centro la persona in quanto tale.

La testimonianza più concreta della rarefazione della solidarietà è nell'azione di contorno di quei soggetti privati posti alle strette dipendenze dei colossi virtuali, assunti al solo scopo di implementare demograficamente il mondo parallelo attraverso la decantazione delle straordinarie opportunità esclusivamente economiche riservate agli immigrati digitali, attraverso l'esercizio di una pressione psicologica al di fuori delle tradizionali attività di marketing[133].

È chiaramente un diverso modo di intendere la coesione sociale, non tanto (anzi, per nulla) fondata sugli schemi tradizionali dei doveri costituzionali, piuttosto su una spirale economica che travolge l'individuo e lo rende impermeabile al principio solidaristico, incoerente con le spietate logiche concorrenziali. Dopotutto, si tratta di un'esperienza negativa già oggetto di attenzione nella dimensione più limitata dei social network, ma che è in realtà un problema più ampio e generale, presente in ogni contesto digitale ove si muovono utenti e fornitori di servizi, due categorie ontologicamente diverse, legate da una «solidarietà alquanto artificiosa»[134].

Nonostante si trattasse di conquiste date quasi per scontate da una legislazione che si avviava a considerare la persona come centro di gravità permanente, anche in una prospettiva quasi astratta e in riferimento alle generazioni future[135], il Metaverso, scambiato per una conquista millenaristica, ove il corpo virtuale dovrebbe massimizzare il benessere fisico ed economico, finanche a divenire immortale e resiliente ad ogni forza distruttiva, è, al contrario, il momento conclusivo della progressiva «svalutazione del principio di solidarietà»[136], tanto da consegnare una società più povera e retrograda, dove la «retorica individualista»[137], fondata sull'affrancamento del mondo virtuale dai principi dell'art. 2 Cost., prende il sopravvento su ogni prospettiva solidaristica schiacciata da chi non riesce a maturare la consapevolezza di come la costruzione di una società perfetta non è strettamente legata al solo benessere economico, ma poggi su ulteriori valori e principi in cui la società stessa si riconosce e di cui non può certamente farne a meno anche in uno spazio digitale oggi pressoché «vuoto e impermeabile alle

---

132 L. Violante, *Il dovere di avere doveri*, Torino, 2014.

133 Si tratta di veri e propri intermediari finanziari, benché non iscritti all'albo (e ciò comporta anche profili penalmente rilevanti, tra cui la violazione dell'art. 348 c.p.) che soggiogano psicologicamente tutti quelli che finiscono poi nella *rete*. Anche tali soggetti partecipano ai ricavi *pro quota*: più è grande la rete da essi creata, maggiori sono i guadagni.

134 M. Cuniberti, *Potere e libertà nella rete*, cit., 44.

135 Sul punto, cfr. E. Rossi, *Art. 2*, cit., 57 ss., L. Buffoni, *La "dottrina" dello sviluppo sostenibile e della solidarietà generazionale. Il giusto procedimento di normazione ambientale*, in *Federalismi.it*, 8, 2007, R. Bifulco, *Diritto e generazioni future. Problemi giuridici della responsabilità intergenerazionale*, Milano, 2008 e D. Porena, *Il principio di sostenibilità. Contributo allo studio di un programma costituzionale di solidarietà intergenerazionale*, Torino, 2017. Più di recente, L. Bartolucci, *Il più recente cammino delle generazioni future nel diritto costituzionale*, in *Osservatorio costituzionale,* 4, 2021.

136 A. Apostoli, *La svalutazione del principio di solidarietà*, cit., *passim*.

137 D. Tega, *Articolo 2*, cit., 26.

garanzie storiche del costituzionalismo»[138].
In assenza della solidarietà, in quanto elemento sintomatico di connessione tra le Costituzioni del Novecento, «viene meno il cemento che tiene unita la Repubblica»[139] e quell'indissolubile sodalizio con l'inviolabilità attraverso il quale la persona resiste come centro di attrazione dei diritti, in mancanza del quale «viene fatalmente a mancare anche la Repubblica dei diritti inviolabili»[140].

3.3. Il Metaverso come «formazione sociale»?

L'avvento del Metaverso non può essere considerato soltanto guardando alla modifica, sempre più a portata di mano, del corpo in sé (c.d. *body swapping*), ma per il modo in cui il corpo stesso, dunque la persona, entra in relazione con gli altri e con «il mondo nella rete»[141] – uno spazio molto più dilatato rispetto alle piattaforme social – all'interno del quale si trova a vivere.
La personalità di un individuo è uno degli elementi sintomatici della propria identità, legata alla comunità nella quale si relaziona, a prescindere dalla natura reale o virtuale. La società pluralista non si compone solo di una sommatoria di individui isolati, ma si articola in una molteplicità di formazioni intermedie, frapposte fra il singolo e lo Stato, all'interno delle quali gli individui organizzano la propria vita.
La prospettiva della primazia della persona trova così specificazione e completamento nel principio pluralista che segna il superamento della concezione individualista propria del liberalismo classico: la persona non è considerata un atomo nella società, piuttosto come nucleo di un fascio di relazioni più ampie, intrecciate in organizzazioni plurali autonome, ma non per questo affrancate dallo Stato[142].
Il riconoscimento dei «diritti inviolabili dell'uomo» come singolo, certo, ma allo stesso tempo nella dimensione delle «formazioni sociali», li coniuga, come una endiadi, ai «doveri inderogabili di solidarietà politica, economica e sociale», saldando il principio personalista con il principio solidarista[143] nella dimensione pluralista, segnando il passo del definitivo abbandono di quella concezione che tendeva a «funzionalizzare le libertà o viceversa a dare ad esse contenuti sostanzialmente antistatalistici»[144].

---

138 A. Venanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, cit., 10.

139 M. Fioravanti, *Articolo 2*, cit., 7.

140 *Ibidem*.

141 Si tratta di un'espressione di S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, 28, benché l'Autore, in quel frangente, non si riferisse ovviamente al Metaverso.

142 A. Barbera - F. Cocozza - G. Corso, *Le situazioni soggettive. Le libertà dei singoli e delle formazioni sociali. Il principio di eguaglianza*, cit., 201, legano la «personalità a chi è ritenuto dal diritto oggettivo centro i imputazione di qualifiche giuridiche: cioè la persona fisica o le persone giuridiche (raggruppamenti di persone o di beni riconosciuti e assimilati alle persone fisiche) ovvero determinate associazioni, anche se non riconosciute».

143 Così, S. Galeotti, *Il valore della solidarietà*, cit.

144 A. Barbera - F. Cocozza - G. Corso, *Le situazioni soggettive. Le libertà dei singoli e delle formazioni sociali. Il principio di eguaglianza*, cit., 211.

L'art. 2 Cost., diversamente dalla concezione digitale imposta dal Metaverso, «riconosce e garantisce» l'esercizio di diritti umani inviolabili in una dimensione plurale, non esclusivamente nel rapporto uomo-uomo, bensì in un contesto più ampio, costituzionalizzando tutte quelle «formazioni sociali» che contribuiscono al perfezionamento dell'uomo stesso «mediante una reciproca solidarietà economica e spirituale»[145].
Si tratta di «articolazioni materiali»[146] multiformi, di varia natura, come le confessioni religiose (art. 8 Cost.), la famiglia (art. 29 Cost.), le associazioni generalmente intese (art. 18 Cost.) ovvero individuate più specificamente rispetto al fine (i partiti politici, art. 49 Cost. e i sindacati, art. 39 Cost.), «fino a ricoprire l'intero insieme delle relazioni sociali tra i consociati e, dunque, la società intera»[147], riconosciute dalla Costituzione «nella misura in cui consentano e favoriscano il libero sviluppo della persona o nella misura in cui garantiscano interessi diffusi rilevanti costituzionalmente»[148]. Sono formazioni sociali quegli «enti nei quali l'integrazione dei singoli è elevata a svolgimento della loro personalità»[149], luoghi ove si concretizza il legame tra il principio pluralista e il principio solidarista nei modi e nelle forme che devono consentire all'individuo di massimizzare la propria «vocazione sociale»[150].
La Costituzione riconosce ai singoli ampia libertà di dar vita ad aggregazioni sociali per il perseguimento delle più diverse finalità, finanche attraverso la valorizzazione dell'iniziativa dell'associazionismo privato (art. 118 c.c.) per lo svolgimento di attività e compiti di interesse generale, per esercitare in maniera più efficace i diritti che la Costituzione attribuisce loro. Per il raggiungimento di fini costituzionalmente rilevanti, le formazioni sociali godono, con gli opportuni adattamenti, delle libertà riconosciute ai singoli come la libertà di darsi un ordinamento interno e l'autonomia nell'esercizio dei poteri da esso previsti, coerentemente con i principi costituzionali.
L'erosione di due pilastri dell'art. 2 Cost., inviolabilità e solidarietà, potrebbe condurre a ritenere irrilevante il prosieguo della riflessione proposta. In effetti, laddove sia deficitaria ogni prospettiva di tutela e di garanzia della persona umana nell'esercizio dei propri diritti inviolabili, come potrebbero aprirsi scenari diversi nella dimensione pluralista dei Metaversi è un qualcosa che, nell'immaginario del giurista, prende forma come una vera e propria utopia, pur non essendo, per certi aspetti, un problema nuovo e slegato dalla storia passata delle stesse formazioni sociali[151].
La natura oligopolistica delle piattaforme virtuali immersive appare infatti antitetica allo stesso principio pluralista che pretende lo sviluppo della persona umana non solo

[145] D. Tega, *Articolo 2*, cit., 21.

[146] M. Fioravanti, *Articolo 2*, cit., 13.

[147] Ivi, 34-35.

[148] A. Barbera, *Art. 2*, cit., 109.

[149] L. Elia, *Le norme sulle «formazioni sociali» nella Costituzione repubblicana*, in Aa.Vv., *Studi in onore di Gustavo Vignocchi*, Modena, 1992, 545.

[150] A. Apostoli, *La svalutazione del principio di solidarietà*, cit., 107.

[151] A. Barbera, *Art. 2*, cit., evidenziava che «i modelli pluralistici si pongono oggi come dei modelli non sempre avanzati e tali da costituire talvolta un ostacolo allo sviluppo della persona, in riferimento al quale, in una società fortemente integrata, non è indifferente il modo in cui certi interessi collettivi vengono tutelati […]; le formazioni sociali sono state di fatto utilizzate, talvolta, come strumento di mediazione e di controllo sociale anziché come strumento di tutela delle libertà personali».

nella stretta dimensione individuale, piuttosto in una visione più ampia, in una cornice istituzionale idonea alla edificazione e allo sviluppo della propria personalità.

Insomma, si fa sempre più concreta l'idea che il Metaverso, almeno per come la sua struttura e le sue caratteristiche si presentino oggi, si collochi al di fuori del perimetro costituzionale[152].

In effetti, lo scarto tra le «formazioni sociali» intese dall'art. 2 Cost. e il Metaverso appare sin dal principio notevole: non va certamente dimenticata quella parte dell'articolo in esame ove si afferma, in maniera scultorea, «l'adempimento di doveri inderogabili di solidarietà politica, economica e sociale» dai quali, tuttavia, le piattaforme tendono ad affrancarsi per costruire una comunità antitetica rispetto ai principi costituzionali attinenti alla persona umana, tecnicamente impossibili da preservare per l'esclusiva natura economica del Metaverso ove il profitto, la rendita, la concorrenza, inibiscono l'espansione delle libertà costituzionali tanto in una direzione verticale (tra i proprietari delle piattaforme e gli utenti) quanto orizzontale (tra i corpi virtuali)[153], in un contesto nel quale «valorizzazione e salvaguardia delle posizioni soggettive all'interno delle formazioni stesse, tra le quali è da annoverare lo stesso diritto alla partecipazione»[154], vengono decisamente rifiutate.

Dopotutto, i prodromi all'esasperazione del conflitto tra la persona (con il proprio bagaglio di diritti) e il potere privato di grandi piattaforme digitali, si erano già sedimentati nella tensione emersa tra gli interessi economici e gli interessi privati nella versione più generale della rete telematica[155]. Non a caso, «la natura sociale di tali aggregazioni è profondamente condizionata e compenetrata dalla dimensione economico-imprenditoriale»[156] prevalente in Internet e assorbente nel Metaverso, trasferendo così nella rete quella tensione generata dalle storiche «contraddizioni del processo produttivo capitalistico che ha fatto sorgere la necessità della difesa attiva di interessi di cui nessun gruppo è portatore in via diretta e che non possono quindi essere adeguatamente tutelati attraverso la normale dialettica dei gruppi stessi»[157]. Per tale motivo, già in passato, parte della dottrina faceva registrare una forte resistenza verso particolari forme di aggregazioni, così da escludere dal novero delle «formazioni sociali» le associazioni costituite per fini economici[158], mettendo in luce la più intima contraddizione tra chi detiene la ricchezza, manifestatasi molte volte come forma di potere diversa da quella statale, e il singolo. Tuttavia, mentre nella dimensione delle relazioni industriali, a garanzia e a tutela dei lavoratori, dunque di tutte quelle norme cardine per la dignità (su tutte l'art. 36 Cost.), sono però collocati quei sindacati che si identificano come vere

[152] Su cosa può essere o non può essere formazione sociale, cfr. A. Ruggeri, *Costituzione e formazioni sociali: modello ed esperienze a confronto (note minime, introduttive ad un dibattito)*, in *Consulta on line*, 2, 2019.

[153] Su questi temi, cfr. F. Pizzolato, *Mutazioni del potere economico e nuove immagini della libertà*, in *Costituzionalismo.it*, 3, 2017, 3, ma anche, il volume a cura dello stesso Autore, *Libertà e potere nei rapporti economici. Profili giuspubblicistici*, Milano, 2010.

[154] A. Ruggeri, *Costituzione e formazioni sociali*, cit., 272.

[155] P. Passaglia, *Internet nella Costituzione italiana: considerazioni introduttive*, in M. Nisticò - P. Passaglia (a cura di), *Internet e Costituzione*, cit., spec. 37 ss.

[156] M. Cuniberti, *Potere e libertà nella rete*, cit., 44.

[157] A. Barbera, *Art. 2*, cit., 110.

[158] P. Rescigno, *Persona e comunità. Saggi di diritto privato*, Padova, 1967.

e proprie formazioni volte a stemperare le tensioni sociali[159], nel Metaverso è assente ogni manifestazione di garanzia anche minima per la persona umana, anzi un potere sregolato, esercitato su un numero crescente di soggetti geneticamente mutati in corpi virtuali e immersi in una potente e ramificata organizzazione sociale.

Ed allora, se questo è il teatro nel quale l'inviolabilità, la solidarietà e i doveri né giocano ruoli da protagonisti, né sono parte di un copione già scritto nei "proto-Metaversi", non affatto imperniato su solidi fondamenti costituzionali, anzi legato strettamente ad una regolazione di natura economica volta alla massimizzazione del profitto in una logica «privatistica e proprietaria»[160], la riflessione potrebbe chiudersi già ora estromettendo il Metaverso da qualsiasi discorso sulla coerenza con il nostro sistema ordinamentale, collocandolo al di fuori della categoria «formazioni sociali» anche per la difficoltà ad intercettare garanzie ulteriori per i diritti fondamentali.

È vero, al pari delle altre comunità di utenti, che la classificazione del Metaverso come formazione sociale potrebbe comportare paradossalmente una restrizione delle libertà del singolo piuttosto di una dilatazione[161], ma sarebbe opportuno, a sommesso avviso, recuperare almeno quella dimensione istituzionale o ordinamentale di siffatte aggregazioni virtuali al fine di legittimarle nei confronti dei pubblici poteri, così consentendo allo Stato di estendere progressivamente il proprio raggio di azione allo scopo di restituire piena effettività ai diritti fondamentali non tanto secondo lo schema tipico delle situazioni soggettive individuali, piuttosto anticipando la tutela alla persona attraverso un paradigma diverso, vietando piuttosto che riconoscendo. Dopotutto, si tratta di recuperare la concezione istituzionale dei diritti fondamentali, flagellata nel Metaverso, attraverso un'azione dei pubblici poteri diversa e fondata sulla limitazione della libertà di iniziativa economica dei gestori delle piattaforme, pure consentita dai c. 2 e 3 dell'art. 41 Cost., e sulla moderazione della stessa comunità degli utenti prim'ancora che si trasformi in una comunità immersiva.

Ci tornerò nelle conclusioni, ma l'accostamento – non proprio il riconoscimento – del Metaverso alle «formazioni sociali» rappresenta invero un'ulteriore spinta per il legislatore a rompere quella cortina di ferro, quel muro invalicabile e apparentemente impenetrabile di un anfratto di silicio refrattario a divenire parte di una dimensione ordinamentale caratterizzata da una configurazione dei diritti fondamentali solida, nella quale, similmente alle formazioni sociali tradizionali, possano prendere forma una serie di garanzie, anche indicando il perimetro dei principi non negoziabili in un contesto plurale, per non offuscare la persona nell'anonimato di potenti e ramificate organizzazioni sociali anti-costituzionali.

4. Un rimedio per l'insostenibilità costituzionale del Metaverso: una Carta dei doveri?

La tutela dei diritti fondamentali è un tratto caratteristico dell'età delle Costituzioni,

[159] Sulla funzione dei sindacati, cfr. G. Pera, *Problemi costituzionali del diritto sindacale*, Milano, 1960.

[160] M. Cuniberti, *Potere e libertà nella rete*, cit., 49.

[161] In tal senso, ancora M. Cuniberti, *Potere e libertà nella rete*, cit., spec. 46-50.

ove la persona ha da sempre assunto una posizione dominante rispetto all'architettura complessiva delle garanzie, certamente anche nella prospettiva inversa e per lo più limitante dei doveri.

Tuttavia, il cammino universalizzante dei diritti fondamentali, collocati finanche al di là dei singoli ordinamenti, divenuti con il tempo patrimonio comune e intangibile dell'umanità, anteriori e precedenti al riconoscimento degli Stati[162], si arresta, anzi arretra nel Metaverso, ove la persona virtuale non riceve il medesimo tipo di tutela riservatele nella realtà umana. Non si tratta, come accade tra ordinamenti diversi, di una disciplina differenziata del nucleo duro di ogni singolo diritto individuale, quanto piuttosto di uno sconfinamento unilaterale del diritto di iniziativa economica e della proprietà, in assenza di qualsivoglia collegamento tra l'ordinamento costituzionale e convenzionale (europeo e internazionale) con il mondo sregolato del "Meta-Stato" digitale.

Così, mentre nella realtà umana i diritti fondamentali traggono tutela anche in atti sovra-statali come i Trattati internazionali, le Convenzioni dei diritti che impegnano lo Stato nei confronti degli altri Stati nella disciplina di materie sensibili e legate alla salvaguardia dei diritti umani inviolabili (la tutela dei minori, la tutela dei disabili, dei soggetti disagiati), la tutela nel "Meta-Stato" non riconosce situazioni soggettive ai singoli appartenenti a quell'ordinamento di natura prettamente economica, ma vincola esclusivamente i corpi virtuali, sulla base di meri patti negoziali, alle logiche del mercato, alla ricerca spasmodica del profitto, a tenere determinati comportamenti per salvaguardare le posizioni dominanti assunte dai «sovrani con la corona di silicio»[163] che muovono i corpi virtuali come pedine in uno scacchiere, ne traggono benefici, e per questo tendono a conservare una legittimazione autonoma e diretta a non far emergere le situazioni soggettive di garanzia individuali.

Dopotutto, è marcatamente percepibile come le condotte giuridicamente rilevanti, in particolare tutte quelle che si pongono in direzione ostinata e contraria ai pilastri dell'art. 2 Cost., sedimentate anche al di fuori della realtà aumentata, con il fine specifico di travolgere l'uomo attraverso straordinarie raffigurazioni utopistiche, restino ancora legate ad una concezione tradizionale delle categorie classiche dei presidi civili e penali codificati nel secolo scorso e in parte adattati al digitale.

Ora, la permanente vitalità[164] dimostrata dall'art. 2 Cost. ha consentito di tradurre le riflessioni tradizionali, proposte da quella dottrina dalla quale abbiamo ereditato solide basi epistemologiche, per uno *screening* preliminare di ciò che può porsi dentro o fuori il perimetro costituzionale. Se potevano già annebbiarsi dubbi e perplessità sulla forza solidale dei doveri come argine «all'espansione delle situazioni di interesse individuale»[165], in un'epoca nella quale i bisogni e le aspirazioni individualistiche non erano poi così diffuse, il Metaverso concretizza la preoccupazione di una propagazione illimitata non tanto del potere pubblico, quanto privato e di natura economica.

---

[162] Secondo N. Bobbio, *L'età dei diritti*, Torino, 2014, XII, «i diritti fondamentali nascono come diritti naturali, si sviluppano come diritti costituzionali e si dirigono verso la meta dei diritti universali».

[163] A. Venanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, cit., 1.

[164] Parla di «carica innovativa», D. Tega, *Articolo 2*, cit., 22.

[165] A. Barbera, *Art. 2*, cit., 101.

Si pongono, insomma, preoccupazioni in parte diverse e in parte nuove rispetto a quelle poste dal costituzionalismo come limite al potere statuale. Nel Metaverso viene infatti rovesciata l'impostazione di fondo dell'art. 2 Cost. e di tutti quei diritti che da esso promanano. L'inviolabilità stessa, come qui rilevato, è un concetto incoerente con l'impostazione di una società virtuale incatenata in una continua ascesa verso il profitto: le libertà sono funzionalizzate per nulla allo sviluppo della persona, piuttosto al rafforzamento di un regime oligopolistico volto alla massimizzazione del benessere economico di pochi; i valori democratici regrediscono e l'ordine istituzionale non è retto dai doveri di solidarietà politica, economica e sociale.

Insomma, il corpo virtuale rimane impotente innanzi ad un potere illimitato e sregolato, benché sembri quasi non percepirlo, anzi lo accetta nel momento in cui apre la porta dei mondi virtuali: cede i propri diritti a mezzo di un accordo negoziale senza sottoscriverlo, ma semplicemente "flaggando" il consenso all'utilizzo spasmodico dei propri diritti inviolabili, eradicando da essi le caratteristiche di inalienabilità, assolutezza, irrinunciabilità, indisponibilità, imprescrittibilità. Vittima e complice di un processo di trascendenza di un corpo che diventa personalità "altra", fuori il controllo umano, piegato irreversibilmente alle dure logiche del profitto, in una dimensione in cui la sovranità (anche monetaria)[166] non appartiene né allo Stato e né al popolo, piuttosto a poteri occulti non identificabili se non dietro a nomi di fantascienza (*Roblox*, *Decentraland*, *MetaUtopia*, ecc.) che celano «una combinazione agghiacciante e poderosa di impalpabilità e onnipotenza, non-fisicità e potere di determinare la realtà»[167]. Si tratta, insomma, di uno spazio ancor più «aterritoriale»[168] di quello fino ad oggi conosciuto dalla rete che ormai possiamo definire, quasi paradossalmente, "tradizionale", per la definitiva «eclissi della sovranità statale, sia perché gli Stati nazione [appaiono] "*too big, too slow, and too geographically and technically limited to regulate a global citizenry's fleeting interactions over mercurial medium*"[169] , sia perché il cyberspazio [è] utilizzato dai poteri economici per slegarsi dai limiti territoriali su cui si fondano i modelli tradizionali di government»[170].

L'errore degli Stati è stato sin dal principio quello di «fare affidamento sulle magnifiche sorti progressive che la Rete e i suoi signori sarebbero [stati] in grado di garantire, [sottovalutando] la garanzia degli interessi dei cittadini che gli ordinamenti giuridici statali, ancorché offuscati, sono in grado di apprestare mercé la loro concreta attribuzione e attuazione»[171].

In definitiva, squarciate le fondamenta dell'architettura complessiva sulla quale si reg-

---

[166] che da sempre ha costituito la premessa indispensabile per l'esercizio degli istituzionali compiti di iniziativa e di direzione della politica economica. Invece, anche su questo aspetto, i *Metaversi* vivono su monete elettroniche auto-coniate. B. Inzitari, *La moneta*, in B. Inzitari - G. Visentini - A. Di Amato, *Moneta e valuta*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Padova, 1983, 6.

[167] Z. Bauman, *Globalization. The Human Consequences*, New York, 1998, trad. it. *Dentro la globalizzazione. Le conseguenze sulle persone*, Roma-Bari, 1999, 23.

[168] Ho attualizzato, perché mi sembra coerente, il pensiero di M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, in *Rivista Gruppo di Pisa,* 2, 2021, 168.

[169] J. Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, in *University of Cincinnati Law Review*, 66, 1997, 177.

[170] M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, cit., 170.

[171] *Ibidem*.

gono i diritti fondamentali, e venuto meno il ruolo di garanzia dell'autorità statale che non riesce, ad oggi, a porsi come un vero e proprio contro-potere nei confronti dei "Meta-Stati", può considerarsi il Metaverso, con un sufficiente grado di certezza, uno dei luoghi meno ameni per il costituzionalismo tradizionale, un girone infernale per l'uomo che non è più uomo e nel quale la sua identità, la sua autodeterminazione, la sua dignità, sono continuamente violate in nome di una società disposta ad immolare, in nome del bieco profitto, le storiche guarentigie della persona in quanto tale.

In un contesto di grande sviluppo e di grande espansione dei diritti e dei giudici, di Carte e Corti chiamate a tutelarli, il Metaverso si colloca in una fase di «dismissione del reale»[172], avulsa dalla «moltiplicazione dei diritti»[173], caratterizzato per oscurità e ambiguità che conducono ad una rarefazione del contenuto delle garanzie e, dunque, alla difficoltà di applicarle in un futuro ordinamento virtuale[174].

In tale dimensione tecnologica di «smaterializzazione della relazione»[175], dove la «trama del potere»[176] si incunea nei meandri più reconditi della società, va recuperata nella sua interezza la persona, dalla quale promanano i diritti fondamentali da rivendicare anche nel Metaverso, attraverso una rilettura, in chiave digitale se necessario, di alcune categorie giuridiche.

Non è scontato sostenere che un contesto del genere obblighi lo Stato a provvedere[177], andando in contro, diversamente, ad uno svuotamento della solidarietà come conseguenza ineludibile della rarefazione dell'inviolabilità dei diritti collocati nella realtà immersiva, e al definitivo abbandono della sovranità, in un territorio in cui l'uomo diviene suddito di «sovrani dalla corona di silicio»[178].

Il diritto deve prendere posizione, guardare oltre il proprio destino[179] rispetto ad uno scenario enigmatico, rileggendo le categorie giuridiche tradizionali come l'inviolabilità, la solidarietà, la responsabilità, l'identità personale, l'autodeterminazione, comprendere fino a che punto "l'io è padrone in casa propria" quando viene stilata un'identità inumana, collocata nella dimensione del virtuale attraverso logiche inusuali e tecniche completamente diverse.

Come può il legislatore, attraverso l'art. 2 Cost., riprendere il filo interrotto della «garanzia degli spazi individuali di libertà, messi in discussione anche dall'avvento di nuo-

172 E. Mazzarella, *Contro Metaverso*, cit., 29.

173 N. Bobbio, *L'età dei diritti*, cit., 6.

174 Diversi aspetti erano stati già segnalati da M.C. De Vivo, *Viaggio nei metaversi alla ricerca del diritto perduto*, in *Informatica e diritto*, XXXV annata, vol. XVIII, 1, 2009, 191 ss.

175 E. Mazzarella, *Contro Metaverso*, cit., 63.

176 F. Paruzzo, *I sovrani della rete. Piattaforme costituzionali e limiti al potere privato*, cit., 107.

177 La Corte costituzionale, in relazione al principio di solidarietà, ha chiarito che la promozione è «un compito che coinvolge l'intera comunità nazionale e che, pertanto, dev'essere congiuntamente perseguito, nel rispetto delle correlative competenze costituzionali, dallo Stato, dalle Regioni e dalle Province autonome» (sent. 202/1992). Nello stesso senso, A. Apostoli, *La svalutazione del principio di solidarietà*, cit. e F. Giuffrè, *La solidarietà nell'ordinamento costituzionale*, Milano, 2002.

178 A. Venanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, cit., 9.

179 J. Offray de La Mettrie, *L'uomo macchina*, cit., 69, si chiedeva «cosa sappiamo del nostro estino più di quanto non conosciamo della nostra origine?».

ve tecnologie»[180]? Qual è l'approdo della riflessione da avviare sull'esercizio dei diritti di "quinta generazione", «affinché l'ordinato vivere comune sia salvaguardato e i pesi conseguenti siano equamente ripartiti tra tutti, senza privilegi»[181], in una realtà, come quella immersiva, nella quale tutti gli immigrati digitali non «ricevono diritti [ma] restituiscono doveri»[182]? In che modo è possibile risvegliare quel sentimento solidaristico orizzontale che dovrebbe animare la persona come individuo responsabile anche nei confronti dei suoi pari, a prescindere dalla condizione umana o virtuale, emergendo dalla trincea del mondo parallelo, dove la Costituzione vivente (anzi, morente) viene relegata?

Rispetto ad un discorso incentrato sul riconoscimento di diritti fondamentali di natura digitale, il diritto stesso non può perdere la funzione di stabilizzazione, ma deve attribuire alle nuove dinamiche una forma di tutela, la cui manifestazione più intensa non riesce ancora ad essere misurata per essere fortemente instabile e caratterizzata da sovrastrutture (*blockchain*, criptovalute, *asset*) parimenti instabili.

In primo luogo, va riaperta una riflessione seria che coinvolga ogni aspetto riguardante l'autonomia della persona in termini di autodeterminazione[183], in un contesto nel quale certe situazioni non possono essere più valutate attraverso criteri pre-tecnologici.

In secondo luogo, a fronte di una proliferazione straordinaria di Carte dei diritti, sono maturi i tempi per ragionare sui doveri da riservare a chi detiene il potere nei mondi virtuali, a quei soggetti non direttamente percepibili nella realtà umana, ma esistenti, presenti e persistenti, che governano le vite, plasmano la persona umana attraverso un processo di "esomatizzazione" nel corpo virtuale. Tali soggetti hanno dei doveri nei confronti della persona (umana e virtuale) e, perché no, anche nei confronti dello Stato: il dovere di preservare quello che è il patrimonio attuale dell'uomo, il nucleo duro dei diritti inviolabili, senza distruggerlo.

Di qui l'opportunità di porre allo studio non più una Carta dei diritti, piuttosto una Carta dei doveri nei confronti di chi è impalpabile, ma che sappiamo esiste e sarà sempre più presente nel tempo, volta a spezzare dal basso quel legame utente/piattaforma ogni volta in cui vi è anche la sola percezione del pericolo di una aggressione ai diritti fondamentali. L'apposizione di obblighi e divieti molto più stringenti – anche ai corpi che aspirano a divenire digitali – è imprescindibile, da un lato, per la difficoltà ad individuare i soggetti umani che si celano dietro ai "Multiversi", dall'altro per garantire la stessa persona, anticipandone la tutela in un momento precedente al travolgimento della stessa nel buco nero della realtà immersiva.

La realizzazione di una Carta dei doveri – a partire, in virtù della competenza assegnata all'Unione europea, dal pacchetto digitale[184] – volta a regolare gli «intermediari

[180] Ammoniva così già A. Barbera, *Art. 2*, cit., 91.

[181] Corte cost., sent. 43/1997.

[182] Corte cost., sent. 172/1999.

[183] Su cui, già A. Papa, *La problematica tutela del diritto all'autodeterminazione informativa nella big data society*, in *Liber amicorum per Pasquale Costanzo*, in *Consulta on line*, 17 aprile 2020, 1 ss.

[184] *European Digital Strategy, Shaping Europe's Digital Future*, volto alla tutela dei diritti degli utenti nelle piattaforme di mercati digitali, tra cui il Digital Services Act e il Digital Market Act, applicabili ai servizi di intermediari online, di contenuti, prodotti e servizi, messi a disposizione di terzi. Su questi aspetti, O. Pollicino - G. De Gregorio, *L'alba di nuove responsabilità sulle piattaforme digitali: il Digital Services Act*, in

digitali»[185] che oggi tentano in ogni modo e con condotte imprudenti di sfuggire ai controlli[186] – assumendo una posizione di riluttanza verso doveri di solidarietà e ordine morale che sarebbe auspicabile possano divenire giuridici – è la condizione imprescindibile per impedire ai Metaversi di strutturarsi come veri e propri "far west virtuali", in cui la cortina di «incomunicabilità tra diritto pubblico e diritto privato»[187] rappresenta la definitiva negazione dei diritti fondamentali.

Questa è la prossima sfida. Una sfida che è, in parte, un lascito della pandemia. Questo sarà (o, per certi versi, già è) il Metaverso che non può prescindere dal riconoscimento e dalla garanzia di doveri e "diritti di quinta generazione" riletti in una dimensione, per così dire, «cybercostituzionale»[188], non preclusa dalla Costituzione[189] e verso cui il diritto e le istituzioni non possono continuare ad essere così distanti e indifferenti, avendo il dovere di preservare il patrimonio di diritti «eterni, sacri, innati, originari, essenziali»[190] per consentirne il pieno godimento senza permettere ad interessi privatistici di distruggerlo.

Agenda Digitale, 15 dicembre 2020 e O. Pollicino, *Verso una democrazia digitale europea con meno opacità*, in *IlSole24Ore*, 24 dicembre 2020, O. Pollicino - G. De Gregorio - M. Bassini, *Verso il Digital Services Act: problemi e prospettive. Presentazione del simposio*, in *medialaws.eu*, 23 novembre 2020, G. Contaldi, *Il DMA (Digital Markets Act) tra tutela della concorrenza e protezione dei dati personali*, cit., 293. Secondo M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, in *Rivista Gruppo di Pisa*, 2, 2021, spec. 179-182.

[185] L'espressione è di F. Paruzzo, *I sovrani della rete. Piattaforme costituzionali e limiti al potere privato*, cit., 121 ss.

[186] Si tratta, per vero, di una impostazione tipica del mondo digitale che si vuole scevro da ogni controllo, governato da una *Lex Informatica* speciale, caratterizzato da un intervento statale al massimo sussidiario. In tal senso, cfr. J.R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Review*, 1998, 553 ss.

[187] A. Barbera, *Art. 2*, cit., 69 che richiama le pagine di S. Rodotà, *Ipotesi sul diritto privato*, in *Diritto privato della società moderna*, 1970, 9 ss.

[188] A. Venanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, cit., 5 ss.

[189] In questo senso, benché in una prospettiva classica, nella quale è stato dimostrato che i diritti non devono essere esclusivamente garantiti da un'autorità pubblica, G. Lombardi, *Potere privato e diritti fondamentali*, Torino, 1970, 94, ma anche, in chiave digitale, S. Rodotà, *Una Costituzione per Internet?*, in *Pol. Dir.*, 3, 2010. Recentemente, nella prospettiva di riconoscimento della *lex digitalis*, G. Azzariti, *Internet e Costituzione*, in *Costituzionalismo.it*, 2, 2011.

[190] A. Barbera, *Art. 2*, cit., 81.

Libertà d'impresa e diritto alla protezione dei dati personali*

Raffaele Torino

Abstract

La libertà d'impresa (o libertà di iniziativa economica) e il diritto alla protezione dei dati personali costituiscono due diritti fondamentali riconosciuti a livello europeo e nazionale, ma che possono venire in contrapposizione nel contesto della regolamentazione del mercato unico digitale e del concreto declinarsi dell'esercizio di entrambi. Il necessario bilanciamento di questi due diritti fondamentali – nessuno dei quali può essere considerato assoluto e apoditticamente prevalente a priori sull'altro - richiede una attenta e approfondita analisi delle caratteristiche di entrambi questi diritti, del loro reciproco valore assiologico e dei molteplici interessi sottesi ad entrambi.

The freedom to conduct business and the right to the protection of personal data are two fundamental rights recognized at both the European and national levels, but they can come into conflict within the context of the rules governing the Digital Single Market and the implementation of both rights. The necessary balance of these two fundamental rights - neither of which can be considered absolute and unequivocally prevailing over the other - requires a careful and thorough analysis of the specific characteristics of both these rights, their mutual axiological value, and the multiple interests underlying both.

Sommario

1. Introduzione – 2. La libertà d'impresa quale diritto fondamentale – 2.1. La libertà d'impresa nella giurisprudenza della Corte di giustizia – 3. La protezione dei dati personali quale diritto fondamentale – 4. Osservazioni finali

Keywords

libertà d'impresa - diritti fondamentali - dati personali – consenso – legittimo interesse

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1. Introduzione

Nei luoghi digitali, dalle reti di comunicazioni elettroniche alle *social platform*, per giungere ai nuovi spazi creati dai metaversi, si intrecciano e si confrontano quotidianamente gli interessi delle imprese dell'economia digitale e degli utenti digitali, alla ricerca di un equilibrato bilanciamento che ne consenta la proficua coesistenza[1].

Se l'interesse delle imprese dell'economia digitale – come di tutti gli operatori economici professionali – è ordinariamente e legittimamente quello di massimizzare il profitto derivante dalla propria attività imprenditoriale, l'interesse degli utenti digitali è anzitutto quello di poter usufruire dei servizi e contenuti digitali offerti online, pienamente beneficiando anche in tale ambito dei diritti fondamentali riconosciuti a ogni persona fisica, secondo il contesto normativo ricostruito dagli studi di *Digital Constitutionalism*[2].

Tale situazione vede porre (sebbene non sulla base di un dato legislativo) in maniera solitamente antagonista, sotto il profilo delle libertà e dei diritti che conformano giuridicamente le relazioni che si svolgono online, da una parte, una libertà ampiamente (quantunque variamente) riconosciuta nei sistemi giuridici occidentali agli operatori economici professionali, ossia la libertà di impresa (*freedom to conduct business* o, per stare alla Costituzione italiana, la libertà di iniziativa economica) e, dall'altra parte, la protezione dei dati personali quale diritto fondamentale per come progressivamente emerso nella *Weltanschauung* della regolamentazione che innerva la specifica area del processo di integrazione europea che oggi in senso ampio possiamo ricondurre al Mercato Unico Digitale.

La relazione fra libertà d'impresa (una libertà presente sin dall'origine del processo di integrazione europea) e diritto alla protezione ai dati personali (un diritto fondamentale di più recente apparizione) appare da subito complicata (in ragione dei molteplici elementi da prendere in considerazione) e complessa (in ragione delle molteplici interazioni fra questi elementi, non sempre immediatamente decifrabili), specie ove considerata nel contesto di quella che resta la pietra angolare del processo di integrazione europea, ossia la creazione del mercato unico e, nello specifico, del già richiamato mercato unico digitale[3].

Nell'ambito del decennio digitale europeo, tale relazione deve essere necessariamente conforme alla "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale" (2023/C 23/01) e, conseguentemente, parte coerente di «un modello europeo per la trasformazione digitale, che metta al centro le persone, sia basato sui valori europei e sui diritti fondamentali dell'UE, riaffermi i diritti umani universali e apporti benefici a tutte le persone, alle imprese e alla società nel suo complesso».

---

[1] O. Pollicino - G. De Gregorio, *The Quest for Balancing Rights in the Digital Age: Perspectives from the Metaverse*, in *medialaws.eu,* 27 aprile 2023; G Pino, *Conflitto e bilanciamento fra diritti fondamentali. Una mappa dei problemi*, in *Etica&Politica*, 2006, 1.

[2] O. Pollicino, *Potere digitale*, in *Enciclopedia del* diritto, *I tematici*, 2023, in M. Cartabia - M. Rutolo (diretto da), *Potere e Costituzione*, Milano, 410; O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. European and Constitutional perspectives*, Oxford, 2021; G. De Gregorio, *Digital Constitutionalism in Europe*, Cambridge, 2022.

[3] F. Ferri, *Il bilanciamento dei diritti fondamentali nel mercato unico digitale*, Torino, 2022.

Per altro verso, da un lato, il considerando 4 del RGPD riconosce che il diritto alla protezione dei dati personali non è una prerogativa assoluta, che tale diritto va considerato alla luce della sua funzione sociale e va contemperato – seguendo il principio di proporzionalità – con altri diritti fondamentali (fra cui viene espressamente menzionata la libertà d'impresa)[4]; dall'altro lato, anche la libertà d'impresa non rappresenta una prerogativa assoluta e può subire limitazioni di fronte all'esigenza di proteggere i diritti altrui, secondo l'insopprimibile principio di proporzionalità.

Ora, sembra generalmente acquisita ed accettata nel ragionamento degli interpreti la prevalenza assiologica del diritto alla protezione dei dati personali (in quanto diritto della personalità) sulla libertà d'impresa (in quanto libertà di stampo economico).

Infatti, sulla scorta di riflessioni sviluppate in passato anzitutto rispetto al diritto di proprietà, torna utile rammentare la distinzione (dal forte impatto valoriale) proposta in dottrina fra "diritti fondamentali inviolabili" (quelli della persona) e diritti fondamentali non corredati dall'attribuito della inviolabilità (in cui rientrerebbero la proprietà e l'iniziativa economica privata). I primi sarebbero posti a fondamento dello Stato, di uno Stato di diritto e democratico[5], i secondi sarebbero tali da imprimere allo Stato di diritto una specifica fisionomia. In maniera analoga, secondo una ricostruzione più recente, è stata proposta la articolazione dell'inviolabilità dei diritti in inviolabilità "in senso stretto" (riferibile ai soli diritti della persona) e inviolabilità "in senso ampio" (da riferirsi alla proprietà e alla libera iniziativa economica privata)[6].

Seguendo questa linea di pensiero, in via generale, mentre il diritto alla protezione dei dati personali appare essere assistito da una inviolabilità forte, alla libertà di impresa viene invece riconosciuta una inviolabilità maggiormente permeabile e, dunque, in qualche modo affievolita.

La distinzione e conseguente diversità di valore assiologico fra diritti fondamentali e libertà economiche ha già generato (sebbene nel contesto assai peculiare dei diritti sociali e del diritto di sciopero) lo specifico quesito se esista un rapporto gerarchico fra i diritti fondamentali (che valgono in quanto principi generali del diritto europeo) e le quattro libertà economiche fondamentali sancite nei Trattati (v. le conclusioni dell'Avvocato generale Stix Hackl nella causa C-36/02, § 48)[7]. A tal quesito è stata data una risposta tutto sommato generica e non risolutiva dall'Avvocato generale; egli ha infatti affermato che le libertà economiche fondamentali andrebbero interpretate «quanto più possibile nel senso di non consentire alcun provvedimento che ecceda i

[4] Il considerando 4 del RPGD recita: «(4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

[5] E. Navarretta, *Libertà fondamentali dell'U.E. e rapporto fra private: il bilanciamento di interessi e I rimedi civilistici*, in *Rivista Diritto Civile*, 2015, 894.

[6] A. Baldassarre, *Diritti inviolabili*, in *Enciclopedia Giuridica Treccani*, Roma, 1989, 23.

[7] S.A. de Vries, *Balancing Fundamental Rights with Economic Freedoms According to the European Court of Justice*, in *Utrecht Law Review*, 2013, 169.

limiti di un intervento lecito sui diritti fondamentali in questione e di non permettere quindi alcuna misura che non si concili con i diritti fondamentali» (Conclusioni causa C-36/02, § 56)[8].

In tale contesto, se non appare contestabile (e non è desiderabile che sia contestato) l'impostazione di fondo dei sistemi giuridici europei secondo cui la dignità umana è valore primario e insuperabile, principio cardine dell'intera architettura dei diritti fondamentali, da cui si fa discendere la primazia dei diritti della personalità sulle libertà economiche, appare lecito interrogarsi – al fine di una corretta ed equilibrata analisi del rapporto fra la libertà d'impresa e il diritto alla protezione dei dati personali, nonché del loro necessario bilanciamento nel rispetto del principio di proporzionalità – se il diritto a proteggere (forse sarebbe più corretto dire il diritto a controllare – nel senso di governare – i propri dati personali, secondo i principi della c.d. "*user freedom*") si collochi al medesimo livello valoriale degli altri diritti della personalità.

Così come, pur mantenendo fermo il superiore gradiente assiologico del diritto alla protezione dei dati personali, non risulta altrettanto chiaro come questo superiore valore assiologico debba concretamente declinarsi. Una via percorribile appare essere quella per cui sarebbe il RGPD – con i suoi principi (anzitutto quelli di cui all'art. 5), le sue indicazioni di dettaglio e i suoi procedimenti e percorsi – a dover fornire gli strumenti all'interprete (ed al titolare del trattamento) per individuare il 'nucleo essenziale' della protezione dei dati personali. Tale nucleo essenziale, tuttavia, non può essere apoditticamente individuato invocando una generica ed assoluta indisponibilità dei diritti del soggetto interessato, pena una ingiustificata eliminazione di qualsiasi considerazione della libertà d'impresa e la rinuncia a qualsivoglia processo di bilanciamento fra quest'ultima e il diritto alla protezione dei dati personali, che non rappresenta per certo un "diritto tiranno".

Assumendo tale punto di vista, va tenuto in debita rilevanza che il diritto alla protezione dei propri dati personali risulta essere costituito – anzitutto per il soggetto interessato - da un "fascio di diritti" (il diritto di accesso, il diritto di rettifica, il diritto alla cancellazione o c.d. "diritto all'oblio", il diritto di limitazione del trattamento, il diritto alla portabilità dei dati, il diritto di opposizione, il diritto di non essere sottoposto a decisioni automatizzate, il diritto di presentare reclami all'autorità di controllo), rispetto a ciascuno dei quali il rapporto di prevalenza assiologica rispetto alla libertà di impresa può assumere inevitabilmente connotati differenziati, sì da assicurare – nella prevalenza dello specifico diritto di protezione dei dati personali - la minore possibile incidenza su tale antagonista libertà.

Infine, sempre per stare nel perimetro del RGPD, merita di essere approfondito il profilo del legittimo interesse del titolare (o di terzo) quale presupposto di legittimità del trattamento dei dati personali. Ci si potrebbe, infatti, chiedere se – a fronte di una possibile apertura alla considerazione dei dati personali come oggetto di controprestazione (v. la direttiva (UE) 2019/770 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali[9]) – la libertà d'impresa rispetto al

[8] E. Navarretta, *Libertà fondamentali dell'U.E. e rapporti tra privati: il bilanciamento di interessi e rimedi civilistici*, cit., 878

[9] E.M. Tripodi, *Consumi digitali e dati personali*, in (a cura di) Torino R., *I diritti dei consumatori digitali. I*

trattamento dei dati personali del consumatore/utente non recuperi (almeno in parte e/o con dei limiti) una parità assiologica (o, quanto meno, un "riavvicinamento valoriale") proprio sotto il profilo del legittimo interesse dell'impresa a perseguire i suoi obiettivi di profitto[10].
Per rispondere ai sopra menzionati quesiti, vanno anzitutto ricostruiti i connotati di fondo della libertà d'impresa nel diritto europeo.

2. La libertà d'impresa quale diritto fondamentale

Alla libertà di impresa o alla libertà di iniziativa economica i Trattati originari non fanno riferimento. Occorrerà, infatti, attendere la Carta dei diritti fondamentali dell'UE (di seguito, la 'Carta') per vedere un suo riconoscimento esplicito da parte di uno dei testi costituzionali europei della libertà di impresa.
Tuttavia, non può essere revocato in dubbio – dal complesso dell'evoluzione del processo di integrazione europea, sotto tutti i profili (politici, normativi e giurisprudenziali) – che, nella misura in cui l'Unione europea si fonda su un'economia di libero mercato[11], la libertà d'impresa costituisca uno dei cardini della Costituzione economica europea sin dai primordi, rappresentandone indubbiamente uno dei principi generali[12].
Tale affermazione risulta inizialmente confortata dalla (invero non numerosa) giurisprudenza in termini della Corte di giustizia dell'Unione europea che, nel contesto della tutela dei diritti fondamentali (in quanto principi generali del diritto comunitario) per come riconosciuti dalle tradizioni costituzionali comuni agli Stati membri, ha affermato che il «libero esercizio del commercio, del lavoro e di altre attività economiche» godono di tutela analoga al fondamentale diritto di proprietà (*Nold*, 4/73, § 14).
Per altro verso, in questa giurisprudenza della corte europea, si è da subito precisato che la libertà d'impresa non costituisce una prerogativa assoluta e che – ferma la sostanza della medesima – essa può subire limitazioni[13].
Sicché, il riconoscimento della libertà d'impresa quale diritto fondamentale da parte dell'art. 16 della Carta (come affermato dalle Spiegazioni della Carta) si è basato sulla giurisprudenza della Corte di giustizia che ha da sempre riconosciuto la libertà di esercitare un'attività economica e commerciale e la libertà contrattuale, nonché sull'art. 119

contratti di fornitura di contenuti e servizi digitali e di beni con elementi digitali, Pisa, 2023, 267.

[10] F. V. Bravo, *Il "diritto" a trattare i dati personali nello svolgimento dell'attività economica*, Padova, 2018.

[11] C. Malberti, *commento all'art. 16*, in (a cura di) R. Mastroianni - O. Pollicino - S. Allegrezza - F. Pappalardo - O. Razzolini, *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, 308.

[12] A. Usai, *The Freedom to Conduct a Business in the EU, Its Limitation and Its Role in the European Legal Order: A New Engine for Deeper and Stronger Economic, Social, and Political Integration*, in *German Law Journal*, 2013, 1867.

[13] CGUE, 4/73, *J. Nold, Kohlen- und Baustoffgroßhandlung contro Commissione delle Comunità europee* (1973), § 14: «[n]ell'ordinamento giuridico comunitario, appare legittimo sottoporre tali diritti a taluni limiti giustificati dagli obiettivi d'interesse generale perseguiti dalla Comunità, purchè non resti lesa la sostanza dei diritti stessi. Per quanto riguarda in particolare la tutela dell'impresa, non la si può comunque estendere alla protezione dei semplici interessi o possibilità d'indole commerciale, la cui natura aleatoria è insita nell'essenza stessa dell'attività economica». CGUE, C-351/99, *Eridania* (2001); CGUE, C-44/79, *Hauer* (1979), § 32.

del TFUE che riconosce la libera concorrenza[14]. La libertà d'impresa ha in tal modo trovato collocazione nel Titolo II della Carta, dedicato alle "Libertà", incastonata fra la libertà professionale e il diritto di lavorare (art. 15) e il diritto di proprietà (art. 18), con cui presenta dei punti di contatto che ne possono influenzare l'interpretazione[15].
Sotto il profilo meramente testuale va osservato che, mentre negli altri articoli del "Titolo II – Libertà" i diritti o le libertà sono nettamente affermati o vietati, la libertà d'impresa è (più semplicemente?) riconosciuta; il che è probabilmente da attribuirsi alla circostanza che essa è da sempre intesa come una libertà che si deve confrontare con il diritto dell'Unione e le legislazioni e prassi nazionali, nell'ambito di una relazione dialettica (e, dunque, da bilanciare) fra diversi diritti (e finanche con prassi nazionali). Infatti, oltre ai limiti generali (applicabili a tutti i diritti e libertà affermati o riconosciuti dalla Carta in forza dell'art. 52 della Carta medesima), la libertà d'impresa trova espliciti e specifici limiti nel Diritto dell'Unione (riferimento da intendersi non solo ai Trattati, bensì anche a tutto il diritto derivato e al diritto europeo di formazione giurisprudenziale) e nelle legislazioni e prassi nazionali (il che appare porre da subito il problema di un riconoscimento differenziato sulla base dei singoli sistemi giuridici nazionali).
Sebbene in alcune decisioni i giudici europei non siano stati particolarmente analitici nell'eseguire l'operazione di bilanciamento, da come risulterà in dettaglio nel paragrafo successivo (par. 2.1), si può anzitutto osservare che libertà d'impresa riconosciuta dall'art. 16 della Carta, nella misura in cui è stato più volte ribadito che essa non costituisce una prerogativa assoluta e che la sua tutela dipende dalla sua funzione della società rispetto al contesto concreto in cui è invocata, subisca maggiori o minori compressioni in relazione al diritto fondamentale con cui è chiamata a confrontarsi. Tale maggiore o minore compressione deve ovviamente avvenire nel rispetto – da parte di tutti i soggetti coinvolti – anzitutto di garanzie procedurali e senza sopprimerne irrimediabilmente il suo nucleo essenziale.
Per quanto concerne le garanzie procedurali, le limitazioni alla libertà d'impresa devono essere previste dalla legge e devono rispettare il principio di proporzionalità, ossia essere necessarie e rispondere effettivamente: (*i*) a finalità di interesse generale riconosciute dall'UE; o, in alternativa, (*ii*) all'esigenza di proteggere i diritti e le libertà altrui.
Con riferimento all'esistenza di un nucleo essenziale della libertà d'impresa che le predette limitazioni non possono intaccare, può essere sin d'ora anticipato che finanche detto nucleo essenziale assume un perimetro variabile a seconda dell'interesse generale o del diritto/libertà con cui la libertà d'impresa viene posta in competizione e che, in ultima istanza, esso appare riconducibile alla insopprimibile necessità che l'attività imprenditoriale non sia del tutto impedita o soppressa e che l'imprenditore conservi la necessaria autonomia decisionale nell'impiego delle proprie risorse, non venendo ad essere sottoposto a insostenibili perdite economiche che ne possano compromettere l'esistenza.

[14] Art. 16 della Carta: «È riconosciuta la libertà d'impresa, conformemente al diritto dell'Unione e alle legislazioni e prassi nazionali».

[15] X. Groussot - G.T. Petursson - J. Pierce, *Weak Right, Strong Court – The Freedom to Conduct Business and the EU Charter of Fundamental Rights,* Lund University Research Paper, 2014.

2.1 La libertà d'impresa nella giurisprudenza della Corte di giustizia

Un settore in cui la libertà d'impresa è stata più volte evocata è certamente quello della tutela della proprietà, segnatamente della proprietà intellettuale. In tale ambito vanno rammentati i casi *Scarlet Extended* (C-70/10), *Sabam* (C-360/10), *Sky Österreich* (C-283/11) e *UPC Telekabel Wien* (C-314/12).

Nel caso *Scarlet Extended* (deciso nel novembre 2011), nascente dal rifiuto della società Scarlet di predisporre un sistema di filtraggio delle comunicazioni elettroniche realizzate tramite programmi per lo scambio di archivi (*peer-to-peer*), richiesto al fine di impedire gli scambi dei file che ledono i diritti d'autore, i giudici europei hanno affermato la necessità di garantire «un giusto equilibrio tra la tutela del diritto di proprietà intellettuale, di cui godono i titolari di diritti d'autore, e quella della libertà d'impresa, appannaggio di operatori come i FAI»[16].

Nel caso *Sabam* (deciso nel febbraio 2012), analogo al caso *Scarlet Extended*, la Corte di giustizia ha ribadito la necessità di rintracciare il predetto "giusto equilibrio"[17]. Su tale presupposto è stato ritenuto che una ingiunzione di predisporre un sistema di filtraggio e sorveglianza sulla totalità o sulla maggior parte delle informazioni memorizzate presso il prestatore di servizi di hosting, illimitata nel tempo, riguardante qualsiasi futura violazione di opere esistenti e ancora da creare, avrebbe causato una grave violazione della libertà d'impresa[18].

Nel caso *Sky Österreich* (deciso nel gennaio 2013), relativo all'accesso da parte di una emittente televisiva al segnale satellitare di un'altra emittente televisiva al fine di realizzare brevi estratti di cronaca, la Corte di giustizia ha anzitutto riconosciuto che l'art. 15 della direttiva 2010/13 (direttiva sui servizi di media audiovisivi[19]) «costituisce un'inge-

[16] CGUE, C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL* (2011), § 46: «le autorità ed i giudici nazionali devono in particolare garantire un giusto equilibrio tra la tutela del diritto di proprietà intellettuale, di cui godono i titolari di diritti d'autore, e quella della libertà d'impresa, appannaggio di operatori come i FAI [n.d.r. Fornitore di Accesso a Internet] in forza dell'art. 16 della Carta». È stato, quindi, deciso che «l'ingiunzione che costringe il FAI a predisporre il sistema di filtraggio controverso, il giudice nazionale in questione non rispetterebbe l'obbligo di garantire un giusto equilibrio tra, da un lato, il diritto di proprietà intellettuale e, dall'altro, la libertà di impresa, il diritto alla tutela dei dati personali e la libertà di ricevere o di comunicare informazioni» (§ 53).

[17] CGUE, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (2012), § 44: «le autorità ed i giudici nazionali devono, in particolare, garantire un giusto equilibrio tra la tutela del diritto di proprietà intellettuale, di cui godono i titolari di diritti d'autore, e quella della libertà d'impresa, di cui beneficiano operatori quali i prestatori di servizi di hosting in forza dell'articolo 16 della Carta».

[18] Ivi, § 46: «causerebbe, quindi, una grave violazione della libertà di impresa del prestatore di servizi di hosting, poiché l'obbligherebbe a predisporre un sistema informatico complesso, costoso, permanente e unicamente a sue spese, il che risulterebbe peraltro contrario alle condizioni stabilite dall'articolo 3, paragrafo 1, della direttiva 2004/48, il quale richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale non siano inutilmente complesse o costose». Dunque, l'ingiunzione richiesta nel caso di specie «non può considerarsi conforme all'esigenza di garantire un giusto equilibrio tra, da un lato, la tutela del diritto di proprietà intellettuale, di cui godono i titolari dei diritti d'autore, e, dall'altro, quella della libertà d'impresa, di cui beneficiano operatori come i prestatori di servizi di hosting».

[19] G. B. Abbamonte - E. Apa - O. Pollicino, *La riforma del mercato audiovisivo europeo*, Torino, 2019.

renza nella libertà d'impresa dei titolari dei diritti esclusivi di trasmissione televisiva» (§ 43), poiché impedisce a detti titolari di scegliere liberamente le proprie controparti contrattuali con cui concludere un accordo per la concessione del diritto di realizzazione di brevi estratti di cronaca e di decidere liberamente il prezzo a cui concedere tale diritto. Tuttavia anche in tale sede i giudici europei hanno ribadito che la libertà d'impresa non costituisce una prerogativa assoluta[20]. Distinguendo la libertà d'impresa dalle altre libertà di cui al Titolo II della Carta, essi hanno concluso affermando che «la libertà d'impresa può essere soggetta ad un ampio ventaglio di interventi dei poteri pubblici suscettibili di stabilire, nell'interesse generale, limiti all'esercizio dell'attività economica»[21]. A questo punto la Corte di giustizia ha affrontato il tema delle modalità con cui possono essere imposti limiti alla libertà d'impresa, anzitutto rammentando la necessità che venga rispettato quanto previsto dall'art. 52, par. 1, della Carta e che, dunque, ««qualsiasi limitazione all'esercizio dei diritti e delle libertà riconosciuti dalla Carta deve essere prevista per legge, deve rispettarne il contenuto essenziale e deve, nel rispetto del principio di proporzionalità, essere necessaria e rispondere effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui» (§ 48). Nello specifico, i giudici europei hanno rilevato che «l'articolo 15, paragrafo 6, della direttiva 2010/13 non incide sul contenuto essenziale della libertà d'impresa. Infatti, tale disposizione non impedisce l'esercizio dell'attività imprenditoriale stessa da parte del titolare di diritti esclusivi di trasmissione televisiva. Inoltre, essa non esclude che il titolare medesimo possa sfruttare i propri diritti effettuando egli stesso, a titolo oneroso, la ritrasmissione dell'evento di cui trattasi o, ancora, cedendo contrattualmente tale diritto, a titolo oneroso, ad un'altra emittente televisiva o a qualsivoglia altro operatore economico» (§ 49). Quanto al rispetto del principio di proporzionalità, la Corte di giustizia ha ricordato che quest'ultimo principio «esige, secondo costante giurisprudenza della Corte, che gli atti delle istituzioni dell'Unione non superino i limiti di quanto è opportuno e necessario al conseguimento degli scopi legittimamente perseguiti dalla normativa di cui trattasi, fermo restando che, qualora sia possibile una scelta tra più misure idonee, si deve ricorrere a quella meno restrittiva e che gli inconvenienti causati non devono essere sproporzionati rispetto agli scopi perseguiti (sentenze dell'8 luglio 2010, Afton Chemical, C-343/09, […] punto 45, nonché del 23 ottobre 2012, Nelson e a., C-581/10 e C-629/10, punto 71, nonché giurisprudenza citata)» (§ 50). In conclusione, i giudici di Lussemburgo hanno approvato che il legislatore europeo abbia privilegiato la libertà del pubblico di ricevere informazioni rispetto alla libertà d'impresa, ritenendo che «gli inconvenienti che discendono da tale disposizione [n.d.r.: l'art. 15 della Dir. 2010/13] non siano

[20] CGUE, C-283/11, *Sky Österreich GmbH v. Österreichischer Rundfunk* (2013), § 45: «conformemente alla giurisprudenza della Corte, la libertà d'impresa non costituisce una prerogativa assoluta, bensì deve essere presa in considerazione rispetto alla sua funzione nella società (v., in tal senso, sentenze del 9 settembre 2004, Spagna e Finlandia/Parlamento e Consiglio, C-184/02 e C-223/02 […] punti 51 e 52, nonché del 6 settembre 2012, Deutsches Weintor, C-544/10, punto 54 e giurisprudenza citata)».

[21] Ivi, § 46: «in considerazione del tenore dell'articolo 16 della Carta, che si distingue da quello relativo alle altre libertà fondamentali sancite nel titolo II della stessa pur essendo simile a quello di talune disposizioni del successivo titolo IV, la libertà d'impresa può essere soggetta ad un ampio ventaglio di interventi dei poteri pubblici suscettibili di stabilire, nell'interesse generale, limiti all'esercizio dell'attività economica».

sproporzionati rispetto agli scopi perseguiti e siano di natura tale da realizzare un giusto equilibrio tra i singoli diritti e le singole libertà fondamentali in gioco nella specie» (§ 67).

Nel caso *UPC Telekabel Wien* (deciso nel marzo 2014), riguardante un giudizio nazionale avente ad oggetto una domanda di ingiunzione diretta a bloccare l'accesso a un sito Internet che mette a disposizione del pubblico taluni film di alcune case produttrici cinematografiche senza il loro consenso, la Corte di giustizia ha *in primis* rilevato che l'ingiunzione determinava una limitazione alla libertà d'impresa risultante per l'imprenditore dal non poter disporre liberamente delle proprie risorse economiche e dall'essere obbligato ad adottare misure che «possono rappresentare un costo notevole per lo stesso, avere un impatto considerabile sull'organizzazione delle sue attività o richiedere soluzioni tecniche difficili e complesse»[22]. Tuttavia, ad avviso dei giudici europei, la predetta ingiunzione «non risulta pregiudicare la sostanza stessa del diritto alla libertà d'impresa di un fornitore di accesso ad Internet, quale quello di cui al procedimento principale» (§ 51), poiché, da un lato, una simile ingiunzione «lascia al suo destinatario l'onere di determinare le misure concrete da adottare per raggiungere il risultato perseguito, con la conseguenza che quest'ultimo può scegliere di adottare misure che più si adattino alle risorse e alle capacità di cui dispone e che siano compatibili con gli altri obblighi e sfide cui deve far fronte nell'esercizio della propria attività» (§ 52) e, dall'altro lato, «tale ingiunzione consente al suo destinatario di sottrarsi alla propria responsabilità qualora dimostri di aver adottato tutte le misure ragionevoli. Orbene, tale possibilità di esenzione dalla responsabilità ha, ovviamente, la conseguenza che il destinatario di tale ingiunzione non sarà tenuto a fare sacrifici insostenibili, circostanza che appare in particolare giustificata alla luce del fatto che quest'ultimo non è l'autore della violazione del diritto fondamentale della proprietà intellettuale che ha dato luogo alla pronuncia della suddetta ingiunzione» (§ 53).

Un altro settore in cui la libertà d'impresa è stata più volte presa in esame è quello della commercializzazione dei prodotti e, in particolare, dei relativi obblighi informativi a tutela degli interessi (patrimoniali e non) dei consumatori. Si tratta dei casi *Deutsches Weintor* (C-544/10), *Neptune* (C-157/14), *Lidl* (C-134/15) e *Dextro* (T-100/15).

Nel caso *Deutsches Weintor* (deciso nel settembre 2012), in materia di indicazioni nutrizionali e sulla salute fornite sui prodotti alimentari, in cui si è trattato di confrontare la tutela della salute con la libertà professionale e la libertà d'impresa, i giudici europei hanno anzitutto affermato che entrambi tali libertà non costituiscono una prerogativa assoluta[23]. Sulla base di quanto sopra, la Corte ha ritenuto – invero apoditticamente

[22] CGUE, C-314/12, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH e Wega Filmproduktionsgesellschaft mbH* (2014), § 50: «un'ingiunzione, quale quella di cui al procedimento principale, fa pesare in capo al suo destinatario un obbligo che limita il libero utilizzo delle risorse a sua disposizione, in quanto lo obbliga ad adottare misure che possono rappresentare un costo notevole per lo stesso, avere un impatto considerabile sull'organizzazione delle sue attività o richiedere soluzioni tecniche difficili e complesse».

[23] CGUE, C-544/10, *Deutsches Weintor eG v. Land Rheinland-Pfalz* (2012), § 73: «Per quanto attiene, in secondo luogo, alle libertà professionale e d'impresa, va ricordato che, secondo la giurisprudenza della Corte, il libero esercizio di un'attività professionale, al pari del diritto di proprietà, non risulta essere una prerogativa assoluta, ma va considerato in relazione alla sua funzione nella società (v., in tal senso, sentenza del 14 dicembre 2004, Swedish Match, C-210/03 […] punto 72). Di conseguenza, è possibile

– che «sebbene il divieto delle indicazioni di cui trattasi imponga talune restrizioni all'attività professionale degli operatori economici interessati riguardo ad un aspetto preciso, il rispetto di tali libertà è tuttavia garantito per gli aspetti essenziali» (§ 56) e che «[p]ertanto, in una fattispecie come quella del procedimento principale, l'indicazione controversa non incide affatto sulla sostanza stessa della libertà professionale e della libertà d'impresa. Da quanto precede emerge che il divieto assoluto, di cui al regolamento n. 1924/2006, di un'indicazione come quella in esame nel procedimento principale deve essere considerato conforme al requisito teso a conciliare i vari diritti fondamentali coinvolti e a stabilire un giusto equilibrio tra di essi» (§§ 58 e 59).

Nel caso *Neptune* (deciso nel dicembre 2015), in materia di indicazioni nutrizionali ed etichettatura di acque minerali, i giudici europei si sono trovati a raffrontare gli obblighi di etichettatura (a tutela della salute del consumatore) con i diritti fondamentali riconosciuti dall'art. 11 della Carta (libertà di espressione e informazione) e dall'art. 16 (libertà d'impresa). Al riguardo, è stato anzitutto riconosciuto che il divieto di far figurare sulle confezioni, sulle etichette e nella pubblicità delle acque minerali naturali qualsiasi indicazione o menzione che faccia riferimento al basso contenuto di sodio di tali acque costituisce un'ingerenza nella libertà d'impresa[24]. Per altro verso, nel valutare che le eventuali limitazioni alla libertà d'impresa (*i*) rispettino il contenuto essenziale di tale libertà, (*ii*) siano rispettose del principio di proporzionalità e (*iii*) siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'UE o all'esigenza di proteggere diritti e libertà altrui (§ 68), la corte europea ha ritenuto che «la necessità di garantire al consumatore l'informazione più precisa e trasparente possibile circa le caratteristiche del prodotto è in stretta connessione con la tutela della salute umana e costituisce una questione di interesse generale […] che può giustificare limitazioni alla libertà di espressione e d'informazione dell'imprenditore, nonché alla libertà d'impresa di quest'ultimo» (§ 74). In conclusione, anche in applicazione del principio di precauzione, i giudici di Lussemburgo hanno affermato che il legislatore dell'Unione ha potuto correttamente ritenere che vincoli e restrizioni relativi l'utilizzo di indicazioni o menzioni che fanno riferimento ad un basso contenuto di sodio delle acque minerali naturali erano adeguati e necessari per garantire la tutela della salute umana all'interno dell'Unione (§ 84); conseguentemente, «[a]lla luce di quanto esposto, si deve concludere che l'ingerenza nella libertà di espressione e d'informazione dell'imprenditore, nonché nella libertà d'impresa di quest'ultimo è, nel caso di specie, proporzionata agli obiettivi perseguiti» (§. 85)

Nel caso *Lidl* (deciso nel giugno 2016), in materia di commercializzazione di carni di pollame ed obblighi di etichettatura (sulla scorta del regolamento (CE) 543/2008

apportare restrizioni all'esercizio di dette libertà, purché dette restrizioni rispondano effettivamente a finalità di interesse generale perseguite dall'Unione e non si risolvano, considerato lo scopo perseguito, in un intervento sproporzionato e inammissibile che pregiudichi la stessa sostanza di tali diritti (sentenze del 15 aprile 1997, Irish Farmers Association e a., C-22/94, […] punto 27, nonché del 10 luglio 2003, Booker Aquaculture e Hydro Seafood, C-20/00 e C-64/00, […] punto 68)».

[24] CGUE, C-157/14, *Neptune Distribution SNC contro Ministre de l'Économie et des Finances* (2015), § 67: «il divieto di far figurare sulle confezioni, sulle etichette e nella pubblicità delle acque minerali naturali qualsiasi indicazione o menzione che faccia riferimento al basso contenuto di sodio di tali acque, la quale possa indurre in errore il consumatore circa tale contenuto, costituisce una ingerenza nella libertà di espressione e d'informazione dell'imprenditore, nonché nella libertà d'impresa di quest'ultimo».

avente ad oggetto le norme di commercializzazione per le carni di pollame), riconoscendo che l'obbligo di etichettatura può limitare la libertà d'impresa poiché incide sul suo libero uso delle proprie risorse[25], i giudici europei hanno nuovamente ribadito che la libertà d'impresa non è una prerogativa assoluta[26]. Il principio di proporzionalità è stato ritenuto rispettato poiché le norme sulla commercializzazione delle carni perseguono obiettivi di interesse generale riconosciuti dal diritto primario dell'Unione (in quanto contribuiscono a migliorare la qualità di tali carni - a tutela dei consumatori - e ad agevolarne la vendita, migliorando i redditi di produttori ed operatori del settore). In conclusione, «l'ingerenza nella libertà d'impresa della ricorrente nel procedimento principale è, nel caso di specie, proporzionata agli obiettivi perseguiti» (§ 40).

Nel caso *Dextro* (deciso nel marzo 2016), in materia di indicazioni sulla salute fornite sui prodotti alimentari, in cui la produttrice di un certo alimento ha lamentato, fra l'altro, la violazione dell'art. 16 della Carta da parte del regolamento (CE) 1924/2006, i giudici del Tribunale hanno rilevato che «se è vero che il divieto delle indicazioni sulla salute in questione impone talune restrizioni all'attività professionale della ricorrente in relazione ad un aspetto specifico, il rispetto di tali libertà è tuttavia garantito per quanto riguarda gli aspetti essenziali. Infatti, lungi dal vietare la produzione e la commercializzazione dei prodotti della ricorrente o la pubblicità relativa ai medesimi, il regolamento impugnato si limita, in forza dell'articolo 1, paragrafo 2, del regolamento n. 1924/2006, a circoscrivere l'etichettatura, la presentazione degli alimenti in questione e la loro pubblicità, al fine di tutelare la sanità pubblica, la quale costituisce un obiettivo di interesse generale idoneo a giustificare una restrizione di una libertà fondamentale […]. In tal senso, il diniego di autorizzazione delle indicazioni sulla salute in questione non incide affatto sulla sostanza stessa delle libertà riconosciute dagli articoli 6 e 16 della Carta dei diritti fondamentali, e deve essere considerato conforme al requisito teso a conciliare i vari diritti fondamentali coinvolti e a stabilire un giusto equilibrio tra di essi […]».

Anche in materia di diritti dei lavoratori, la libertà d'impresa ha rappresentato uno degli elementi valutazione nelle decisioni prese dalle corti che presidiano il legittimo sviluppo del processo di integrazione europea. In particolare, vanno rammentati i casi *Alemo-Herron* (C-426/11), *Aget* (C-201/15) e *IX e MJ* (cause riunite C-804/18 e C-341/19).

Nel caso *Alemo-Herron* (deciso nel luglio 2013), riguardante un caso di opponibilità al cessionario di un'azienda dei contratti collettivi di lavoro relativi ai dipendenti occupati nell'azienda in questione, la Corte di giustizia – sul presupposto che la libertà d'impresa comporta la libertà contrattuale – ha ritenuto che potesse costituire una

[25] CGUE, C-159/09, *Lidl SNC v. Vierzon Distribution SA* (2011), § 29: «poiché un obbligo di tal genere fa pesare in capo al suo destinatario un vincolo che limita il libero utilizzo delle risorse a sua disposizione, in quanto lo obbliga ad adottare misure che possono rappresentare un costo per lo stesso e avere un impatto sull'organizzazione delle sue attività».

[26] Ivi, § 30: «la libertà d'impresa non costituisce una prerogativa assoluta, bensì dev'essere presa in considerazione rispetto alla sua funzione nella società» e che conseguentemente (§ 31) «possono essere apportate restrizioni all'esercizio di tale libertà, a condizione che, ai sensi dell'articolo 52, paragrafo 1, della Carta, da un lato, esse siano previste dalla legge e rispettino il contenuto essenziale di detta libertà e, dall'altro, che, in osservanza del principio di proporzionalità, risultino necessarie e rispondano effettivamente a obiettivi di interesse generale riconosciuti dall'Unione europea o all'esigenza di tutelare diritti e libertà altrui».

violazione della libertà d'impresa rendere opponibile al cessionario di un'azienda un determinato contratto collettivo di lavoro rispetto a cui il predetto cessionario non aveva avuto «alcuna possibilità di fare parte dell'organismo di contrattazione collettiva in parola […poiché] tale cessionario non ha la facoltà né di fare valere efficacemente i propri interessi in un iter contrattuale né di negoziare gli elementi che determinano l'evoluzione delle condizioni di lavoro dei suoi dipendenti in vista della sua futura attività economica» (§ 34). È stato così ritenuto che in una «situazione siffatta, la libertà contrattuale del suddetto cessionario è talmente ridotta che una limitazione del genere può pregiudicare la sostanza stessa del suo diritto alla libertà d'impresa» (§ 35).

Nel caso *Aget* (deciso nel dicembre 2016), riguardante la mancata autorizzazione da parte del Ministro greco del lavoro, della previdenza sociale e della solidarietà sociale, per poter procedere a un licenziamento collettivo, sono state prese in considerazione le restrizioni alla libertà di stabilimento (art. 49 TFUE) e alla libertà di impresa derivanti dalla protezione dei lavoratori e dell'occupazione. Nel caso di specie, premesso che un regime autorizzatorio dei licenziamenti collettivi «deve mirare, in tale settore sensibile, ad una conciliazione e ad un giusto equilibrio tra gli interessi collegati alla protezione dei lavoratori e dell'occupazione, in particolare contro licenziamenti ingiustificati e contro le conseguenze dei licenziamenti collettivi per i lavoratori, e quelli attinenti alla libertà di stabilimento e alla libertà d'impresa degli operatori economici, sancite dagli articoli 49 TFUE e 16 della Carta» (§ 90), la Corte di giustizia ha ritenuto che detto regime autorizzatorio è fondato su criteri non precisi e su condizioni non oggettive e controllabili, che dunque «vanno oltre quel che è necessario per conseguire gli obiettivi indicati e non possono pertanto soddisfare quanto esige il principio di proporzionalità» (§ 100). Tale situazione è stata pertanto valutata in violazione del principio di proporzionalità e, in conclusione, della libertà di stabilimento e della libertà d'impresa.

Nei casi *IX* e *MJ* (decisi nel luglio 20219), riguardanti entrambi il divieto imposto da datori di lavoro ai propri dipendenti di indossare sul luogo di lavoro segni di natura politica, filosofica o religiosa, la Corte di giustizia ha riconosciuto che «la volontà di un datore di lavoro di dare ai clienti un'immagine di neutralità rientra nella libertà d'impresa, riconosciuta dall'articolo 16 della Carta, ed ha, in linea di principio, carattere legittimo, in particolare qualora il datore di lavoro coinvolga nel perseguimento di tale obiettivo soltanto i dipendenti che si suppone entrino in contatto con i clienti del medesimo» (§ 63). Per altro verso «la semplice volontà di un datore di lavoro di condurre una politica di neutralità, sebbene costituisca, di per sé, una finalità legittima, non è di per sé sufficiente a giustificare in modo oggettivo una differenza di trattamento indirettamente fondata sulla religione o sulle convinzioni personali, dato che il carattere oggettivo di una siffatta giustificazione può ravvisarsi solo a fronte di un'esigenza reale di tale datore di lavoro, che spetta a quest'ultimo dimostrare» (§ 64).

La libertà d'impresa è stata poi presa in considerazione nelle pronunce della Corte di giustizia *Schaible* (C-101/12), *Pillbox* (C-477/14), *Spika* (C-540/16), *Anie e a.* (C-798/18 e C-799/18) e *Bank Melli Iran* (C-124/20), rientranti in altri (e diversificati) settori del processo di integrazione europea.

Nel caso *Schaible* (deciso nell'ottobre 2013), in materia di controlli veterinari e zo-

otecnici applicabili negli scambi intracomunitari di taluni animali vivi e prodotti di origine animale, i giudici europei hanno ritenuto che il legislatore dell'Unione potesse legittimamente imporre gli obblighi controversi e che gli svantaggi derivanti da questi ultimi per gli allevatori non fossero sproporzionati rispetto agli obiettivi stabiliti dal regolamento n. 21/2004. Sicché è stato riconosciuto che il legislatore europeo non ha commesso errori in sede di valutazione dei vantaggi e degli svantaggi delle suddette obbligazioni in rapporto agli interessi in gioco e che, di conseguenza, non avesse violato la libertà d'impresa degli allevatori di ovini e di caprini.

Nel caso *Pillbox* (deciso nel maggio 2016), relativo alla regolamentazione delle c.d. "sigarette elettroniche", i giudici europei hanno riconosciuto che il divieto di comunicazioni commerciali costituisce un'ingerenza nella libertà d'impresa degli operatori economici (§ 156), ribadendo contestualmente che detta libertà non costituisce una prerogativa assoluta, che essa deve essere presa in considerazione della sua funzione nella società (§157), che può essere soggetta ad un ampio ventagli di interventi dei poteri pubblici purché nell'interesse generale (§ 158) e, infine, che – in applicazione del principio di proporzionalità – «qualsiasi limitazione all'esercizio dei diritti e delle libertà riconosciuti dalla Carta deve essere prevista per legge, deve rispettarne il contenuto essenziale e deve, nel rispetto del principio di proporzionalità, essere necessaria e rispondere effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui» (§ 159). Facendo applicazione dei principi appena riportati, la corte europea ha ritenuto che «che la limitazione in questione è stata stabilita dall'articolo 20, paragrafo 5, della direttiva 2014/40, ovvero dalla legge, ai sensi dell'articolo 52, paragrafo 1, della Carta, e che essa non incide sul contenuto essenziale della libertà di impresa. Infatti, né tale disposizione della direttiva, né peraltro alcun'altra disposizione della medesima, impediscono agli operatori economici di fabbricare e di immettere in commercio sigarette elettroniche e contenitori dei liquidi di ricarica nel rispetto delle condizioni previste a tal proposito dalla direttiva» (§ 161) e che la «ingerenza constatata non eccede nemmeno i limiti di quanto è idoneo e necessario al conseguimento degli obiettivi legittimamente perseguiti dalla direttiva 2014/40, per i motivi esposti ai punti da 109 a 118 della presente sentenza (§ 162)».

Nel caso *Spika* (deciso nel luglio 2018), in materia di assegnazione delle possibilità di pesca, è stato semplicemente ribadito che le limitazioni alla libertà d'impresa devono rispondere a un obiettivo di interesse generale e rispettare il principio di proporzionalità (§ 40).

Nei casi riuniti *Anie e a.* (decisi nell'aprile 2021), in materia di revisione delle tariffe incentivanti per la produzione di energia elettrica da impianti fotovoltaici, i giudici europei anzitutto hanno rammentato che la tutela conferita dall'art. 16 della Carta implica la libertà di esercitare un'attività economica o commerciale, la libertà contrattuale e la libera concorrenza e che «la libertà contrattuale, ai sensi dell'articolo 16 della Carta, si riferisce, in particolare, alla libera scelta della controparte economica nonché alla libertà di determinare il prezzo richiesto per una prestazione (sentenza del 20 dicembre 2017, Polkomtel, C-277/16 […] punto 50)» (§ 57). È stato poi aggiunto che «la libertà d'impresa sancita in quest'ultima disposizione comprende anche il diritto di ogni impresa di poter liberamente utilizzare, nei limiti della responsabilità per le

proprie azioni, delle risorse economiche, tecniche e finanziarie di cui dispone» (§ 62). Tuttavia, in ragione delle circostanze del caso concreto, la Corte di giustizia non ha ritenuto sussistente la violazione della libertà di impresa sancita dall'art. 16 della Carta. Nel caso *Bank Melli Iran* (deciso nel dicembre 2021), riguardante la risoluzione di alcuni contratti aventi ad oggetto la fornitura di servizi di telecomunicazioni in seguito all'inserimento della banca iraniana nell'elenco di soggetti interessati da sanzioni adottate dagli Stati Uniti d'America, i giudici di Lussemburgo hanno ritenuto che la limitazione alla libertà d'impresa fosse necessaria per proteggere gli interessi dell'Unione e giustificata in ragione degli obiettivi perseguiti e dei divieti contenuti nel regolamento 2271/96. In particolare, è stato osservato che «[p]er quanto riguarda la condizione relativa al rispetto del contenuto essenziale della libertà d'impresa, si deve ricordare che quest'ultimo è potenzialmente pregiudicato, in particolare, quando un'impresa viene privata della facoltà di far valere efficacemente i propri interessi in un iter contrattuale» (§ 87), ma che «[n]el caso di specie, tuttavia, annullare la risoluzione dei contratti di cui trattasi nel procedimento principale a causa della violazione dell'articolo 5 del regolamento n. 2271/96 avrebbe l'effetto non già di privare la Telekom della facoltà di far valere i propri interessi in generale nell'ambito di un rapporto contrattuale, ma piuttosto di limitare tale facoltà, poiché tale annullamento è giustificato solo nei limiti in cui la Telekom ha proceduto alla suddetta risoluzione al fine di rispettare gli atti normativi elencati» (§ 88). Resta peraltro fermo nel ragionamento della corte che spetta «al giudice del rinvio, inoltre, effettuare una ponderazione, nell'ambito di tale esame della proporzionalità, tra il perseguimento dei suddetti obiettivi del regolamento n. 2271/96, realizzato mediante l'annullamento di una risoluzione contraria al divieto di cui all'articolo 5, primo comma, del succitato regolamento, e la probabilità che la Telekom sia esposta a perdite economiche, nonché l'entità di queste ultime nel caso in cui tale impresa non possa porre fine ai suoi rapporti commerciali con una persona inserita nell'elenco SDN» (§ 92).

3. La protezione dei dati personali quale diritto fondamentale

La natura formale quale diritto fondamentale del diritto alla protezione dei dati personali risulta, *per tabulas*, dal suo inserimento nella Carta e nei Trattati, nonché dalle esplicite dichiarazioni dei giudici europei nei casi sottoposti al loro esame[27].

Tale natura viene oggi sancita, *in primis*, dall'inserimento del diritto alla protezione dei dati personali nella Carta, che all'art. 8 (nell'ambito del titolo dedicato alle 'Libertà') dispone che «ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano». Previsto anche dall'art. 16, par. 1, del Trattato sul funzionamento dell'Unione europea (TFUE), il carattere di diritto fondamentale del diritto alla protezione dei dati personali era peraltro già emerso sia nel diritto derivato (con la direttiva 95/46/CE, in cui la tutela del trattamento dei dati personali era considerato parte della

[27] M. Brkan *The Essence of the Fundamental Rights to privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, in *German Law Journal*, 2019, 864.

più ampia tutela della vita privata) ed è stato più volte ribadito dalla giurisprudenza della Corte di giustizia[28].

È merito soprattutto dell'opera della giurisprudenza della Corte di giustizia se la protezione dei dati personali si è evoluta nel tempo, passando dall'essere considerata quale mera eccezione alle libertà economiche sancite dai Trattati, all'attuale configurazione "costituzionalizzata" e orientata ai diritti fondamentali.

Va tuttavia ribadito che la protezione dei dati personali, sebbene sia stata formalmente elevata a diritto fondamentale per i cittadini europei, non risulta essere una loro prerogativa assoluta, giacché tale diritto è passibile di subire talune deroghe, specie per consentire l'esercizio di altri diritti fondamentali o, parimenti, per non incidere su specifici interessi dello Stato. Simili limitazioni, in verità, non sono rinvenibili nell'art. 8 della Carta (che, contrariamente a quanto previsto nella Convenzione Europea dei Diritti dell'Uomo, non contiene riferimenti espliciti in tal senso), ma sono il frutto di un più ampio approccio dettato dalla Corte di giustizia, secondo cui la suddetta disposizione deve essere interpretata non come valore assoluto, bensì tenendo presente la sua funzione nella società (cause riunite C-92/09 e C-93/09, *Schecke e Eifert*[29]). Tant'è che nella celebre decisione resa nel caso *Google Spain* (causa C-131/12) i giudici europei non hanno esitato a operare un bilanciamento fra interessi contrapposti, ritenendo infine prevalente il diritto alla protezione della vita privata e dei dati personali rispetto alla libertà economica dei fornitori di servizi elettronici[30].

Dal canto suo il RGPD (art. 1) esprime una ambivalente e apparentemente conflittuale finalità, poiché è diretto a sostenere tanto la protezione dei dati personali quanto la garanzia di libera circolazione degli stessi. È proprio da questa tensione fra la tutela del dato personale - come diritto fondamentale autonomo - e il possibile sfruttamento del dato stesso come merce e attività economica che deriva la necessità di un bilanciamento, di una valutazione attraverso l'utilizzo del principio di proporzionalità, determinando la sostanza dei diritti coinvolti, sotto il profilo delle misure e delle attività concrete. Questo lo si evince – come già ricordato - dal considerando 4 del RGPD, che, da un lato, configura la protezione dei dati personali come una prerogativa non assoluta e, dall'altro, contempla e prescrive il suo contemperamento con altri (elencati) diritti fondamentali. Se si guarda con attenzione al RGPD non si potrà non osservare che esso è permeato da disposizioni che richiedono il bilanciamento della protezione dei dati personali con altri diritti.

Nel RGPD l'onere di bilanciare i diritti è proprio del titolare del trattamento dei dati personali (art. 33 e 34 del RGPD), il quale è chiamato a mantenere una condotta proattiva in tal senso e a dar prova alle autorità di controllo di aver intrapreso tutte le mi-

[28] CGUE, C-293/12 e C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.* (2014); CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* (2017); CGUE, C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs e a.* (2019); C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a. v. Premier ministre e a.* (2020).

[29] A.S. Lind - M. Strand, *A New Proportionality Test for Fundamental Rights?*, in *European Policy Analysis*, 2011, 7.

[30] G. Resta - V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015.

sure tecniche adeguate a garantire la sicurezza del trattamento e ad evitare rischi (art. 24 del RGPD), in ossequio al principio della valutazione *case by case*. Questo approccio ritornerà in svariate decisioni che affronteranno quasi sempre tematiche collegate alla dimensione digitale o, più in concreto, l'extraterritorialità e la circolazione dei dati[31].

In definitiva, quindi, la giurisprudenza della Corte di giustizia (ma anche della corte di Strasburgo) ha dimostrato che il bilanciamento - che è sempre possibile – non può mai comportare in via automatica l'integrale sacrificio dell'una o dell'altra posizione giuridica tutelata. Con riferimento alle restrizioni imponibili al diritto fondamentale alla protezione dei dati personali, tanto la Corte europea dei diritti dell'uomo quanto la Corte di giustizia hanno concorso, ciascuna con i suoi strumenti e ciascuna nel suo ordinamento, a definire alcuni paletti invalicabili. Dal canto suo, il RGPD ha recepito l'orientamento di attenzione verso i diritti fondamentali perseguito dalla Corte di giustizia, che ha sempre ribadito il principio in forza del quale la disciplina di un settore altamente tecnologico o specifico non fa recedere la scienza giuridica dalla sua dimensione sociale, dove l'individuo assume la centralità della tutela e della sostanza dei diritti.

Come detto, nell'ambito del predetto bilanciamento, la protezione dei dati personali è sostenuta dal valore centrale per i sistemi giuridici europei del rispetto della dignità umana. Al potere conferito al titolare del trattamento dei dati, quindi, corrisponde la strenua attenzione dimostrata dagli organi giurisdizionali verso la dignità umana, che influenza anche l'attività attenta e indispensabile delle singole autorità di controllo nazionali.

Ora, per quanto mi è noto, in soli due casi la Corte di giustizia si è trovata a confrontare la protezione dei dati personali quale diritto fondamentale con altri diritti formalmente fondamentali. Si tratta del caso *Promusicae* (C-275/06) e del caso *Satamedia* (C-73/07).

Nel caso *Promusicae* (deciso nel gennaio del 2008), la Corte di giustizia ha affermato la necessità di trovare una conciliazione degli obblighi connessi alla tutela di diversi interessi fondamentali (la proprietà intellettuale, una tutela giurisdizionale effettiva, la tutela dei dati personali) ed ha osservato genericamente che «gli Stati membri sono tenuti, in occasione della trasposizione delle suddette direttive [n.d.r.: si tratta della direttiva 2000/31, della direttiva 2001/29 e della direttiva 2004/48], a fondarsi su un'interpretazione di queste ultime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati nell'ordinamento giuridico comunitario» (§ 68).

Nel caso *Satamedia* (deciso nel dicembre 2008), i giudici europei hanno ritenuto che il diritto alla tutela dei dati personali deve essere conciliato «in una certa misura, con il diritto fondamentale alla libertà di espressione» (§ 53) e che «[t]ale compito incombe agli Stati membri» (§54), sottolineando che «per ottenere un equilibrato contemperamento dei due diritti fondamentali, la tutela del diritto fondamentale alla vita privata richiede che le deroghe e le limitazioni alla tutela dei dati previste ai summenzionati capi della direttiva debbano operare entro i limiti dello stretto necessario» (§ 56).

Al riguardo, in via generale, si può osservare che in entrambi i casi sopra riportati la Corte di giustizia non ha fornito agli interpreti un criterio di bilanciamento fra i diritti

[31] CGUE, C-507/17, *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)* (2019); CGUE, C-154/21, *Österreichische Post* (2023).

che apparivano contrapporsi sufficientemente definito, ma ha sostanzialmente rinviato ogni valutazione alle corti nazionali, adottando quello che è stato definito *deferential approach*, ossia un approccio di prudente attenzione alle prerogative dei sistemi giuridici nazionali e dei loro attori interni[32].
Questa condotta della Corte di giustizia può presentare profili positivi, quali un approccio pluralistico e di rispetto delle diverse identità giuridiche degli Stati membri, ma anche profili negativi, quali una – più o meno significativa – incoerenza di fondo della regolamentazione del mercato interno (dovuta alla creatività dei legislatori nazionali) e un possibile eventuale "indebolimento" di altri diritti fondamentali (il diritto di proprietà, la libertà di espressione).

4. Osservazioni finali

L'analisi sopra riportata consente alcune osservazioni finali, che all'evidenza non possono essere (né pretendono di esserlo) conclusive.
L'affermato superiore valore assiologico del diritto alla protezione dei dati personali rispetto alla libertà d'impresa non può essere intuitivamente assunto, pena scadere in un irrazionale pregiudizio, in una visione monoculare che inevitabilmente condurrebbe al miope ed assoluto *enforcement* di un unico diritto. L'indagine sulla natura del diritto alla protezione dei dati personali deve indirizzarsi anzitutto verso una più precisa ed attuale (nel senso della considerazione della corrente evoluzione dell'ecosistema digitale e degli interessi in esso presenti) individuazione del nucleo essenziale del 'diritto alla protezione dei dati personali'. Devono altresì essere tenuti in debita considerazione le specifiche caratteristiche del diritto alla protezione dei dati personali nel contesto generale dei diritti della personalità, non potendosi trascurare il carattere non-monolitico degli interessi della singola persona rispetto ai "propri" dati personali e delle diverse esigenze di tutela che ne conseguono. In particolare, non appare del tutto convincente la de-patrimonializzazione dei dati personali e la non legittimità giuridica della loro "monetizzazione", peraltro, in qualche modo, messa in discussione dallo stesso legislatore europeo con la direttiva (UE) 2019/770[33]. Infatti, la tradizione giuridica occidentale, che pone al centro dell'universo dei diritti il singolo individuo, dovrebbe spingerci a una maggiore valorizzazione della *user freedom*, ossia di una libera e consapevole (perché informata, in quanto esercitata in un contesto pienamente trasparente) capacità del singolo di controllare e gestire i propri dati personali, fino al punto di poterli cedere come un asset patrimoniale[34]. Ove l'assunto della non-patrimonializzazione dei dati personali venisse smentito o, quanto meno, rimodulato in maniera non assoluta, ne conseguirebbe una particolare posizione del diritto alla pro-

[32] M. Tzanou, *Balancing fundamental rights: united in diversity? Some reflections on the recent case law of the European Court of Justice on data protection*, in *CYELP*, 2010, 53.

[33] E. Tosi, *Circolazione dei dati personali tra contratto e responsabilità. Riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, Milano, 2023, 78 ss.

[34] B. Custers - G. Malgieri, *Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data*, in *Computer Law & Security Rev.*, 2022, 45

tezione dei dati personali nell'ambito dei diritti della personalità e a cascata la necessità del suo riposizionamento sotto il profilo assiologico. Ritengo che andrebbe quanto meno verificata la possibilità di una "graduazione assiologica" dei plurimi diritti in cui si articola al proprio interno il diritto alla protezione dei dati personali, ossia una articolazione più attenta al concreto e specifico diritto relativo ai dati personali che si intende proteggere.

Sotto altro, ma collegato, profilo, una più attenta analisi ontologica del diritto alla protezione dei dati personali dovrebbe far risultare il carattere multifocale della protezione dei dati personali, che non può essere trascurato allorché si realizza la difficile operazione di bilanciamento fra il singolo diritto in cui si concretizza la protezione del dato personale e la specifica attività imprenditoriale che con esso viene a rapportarsi, più o meno antagonisticamente. Infatti, solo un'attenta ed analitica operazione di individuazione e confronto del diritto (quello specifico diritto in cui si sostanzia la protezione dei dati personali nel caso di specie) e della libertà (quella specifica libera attività imprenditoriale che si intende porre in essere), consente di svolgere quell'operazione di bilanciamento che permette di sacrificare al minimo l'una (la libertà) a fronte della più ampia e profonda protezione dell'altro (il diritto). Ancora una volta si sottolinea che l'opera di bilanciamento dell'interprete non può essere gravata da *bias* assiologici, ma va rigorosamente improntata all'analisi concreta degli interessi dei soggetti coinvolti. Come insegna la nostra Corte costituzionale, l'operazione di bilanciamento non può mai operare seguendo una gerarchia fissa e immodificabile, ma deve avvenire caso per caso, in maniera mobile[35].

Sicché, sotto il profilo delle soluzioni rinvenibili nella predetta opera di bilanciamento, va probabilmente superata la comprensibile preferenza verso la *golden rule* del consenso del soggetto interessato rispetto alla base giuridica del trattamento dei dati personali (rammentando che il consenso è base giuridica avente il medesimo valore delle altre basi giuridiche del trattamento dei dati personali) e valorizzata (nel senso che deve essere quanto meno non esclusa *a priori* e valutata con maggiore e specifica attenzione) l'ipotesi che il trattamento dei dati personali possa rispondere al legittimo interesse del titolare di sviluppare la propria attività d'impresa (dovendosi probabilmente anche tenere in debita considerazione le dimensioni e la forza economica dell'impresa e della sua capacità di impatto sui diritti degli utenti digitali, come singoli e come collettività). Tale valorizzazione appare suscettibile di essere condotta specie nella misura in cui i dati personali possano essere considerati un asset patrimoniale condivisibile con terzi e vieppiù quando il terzo – proprio grazie al trattamento dei dati personali – possa in tal modo offrire agli interessati innovativi servizi o contenuti.

Del resto, non può essere trascurato il profilo della obsolescenza della regolamentazione giuridica rispetto all'evoluzione tecnologica e alle sempre nuove capacità di trattamento dei dati personali, che rendono la base giuridica del consenso a volte di assai difficile applicazione, se non asfittica (si pensi, soprattutto, al campo del trattamento dei dati sanitari). Una regolamentazione giuridica che, sotto altro generale profilo, appare oggi guardare alla relazione fra libertà d'impresa e diritto alla protezione dei dati personali in maniera troppo unilateralmente orientata (secondo una dinamica *top-down*

[35] R. Bin, *Diritto e argomenti. Il bilanciamento degli interessi nella giurisprudenza costituzionale*, Milano, 1992.

a senso unico), con prescrizioni che irrigidiscono in maniera eccessiva la necessaria flessibilità che facilita l'operazione di equo bilanciamento dei diritti e degli interessi.
Sembra andare nel senso di una maggiore valorizzazione del legittimo interesse quale base giuridica del trattamento dei dati personali, l'evoluzione (invero ancora *in fieri*) della nota vicenda che a fine marzo u.s. ha visto il Garante Privacy italiano emettere un provvedimento (n. 112 del 30 marzo 2023) di limitazione temporanea del trattamento dei dati personali da parte di ChatGPT sulla scorta di diverse motivazioni, fra cui – per quel che qui interessa – l'apparente assenza di una base giuridica che giustificasse la raccolta e la conservazione dei dati personali utilizzati per "addestrare" gli algoritmi necessari al funzionamento dello strumento di intelligenza artificiale relazionale. Infatti, nel provvedimento dell'11 aprile (n. 114) il Garante Privacy ha ingiunto alla società titolare di ChatGPT (OpenAI L.L.C.) di: «[…] 5. modificare la base giuridica del trattamento dei dati personali degli utenti ai fini dell'addestramento degli algoritmi, eliminando ogni riferimento al contratto e assumendo come base giuridica del trattamento il consenso o il legittimo interesse in relazione alle valutazioni di competenza della società in una logica di accountability […]». In questa ingiunzione può probabilmente essere vista una prudente, ma assai interessante, apertura del Garante Privacy verso il superamento dell'assoluta primazia del consenso quale lecita base giuridica del trattamento dei dati personali, a favore di una maggiore considerazione del "legittimo interesse" del titolare e/o di terzi. Va da sé che una simile strada richiederebbe con tutta probabilità una interpretazione evolutiva del 'legittimo interesse' che – nel rispetto dei diritti degli interessati (fra cui *in primis* il diritto di opposizione da potersi esercitare in un contesto di assicurata trasparenza e di ricercata idonea consapevolezza dell'utente digitale, a sua volta pieno e paritario titolare della *user freedom* di fronte ad una riconosciuta e non mortificata *freedom to conduct business*) – non valuti secondariamente il valore dell'innovazione tecnologica a beneficio dell'intera collettività.
Infatti, non può essere messa in secondo piano l'analisi di un tema di fondo, di assai ampio respiro, ossia il rapporto che deve auspicabilmente sussistere fra l'utilizzazione dei dati personali e l'innovazione quale momento di progresso della condizione umana rispetto a crisi e problemi che potrebbero essere meglio affrontati grazie al trattamento dei dati personali (dal cambiamento climatico alle crisi alimentari, dalla ricerca biologica alla medicina personalizzata). La necessità di non ostacolare l'innovazione può probabilmente in alcune occasioni (da vagliare caso per caso) far ritenere legittimo l'interesse derivante e/o collegato all'attività d'impresa inerente (e, quindi, in qualche modo positivamente reattiva) alle predette crisi o problemi, in un contesto in cui il passaggio dalla base giuridica del consenso a quella del legittimo interesse significa anche responsabilizzare maggiormente l'impresa che tratta i dati personali. Al riguardo, ulteriori spunti di riflessione (anche rispetti ai c.d. 'dati pubblici', ossia raccolti dalle pubbliche amministrazioni, che sovente rappresentano un patrimonio inutilizzato) sono forniti dalla proposta di Data Governance Act - che appare aver accolto il principio della monetizzazione dei dati - e dei futuri strumenti regolatori europei aventi ad oggetto l'intelligenza artificiale.
Un'ultima osservazione: la "visione" della politica europea di protezione dei dati personali appare essere una visione tipicamente occidentale, della *Western Legal Tradition*,

ossia una visione in cui i diritti individuali, del singolo, sono al centro del sistema giuridico (così come il singolo è perno centrale delle relazioni giuridiche), spesso in contrapposizione con i diritti degli altri singoli (siano essi persone fisiche o giuridiche) e/o dei pubblici poteri, secondo i termini e le modalità oggetto delle nostre tradizionali strutture e categorie del 'diritto privato' e del 'diritto pubblico/costituzionale', e su cui così spesso riflettiamo allorché ci apriamo alla comparazione fra concezioni del diritto e sistemi giuridici. Come accennato all'inizio, questa visione ha condotto allo sviluppo e alla affermazione della categoria dei 'diritti inviolabili', dei 'diritti fondamentali'. Va peraltro preso atto che questa visione è una visione relativa, ossia non comune a tutti, a livello globale. Ora, ritenendo che non sia questa la sede per poter approfondire la relatività di questa visione e le conseguenze che ne derivano rispetto al rapporto fra libertà di impresa e diritto alla protezione dei dati personali, sia in termini generali, sia in termini specifici, resta comunque da chiedersi se, rispetto a tale ultimo diritto fondamentale, una visione maggiormente aperta (ma non sottomessa) all'interesse della collettività non possa condurre a "rivedere" alcuni profili (ossia alcune declinazioni) della inviolabilità del diritto alla protezione dei dati personali del singolo individuo, specie ove vi sia un interesse generale primario (ad esempio, all'innovazione in campo medico) e il nucleo essenziale della dignità del singolo individuo possa comunque essere preservata adottando gli opportuni accorgimenti.

European Collective Redress and Data Protection Challenges and Opportunities*

Marina Federico

Abstract

This paper analyses the potential of group actions as an instrument for data protection law enforcement in Europe. The first part investigates whether article 80 GDPR may provide a legal basis for aggregate litigation in data protection law. The second part of the essay explores the relationship between EU Directive 2020/1828 and the GDPR, and evaluates the potential of the new European representative action to enforce data protection rights and deter Big Tech's unfair practices. Lastly, this essay outlines a private enforcement framework to ensure data protection and consumer rights in Europe, one that is able to balance the freedom of data, market needs and the protection of individuals.

Il saggio intende indagare le potenzialità della tutela collettiva come strumento per garantire la protezione dei dati personali. La prima parte del lavoro è volta a verificare se l'art. 80 del Regolamento europeo per la protezione dei dati personali (GDPR), possa offrire una base giuridica per la tutela collettiva in questa materia. La seconda parte è invece dedicata al rapporto tra il GDPR e la nuova direttiva (UE) 1828/2020 sulle azioni rappresentative a tutela degli interessi dei consumatori, ed al possibile impiego della nuova azione rappresentativa europea per la protezione dei dati personali. L'obiettivo del contributo è quello di tratteggiare i caratteri essenziali di un sistema rimediale idoneo a garantire la *data privacy* degli individui, in grado di bilanciare la libera circolazione dei dati e le esigenze di tutela della persona.

Summary

1. Introduction. - 2. Private enforcement and data protection: challenges. - 3. Article 80 GDPR: is there a legal basis for group actions in data protection law? - 4. The case of *Meta Platforms v. the German Federal Union of Consumer Organisations and Associations*. - 5. Collective actions: the European approach. - 6. *Group data protection*: a collective interest? - 7. Data protection and consumer law: an integrated enforcement system. - 8. Compensatory actions. - 9. Private enforcement and data protection: opportunities.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Keywords

data protection - consumer law - group data protection - aggregate litigation - representative actions

1. Introduction

In Informational Capitalism[1], data is viewed as a commodity[2]. It circulates fast on the Internet, and is used to formulate accurate behavioural predictions, using techniques called "big data analytics". More specifically, what is regarded as a valuable good is the information that public and private actors can derive from a huge amount of data[3]. These data, both personal and anonymous, is often referred to as "big data". Big data is data of great volume, velocity and variety[4] from which useful conclusions can be inferred through data mining[5].

In fact, the information that big data analytics can infer from data disseminated by Internet users is often employed for a range of commercial purposes. These include improving services and products, developing targeted advertisements, tailoring goods offered to meet the characteristics and needs of individual users[6]. Personal data pro-

[1] Informational Capitalism refers to: «the alignment of capitalism as a mode of production with informationalism as a mode of development. […] Capitalism is oriented toward profit- maximizing, that is, toward increasing the amount of surplus appropriated by capital on the basis of the private control over the means of production and circulation, while informationalism «is oriented toward accumulation of knowledge and towards higher levels of complexity in information processing». In a regime of informational capitalism, market actors use knowledge, culture, and networked information technologies as means of extracting and appropriating surplus value, including consumer surplus». J. Cohen, *Between Truth and Power. The Legal Constructions of Informational Capitalism,* Oxford, 2019, 5-6.

[2] H. Zech, *Data as a Tradeable Commodity – Implications for Contract Law*, 2017, in J. Drexl (ed.), *Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition*, Edward Elgar Publishing, 1. As famously stated by the British mathematician Clive Humby, in 2006, data have been defined as «the new oil» of our age.

[3] D.L. Rubinfeld-M.S. Gal, *Access Barriers to Big Data*, in *Arizona Law Review*, 2, 2017, 341 ss. See also P.C. Zikopoulos-C. Eaton-G. Deroos-T. Deutsch-G. Lapis, *Understanding Big Data*, New York, 2012; K. Crawford-D. Boyd, *Critical Questions for Big Data. Provocations for a Cultural, Technological and Scholarly Phenomenon,* in *Information, Communication & Society*, 5, 2012, 662 ss.; F. X. Diebold, *A Personal Perspective on the Origin(s) and Development of "Big Data": The Phenomenon, the Term, and the Discipline*, in *PIER Working Paper No. 13-003*, 1 ss.; V. Mayer-Schonberger-K. Cukier, *Big Data: A Revolution That Will Transform Howe We Live, Work and Think*, Boston, 2013; M. T. Maggiolino, *I big data e il diritto antitrust*, Napoli, 2018, 23-72.

[4] According to the Gartner Information Technology Dictionary, big data are: «high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making» (see D. Laney, *3D Data Management: Controlling Data Volume, Velocity and Variety*, Gartner Information Technology Dictionary, 2001). Another definition of big data as «large amounts of different types of data produced with high velocity from a high number of various types of sources» is given in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Towards a thriving data-driven economy**,** COM/2014/0442 final.

[5] T. Zarsky, *"Mine your own business!" Making the case for the implications of the data mining of personal information in the forum of public opinion*, in *Yale Journal of Law and Technology*, 5, 2003, 6-7.

[6] V. Zeno-Zencovich, *Do "Data Markets" Exist?*, in *Rivista di diritto dei media*, 2, 2019, 22 ss.

cessing is a profitable activity which allows companies to develop and offer new services. This would explain why European lawmakers generally regard the flow and the sharing of users' data favorably, since this enables businesses to grow in a competitive market[7]. More generally, data are also necessary for Artificial Intelligence (hereinafter: AI) systems to perform their tasks[8].

However, the collection of huge quantities of personal data leads to a high risk of mass violations of people's fundamental rights, namely self-determination, personal identity, non-discrimination and, *inter alia*, data protection. Examples of the latter include: accidental data breaches; large-scale processing of personal data, carried out without a proper legal basis; people not granted access to their personal data; automated decision-making processes resulting in discrimination against people and harming their self-determination, for example in some machine learning credit scoring algorithms.

When such conducts occur on the Internet, they often have a cross-border dimension, negatively impacting individuals who live in different parts of the world. In these cases, the injured parties can hardly gather to initiate legal proceedings against a data controller. Moreover, individuals alone often have neither the means nor the economic resources to pursue their rights in court; the power imbalance between traders and consumers is therefore particularly high[9]. Consequently, the effectiveness of the General Data Protection Regulation (hereinafter: GDPR)[10], which is the cornerstone of European data protection law, ends up being compromised[11].

Hence, there arises the need for an effective enforcement system of EU data protection law implemented by both public and private actors. Considering the disruptive impact of personal data processing on a vast number of subjects and its potential consequences, a possible approach could be to reassess the law of remedies on a collective basis. It would then be crucial to coordinate the remedial system with the protection offered by National Supervisory Authorities and the risk-based approach

[7] V. Ricciuto., *Authorities and Private Companies in Regulating Software Technologies*, in *Privacy and Data Protection in Software Services*, Berlin, 2022, 16. The EU law approach is evident also in the new proposal for a Regulation of the European parliament and of the council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act, hereinafter: AIA) and amending certain EU legislative acts**,** COM/2021/206 final.

[8] V. Zeno-Zencovich, *Do "Data Markets"*, cit., 30-31. AI systems are «systems that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with» (art. 3, para. 1 («Definitions»), AIA) and they have an increasingly important role in our daily life. For one of the first definitions of AI, see R. Kurzweil, *What is Artificial Intelligence Anyway?*, in *American Scientist,* 3,1985, 258 ss.

[9] See M. Lippi-G. Contissa-A. Jablonowska-H.W. Micklitz-P. Palka- G. Sartor-P. Torroni, *The Force Awakens: Artificial Intelligence for Consumer Law*, in *JAIR (Journal of Artificial Intelligence Research),* 67, 2020, 171; G. Colangelo-M. Maggiolino, *From fragile to smart consumers: Shifting paradigm for the digital era*, in *Computer Law and Security Review,* 2, 2019, 174-176.

[10] 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).

[11] On the relationship between the digital economy based on big data and the GDPR, T. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, 4, 2017, 995 ss.

adopted by the European Union in the law of new technologies[12].

The GDPR places considerable emphasis on public enforcement, conferring significant powers on Data Protection Authorities[13]. However, a purely public enforcement model is inadequate. This is firstly because there is the risk that certain unfair conducts may not be addressed by public regulators. Secondly, the investigative powers of Supervisory Authorities may vary between Member States[14]. In order to enforce compliance with the GDPR, Supervisory Authorities are equipped with corrective powers and can impose administrative fines, depending on the nature of the infringement[15]. While these sanctions certainly do have a strong deterrent effect, they need to be accompanied by civil redress and judicial remedies.

Public enforcement needs to be complemented with remedies which will provide data subjects with fair compensation when their rights are infringed[16]. Moreover, in its defense, public enforcement requires huge public expenditure and time. Furthermore, regulation cannot be totally comprehensive, especially in this field as Information and Communication Technologies (ICTs) are changing at a faster and faster pace. Although EU law provisions attempt to be technologically neutral, the globalized and interconnected world constantly poses new challenges. Hence, an efficient private enforcement system should be designed to complement the public enforcement sphere in order to deal with mass violations of data protection rights. Given that data users are generally consumers of digital services, in developing the private enforcement system it may be helpful to consider the close ties between data protection and consumer law, as group litigation has already been used in the latter.

The paper therefore assesses whether and how collective litigation can be used in data protection law. The analysis focuses on art. 80 GDPR («Representation of data subjects») and the new European Directive 2020/1828 on representative actions for the collective interests of consumers. Its aim is to address the following questions*: i)* Is there a legal basis in the GDPR for private enforcement remedies such as group actions? *ii)* Can consumer law tools be used for collective actions in the field of data protection?

The paper is structured as follows: after this brief introduction, sections 2 and 3 investigate the features of art. 80 GDPR to ascertain whether art. 80 could constitute a legal basis for collective injunctive and compensatory measures. Section 4 reviews a re-

[12] On the risk-based approach see R. Gellert., *The risk-based approach to data protection*, Oxford, 2020; A. Mantelero, *Responsabilità e rischio nel Regolamento UE 2016/679*, in *Le Nuove Leggi Civili Commentate,* 1, 2017, 144 ss.

[13] Chapter VI («Independent Supervisory Authorities»), Section 2 («Competence, Tasks and Powers») and especially art. 58 GDPR («Powers»).

[14] See P. Voigt-A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A practical guide*, Berlin, 2017, 202 ss.

[15] Ivi, 210 ss.

[16] For the different functions of public and private enforcement, even if with reference to antitrust law, see G. Muscolo, *Il nuovo assetto istituzionale del private antitrust enforcement*, in G. Benacchio-M. Carpagnano (a cura di), *Aspetti istituzionali e prospettive applicative del private antitrust enforcement nell'Unione Europea, Atti del VI Convegno Biennale Antitrust Facoltà di Giurisprudenza Trento, 6-8 aprile 2017*, Trento, 2018, 19-21. On private and public enforcement in the GDPR, see P. Voigt-A. von dem Bussche, *The EU,* cit., 201 ss. and P. Lambert, *Data Protection, Privacy Regulators and Supervisory Authorities*, London, 2020, 235 ss.

cent judgment of the European Court of Justice (hereinafter: CJEU), case C-319/20, *Meta Platforms Ireland Ltd. v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (Federal Union of Consumer Organizations and Associations of Germany, hereinafter: the Federal Union) published on April 28, 2022[17]. In sections 5, 6 and 7, it turns to the collective dimension of data protection, looking at the relationship between data protection and consumer law, with special reference to Directive (EU) 2020/1828. In section 8, the paper addresses some concerns regarding compensatory actions. Finally, some future perspectives on the enforcement of EU data protection law are highlighted, and a conclusion drawn.

2. Private enforcement and data protection: challenges

The public enforcement model has always been predominant in Europe, at least up to now. This might be due to the fact that the EU lacks procedural law competencies, apart from measures to develop judicial cooperation in civil and commercial law matters (as provided for in art. 81 of the Treaty on the Functioning of the European Union, hereinafter: TFEU). Consequently, civil procedure remedies still fall within national procedural laws. However, there is a growing trend in favour of private enforcement in consumer law matters, particularly to expand the role of the judiciary[18]; for instance, group litigation has recently been re-evaluated[19]. Directive (EU) 2020/1828[20] (part of the «New deal for Consumers» package[21]) encourages representative actions for the protection of the collective interests of consumers. Meanwhile, on a national level many European States have adopted new pieces of legislation regarding group actions, not only in consumer law[22]. For example, the Italian legislator enacted a new law on class actions in 2019 (arts. 840-*bis* ss. of the Italian Civil Procedure Code)[23]. However, some civil law jurisdictions are still quite skeptical about the application of

[17] CJEU, C-319/20, *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV*. (2022).

[18] H.W. Micklitz-F. Cafaggi, *Administrative and Judicial Enforcement in Consumer Protection: The Way Forward,* in *EUI Working Papers, Law*, 2008, 3-4.

[19] A. Biard, *Collective redress in the EU: a rainbow behind the clouds?*, in *ERA Forum,* 2018, 189 ss. See also H.W. Micklitz-F. Cafaggi, *Administrative and Judicial Enforcement,* cit., 2.

[20] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, OJ 2020 L. 409/1.

[21] Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, A New Deal for Consumers, COM(2018)183 final. On the New Deal for Consumers and its implications for consumer law, M. Grochowski, *European Consumer Law After The New Deal: A Tryptich,* in *Yearbook of European Law*, 1, 2020, 387 ss.

[22] C. I. Nagy, *Collective Actions in Europe: A Comparative, Economic and Transsystemic Analysis*, Berlin, 2019, 71 ss.

[23] On the new Italian law on class action, U. Ruffolo (ed.), *Class action ed azione collettiva inibitoria. Commento sistematico alla legge 12 aprile 2019, n. 31,* Milano, 2021*;* C. Consolo, *L'azione di classe, trifasica, infine inserita nel c.p.c*, in *Rivista di diritto processuale,* 2, 2020, 714 ss.; B. Sassani (ed.), *Class action. Commento sistematico alla legge 12 aprile 2019, n. 31,* Pisa, 2019*;* A. Giussani, *La riforma dell'azione di classe,* in *Rivista di diritto processuale,* 6, 2019, 1572 ss.

collective actions, since these are almost inconceivable in legal systems where court rulings in prior adjudications are binding only on parties to the cases involved[24]. Ostensibly, group actions would seem to be at odds with some of the fundamental rules and principles of civil procedure, such as the private right of action and the principle of party disposition, and the so-called "subjective limits" of *res judicata*[25].

Procedural law instruments are drawn up mainly on an individual basis. European Constitutions state that everyone should be allowed to bring their rights to courts through a judicial complaint.[26] This right is traditionally referred to as the right of action. Judicial authorities are obliged to pronounce their verdicts only on the basis of what parties have alleged and proved, in accordance with the dispositive principle[27]. The possibility of another (natural or legal) person enforcing someone else's rights is regarded as exceptional, and would therefore need to be covered by legal provisions[28]. Moreover, according to the rules on the subjective limits of *res judicata,* individuals who were not litigants in a certain proceeding cannot be bound by its outcome. Otherwise, the interests of non-parties who did not have the opportunity to be heard would be impaired, and their right of defense would be violated[29].

By contrast, in group actions, one subject (a legal entity or a natural person, the so-called "class representative") acts as plaintiff on behalf of a plurality of individuals to uphold their rights; and absent class members are also bound by the final judgment[30].

---

[24] C.I. Nagy, *Collective actions,* cit., 24 ss.

[25] The term "subjective limits of *res judicata*" refers to who is bound by the effects of a judgment.

[26] C.I. Nagy, ivi. See, for instance, art. 24 of the Italian Constitution: «Everyone can start a legal claim to protect their rights and legitimate interests» (*Tutti possono agire in giudizio per la tutela dei propri diritti e interessi legittimi* […]) and art. 24 of the Spanish Constitution «Everyone has the right to obtain effective judicial protection of their rights and legitimate interests, and the right to defense in all the circumstances» (*Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión* […]).

[27] In Italian law, the dispositive principle is laid down in art. 2907, para. 1, Italian Civil Code («Jurisdictional protection is provided by the judiciary, at the request of the interested party […]»); art. 99, Italian Civil Procedure Code («Who wants to assert a right in court must bring a claim before the competent judge»); art. 115, para. 1, Italian Civil Procedure Code («Courts must base their decisions on the basis of the evidence offered by parties or by the public prosecutor, or on the facts which were not specifically contested by the parties during the proceeding, except for the specific cases laid down by law»).

[28] Again, for example, in the Italian legal system, this is provided for in art. 81, Italian Civil Procedure Code («No one can assert someone else's rights in court, except for the specific cases laid down by law»); in the French legal system by art. 31, French Civil Procedure Code («Everyone who has a legitimate interest in the success or rejection of a cause of action can start an action in court […]»). For a general perspective on the principle of party presentation in civil law countries' proceedings, see O.G. Chase-H. Hershkoff-L. J. Silberman-J. Sorabji-R. Stürner-Y. Taniguchi-V. Varano, *Civil Litigation in Comparative Context*, in *NYU School of Law. Public Law & Legal Theory Research Paper Series WP no. 17-37 - Law & Economics Research Paper Series WP no. 17-35*, 2017, 9.

[29] N. Trocker, voce *Giudicato (diritto comparato e straniero),* in *Enc. Giur. Treccani,* Roma, 1989, 3 ss. In Italian law, this principle is enshrined in art. 2909 of the Italian Civil Code. On the Italian rule of *res judicata,* see the landmark work of F. P. Luiso, *Principio del contraddittorio ed efficacia della sentenza verso i terzi*, Milano, 1981. On the rules of *res judicata* and their relationship with aggregate litigation, see also M. Cappelletti-B. Garth, *Access to Justice: The Newest Wave in the Worldwide Movement to Make Rights Effective*, in *Articles by Maurer Faculty,* 1978, 210 ss.; M. Taruffo, "*Collateral estoppel" e giudicato sulle questioni, II*, in *Rivista di diritto processuale*, 2, 1972, 272 ss.

[30] R. Money-Kyrle - C. Hodges, *European Collective Action: Towards Coherence*, in *Maastricht Journal of*

This is particularly evident in opt-out collective redress, but it is also true for opt-in proceedings[31]. In fact, even when group members are required to opt into the litigation, namely to express their will to be included in the proceeding, their judicial rights are limited to a certain extent. Opt-in and opt-out procedures are justified by the benefits that collective litigation may bring in terms of access to justice and procedural economy. Nonetheless, in light of all the foregoing, group actions always need a correct and clear legal basis. Statutes should safeguard the right to due process, striking a balance between judicial efficiency, the right to a fair trial and legal coherence.

As mentioned above, it is well known that collective redress mechanisms[32] can help consumers to share their judicial costs and burdens when pursuing their case in court. As in certain claims the individual loss suffered by the consumer may be too small compared to the cost of litigation[33], collective redress can ensure effective access to justice to individuals, reduce the cost of litigation and achieve judicial economy. Collective litigation can also ensure clarity and consistency between decisions regarding similar matters, perform a regulatory function and deter unfair practices of the "Tech giants".

This is particularly true for compensatory actions in data protection law. The losses suffered by the data subjects are often non-pecuniary[34]. This non-monetary damage arising from a violation of data protection law may vary in nature. For example, users might suffer distress and anxiety after an accidental data breach, or discomfort regarding possible identity theft, or their self-determination may be violated, for instance when purchasing services under the undue influence of targeted advertising. This type of harm may be too small if considered individually and this situation is likely to discourage data subjects seeking redress, given the considerable cost of litigation.

The GDPR clearly states that every data subject shall receive effective judicial protection, in compliance with art. 47 of the Charter of Fundamental Rights of the European Union (CFR). Despite this, access to justice risks being impaired if individuals

European and Comparative Law, 4, 2012, 496.

[31] Opt-in systems require individuals to take a positive action to be included in an aggregate proceeding; on the contrary, in opt-out systems individuals who do not want to be bound by the outcome of a judgment should take a positive action to be excluded by the proceeding. On the advantages and disadvantages of opt-in and opt-out models, see R. Mulheron, *The Class Action in Common Law Legal Systems: A Comparative Perspective*, Oxford, 2004, 37 ss.

[32] Please note that in this paper the term "collective redress" is used broadly, in the sense of: «a broad concept encompassing any mechanism that may accomplish the cessation or prevention of unlawful business practices which affect a multitude of claimants or the compensation for the harm caused by such practices» (Commission Staff Working Document, Public Consultation: Towards a Coherent Approach to Collective Redress, SEC(2011)173 final, cited in N. E. Hatzimihail, *Collective Redress and Global Governance (Concluding Remarks)*, in A. Nuyts - N. E. Hatzimihail (eds.), *Cross-Border Class Actions, The European Way*, Munich, 2014, 315).

[33] C. I. Nagy, *Collective Actions*, cit., 9 ss.

[34] Compensation and liability in European data protection are mainly covered by art. 82 GDPR («Right to compensation and liability») and recital 75 GDPR. On the variety of material and non-material damages as considered in the GDPR, see C. Camardi, *Liability and Accountability in the 'Digital' Relationship*, in R. Senigaglia-C. Irti-A. Bernes (eds.), *Privacy and Data Protection in Software Services*, Berlin, 2022, 26.

do not know how to or do not have the means to assert their rights[35]. Furthermore, the right to data protection is regarded as a fundamental right in the EU legal order, according to art. 8 CFR[36], and fundamental rights violations shall always be compensated[37].

Collective redress might therefore be an appropriate way to compensate large numbers of individuals whose privacy rights have been affected. Furthermore, as far as non-pecuniary damages are concerned, national courts have maintained that personal rights violated by the same unlawful conduct and sharing certain characteristics can be compensated collectively[38]. In such cases, judges generally calculate a lump sum which the defendant shall pay, and then award each class member a percentage of the total. Although damages are awarded in an approximate manner via this method, it is also true that without collective redress the injured parties would not be compensated at all.

Bearing in mind all the potential advantages of aggregate litigation, it is necessary to ascertain if it has a legal basis under the GDPR. As far as EU data protection law is concerned, resorting to group actions is a controversial matter, given that the GDPR is built around the model of individual consent as the main legal basis for personal data processing. Similarly, the remedial system laid down in Chapter VIII GDPR («Remedies, liability and penalties») would seem essentially individualistic[39].

Nevertheless, a legal basis for collective redress might be found in art. 80 GDPR[40]. This allows Member States' laws to permit «bodies, organizations and associations» to lodge a complaint with a Supervisory Authority, or to ask for a judicial remedy, with or without a data subject's mandate, when the rights of the data subjects have been infringed. Even though recital 142 seems to allow an organisation to act on behalf of a multitude of data subjects, art. 80 does not state this explicitly. Recently, this has been addressed by the CJEU in the *Meta Platforms* case, which will be examined further in the next sections.

---

35 See the enlightening study of M. Cappelletti-B.Garth, *Access*, cit., 181 ss.

36 The European Charter of Human Rights (ECHR) also mentions in art. 8 the right to private life. Though not explicitly mentioning the right to data protection, the Convention has been used to protect the right to data privacy. On data privacy and its protection in the EU legal order, see FRA (European Union Agency for Fundamental Rights), *Handbook on European data protection law*, 2018.

37 Affirmed by the Italian Supreme Court in the landmark cases Cass. civ., sez. III, 31 maggio 2003, n. 8827 and 8828, in *Il foro italiano,* 2003, 2273 ss., as well as Cass. civ., sez. un., 11 novembre 2008, n. 26972, in *Il repertorio del foro italiano,* 2008.

38 For instance, see the judgment of the Italian Supreme Court, Cass. civ., sez. III, 31 maggio 2019, n. 14886, in *Il repertorio del foro italiano,* 2019, *Danni in materia civile*, n. 195. In civil law countries, however, this is still regarded as something exceptional. See L. Mullenix, *Lessons from Abroad: Complexity and Convergence*, in *Villanova Law Review*, 1, 2001, 7 ss.

39 F. Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Le Nuove Leggi Civili Commentate,* 2, 2017, 377 ss.; A. Mantelero, *Responsabilità*, cit., 144 ss.

40 A. Biard, *Collective redress*, cit., 202.

3. Article 80 GDPR: is there a legal basis for group actions in data protection law?

In Europe, the topic of collective actions in data protection law has not been researched in depth, for several reasons.

First of all, in the immediate aftermath of the GDPR implementation, the disruptive scope of personal data processing had yet to be seen. Nor was it possible to foresee the enormous success of the Regulation, which is now considered a virtuous model worldwide (the «Brussels effect»[41]). Moreover, legal scholars have tended to focus on the main innovations introduced by the GDPR as compared to the previous piece of legislation (Directive 95/46/EC[42]), for example regarding the «rights of the data subject» (Chapter III, Arts. 15 ss. GDPR). Lastly, the enforcement of data protection law has been carried out almost exclusively by Supervisory Authorities so far, therefore outside the scope of private enforcement[43].

Such an emphasis on public enforcement applies to almost all European countries. EU legislation has mainly intervened in substantive law, leaving its private enforcement to Member States[44]. Hence, private enforcement in the EU has been conceived as «a fantastic beast»[45]. The procedural autonomy principle, devised by the CJEU, precludes the EU from intervening in procedural law matters. Indeed, civil procedure is a branch of law closely tied to national legal traditions, and where legal certainty is pivotal[46].

Nevertheless, resorting to the principle of effectiveness (laid down in art. 47 CFR and in art. 19 (1) TEU) and the principle of *effet utile,* the EU has been intervening more and more in procedural matters[47]. In fact, the CFR affords a high degree of protection to consumers, providing them with adequate remedies and access to justice. Unsurprisingly then, some legal scholars have talked of a «procedural consumer law» in the making[48]. Indeed, the above-mentioned Directive (EU) 2020/1828 on consumer collective interests promotes the harmonization of consumer group actions in the Member States.

---

41 A. Bradford, *The Brussels Effect,* in *Northwestern University Law Review*, 1, 2015, 22 ss.

42 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 2016 L 119/1.

43 M. Requejo Isidro, *Procedural Harmonisation and Private Enforcement in the GDPR*, in F. Gascón Inchausti-B. Hess (eds.), *The Future of the European Law of Civil Procedure. Coordination or Harmonisation?*, Cambridge, 2020, 194.

44 H. W. Micklitz-F. Cafaggi, *Administrative and Judicial Enforcement*, cit., 3 ss.

45 R. Pardolesi, *Il private enforcement del diritto antitrust: un animale fantastico, e dove trovarlo*, in G. A. Benacchio-M. Carpagnano (eds.), *Aspetti istituzionali,* cit., 49.

46 S. Law-J.T. Nowak *Procedural Harmonisation by the European Court of Justice*, in F. Gascón Inchausti-B. Hess, *The future*, cit., 19 ss., 31 ss.

47 F. Cafaggi-P. Iamiceli, *The Principles of Effectiveness, Proportionality and Dissuasiveness in the Enforcement of EU Consumer Law: The Impact of a Triad on the Choice of Civil Remedies and Administrative Sanctions,* in *European Review of Private Law,* 3, 2017, 575 ss.

48 V. Zeno-Zencovich - M. C. Paglietti., *Diritto processuale dei consumatori*, Napoli, 2009.

With specific reference to the protection of personal data, the GDPR contains some provisions relating to judicial remedies (art. 78 ss. GDPR). Firstly, it states that data subjects must have appropriate procedural tools to enforce their rights but does not explicitly mention group actions. However, a wider interpretation of art. 80 GDPR would provide a legal basis for group actions promoting the interests of the data subjects. This was the conclusion reached some years ago by the CJEU, in case C-40/17, *Fashion ID v. Verbraucherzentrale NRW eV*[49], and endorsed more recently in case C-319/20, *Meta Platforms Ireland Ltd. v. the German Federal Union of Consumer Organisations and Asssociations.*

Art. 80 GDPR allows a data subject to be represented in administrative and judicial proceedings «by a not-for-profit body, organisation or association which has been properly constituted under the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data». The GDPR probably limits the type of entities entitled to act as representatives in order to prevent the courts from being flooded with unwarranted claims. Consumers might otherwise become party to unmeritorious procedural initiatives, and risk no longer being able to assert their rights in court[50].

As regards judicial proceedings, art. 80 (1) provides that the data subject can mandate eligible legal entities to appeal against measures undertaken by a Supervisory Authority, or to contest the actions of a data controller. The legal entity should also be able to exercise the right to receive compensation on behalf of the data subject, in accordance with art. 82 («Right to compensation and liability»), where provided for by Member States. In contrast, paragraph 2 of the same article states that it is up to Member States whether they allow entities to start a proceeding independently of a mandate when they consider the rights of the data subjects to have been infringed. In this case, the possibility of seeking damages is not expressly mentioned.

To sum up, in the first scenario, set out in art. 80 (1), the data subject gives a mandate to an entity to procedurally represent her or him; in the second, based on art. 80 (2), an entity asks for an effective judicial remedy for the data subject without her or his mandate, if allowed by the Member States.

Art. 80 does not specify whether the entity can represent more than one data subject. However, the possibility was envisaged while drafting the legislation[51] and emerges in recital 142, which states that an entity can bring judicial proceedings «on behalf of the data subjects».

[49] CJEU, C-40/17, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*. (2019).

[50] H. W. Micklitz-F. Cafaggi, *Administrative and Judicial Enforcement*, cit., 17.

[51] S. Thobani, *Art. 80 GDPR – Rappresentanza degli interessati*, in V. Barba-S. Pagliantini (eds.), *Commentario del Codice Civile,* diretto da E. Gabrielli, *Delle Persone, Leggi collegate,* vol. II, Milano, 2019, 1210.

4. The case of *Meta Platforms v. the German Federal Union of Consumer Organisations and Associations*

In cases *Fashion ID v. Verbraucherzentrale NRW eV* and *Meta Platforms,* the CJEU affirmed that art. 80 GDPR allows representative actions for the interests of a plurality of data subjects. The judgment *Meta Platforms* is of great importance, since the CJEU granted consumer organizations the right to lodge a complaint to enforce data protection law provisions on a collective basis, in accordance with art. 80.

The facts of the case concerned personal data processing conducted by Meta. Specifically, when Facebook users accessed free games on the platform, they accepted that the game providers received certain data and gave them permission to publish content on their behalf. This was deemed in violation of the requirements of consent of the data subjects (see art. 6-7 GDPR) and to the prohibition of unfair commercial practices (Directive 2005/29/EC[52], amended by Directive (EU) 2019/2161[53]).

In this case, the Federal Court of Justice of Germany (*Bundesgerichtshof*) asked the CJEU for a preliminary ruling on the compatibility with art. 80 (2) GDPR of a national provision granting consumer associations legal status to request an injunction against conducts infringing the right to data protection. Indeed, the German provision recognized that legal entities could uphold the rights conferred on individuals through consumer law provisions, without requiring a mandate or proof of consumers having suffered actual harm[54].

The Court first clarified that there is no need for a specific national law implementing art. 80 (2) when Member States laws already have legal provisions granting direct standing of legal entities in representative actions[55]. Accordingly, consumer associations may act without a mandate to enforce the GDPR, requesting a collective injunction.

The Court also stated that represented groups of individuals do not need to identify all their component members. Indeed, the GDPR itself defines the data subject as anyone who is «identified or identifiable». Thus, it is possible to start an injunctive action simply by designating a group of people affected by unlawful data processing[56] (e.g. consumers who have used a certain cloud computing service, or have subscribed to a social media platform).

The Court further stressed that an association or legal entity can bring a represent-

[52] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') OJ 2005, L. 149/22.

[53] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ 2019, L. 328/7.

[54] CJEU, C-319/20, *Meta Platforms,* cit., §§ 27-36.

[55] CJEU, C-319/20, *Meta Platforms,* cit., §§ 60-66.

[56] CJEU, C-319/20, *Meta Platforms,* cit., §§ 68-69.

ative action, asking for injunctive relief, regardless of the infringement of specific rights of the data subjects. The Court affirmed that: «it is sufficient to claim that the data processing concerned is liable to affect the rights which identified or identifiable natural persons derive from that regulation, without it being necessary to prove actual harm suffered by the data subject, in a given situation, by the infringement of his or her rights»[57]. Accordingly, the mere risk of harm is enough for collective injunctions.
The Court also advocated further integration between data protection and consumer law. «In the modern economy, marked by the boom in the digital economy, personal data processing is liable to affect individuals not only in their capacity as natural persons enjoying the rights conferred by Regulation (EU) 2016/679, but also in their capacity as consumers»[58]. These are the opening words of the opinion of Advocate General Jean Richard de la Tour. The CJEU indicated that a legal entity can simultaneously claim an infringement of data protection law and a breach of the prohibition of unfair commercial practices, the prohibition of the use of invalid general terms and conditions, and consumer law provisions in general[59]. Moreover, the CJEU cited Directive (EU) 2020/1828, on the representative actions for the protection of the collective interests of consumers. In fact, the Court noted that interpreting art. 80 GDPR as allowing group actions would be line with the provisions of the Directive. The latter is another legal instrument for collectively enforcing consumer rights, including the protection of their data[60]. The CJEU would therefore seem to have armed consumers with a strong shield for defending their privacy rights.

5. Collective actions: the European approach

On various occasions, the European Union has expressed concern that group actions could lead to an opportunistic use of trials and become a source of easy profits for part of the legal industry. Another worry it highlighted was that group actions would jeopardise the right of defense and due process and cause excessive standardization of adjudication[61]. Some of these fears have now been addressed by Directive (EU) 2020/1828 on representative actions for the collective interests of consumers. This was adopted in December 2020 and must be implemented in national laws by December 2022, and it was mentioned by the CJEU in the *Meta Platforms* case.
Safeguarding consumer collective interests is a topic that has long been discussed in the EU, being covered in a Green Paper in the early 90s already. At that time, the European Commission gave preference to injunctive measures[62]. This led to the adop-

[57] CJEU, C-319/20, *Meta Platforms,* cit., § 72.

[58] Opinion of Advocate General Richard de la Tour, CJEU, C-319/20, *Meta Platforms,* cit., § 1.

[59] CJEU, C-319/20, *Meta Platforms,* cit., §§ 78-79.

[60] CJEU, C-319/20, *Meta Platforms*, cit., §§ 80-82.

[61] C. I. Nagy, *Collective Actions,* cit., 23 ss.

[62] Green Paper, Access of Consumers to Justice And The Settlement of Consumer Disputes in The Single Market, 16 November 1993, COM(93)576 Final.

tion of Directive 1998/27/EC[63], amended and replaced by Directive 2009/22/EC[64], now repealed by Directive (EU) 2020/1828.

Under this new Directive, the EU also acknowledged the need to compensate damages arising from mass injuries together with the necessity to harmonize collective redress measures, since many EU Member States had already endorsed these in their national procedural law[65]. Thus, the Directive provides for both injunctive and compensatory measures (termed collective redress, i.e. «compensation, repair, replacement, price reduction, contract termination or reimbursement of the price paid»[66]).

The EU also devised common rules of harmonization on collective actions in this Directive. The European approach is sectorial, meaning that representative actions (art. 3, para. 1, n. 5, Directive (EU) 1828/2020) are established solely for consumer interests. However, States are free to enable other group actions in different areas of law[67]. This is the case in Italy, where the law on class actions extends to every branch of law[68]. The EU Directive confers standing on qualified entities for starting a representative action (art. 3, para. 1, n. 4; art. 4 Directive (EU) 1828/2020), but States are again free to allow natural persons to act as class representatives when starting group actions according to their national laws.

The Directive applies only to representative actions for enforcing the «collective interests of consumers» (art. 2, Directive (EU) 1828/2020) thereby showing its intention to create a close interrelation between public and private enforcement. Traditionally, public enforcement is aimed at avoiding social harm and defending collective interests, while private enforcement is employed for seeking individual redress. By its reference to collective interests, it is evident that the boundaries dividing public and private enforcement have become increasingly blurred and the two areas are increasingly more intertwined. The explicit reference to the collective interests of consumers can be explained by the need to justify collective actions in European legal systems[69].

Annex I of the Directive lists the GDPR among the legal acts that can be enforced

[63] Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests, OJ 1998 L. 166.

[64] Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests, OJ 2009 L. 110/30.

[65] Study requested by the European Parliament's JURI Committee, commissioned by Policy Department for Citizens' Rights and Constitutional Affairs, *Collective redress in the Member States of the European Union*, 2018, 17 ss. The implications and shortcomings of the fragmentation of collective redress systems were demonstrated in the Dieselgate case (B. Gsell, *The New European Directive on Representative Actions for the Protection of the Collective Interests of Consumers – A Huge, But Blurry Step Forward*, in *Common Market Law Review*, 5, 2021).

[66] Art. 3, n. 10), Directive (EU) 2020/1828.

[67] Art. 2, para. 2, Directive (EU) 2020/1828.

[68] Art. 840-*bis* ss., Italian Civil Procedure Code.

[69] The expression "collective interests of consumers" was previously used in art. 1, Directive 2009/22/EC on injunctions for the protection of consumers' interests, now repealed by Directive (EU) 2020/1828. However, the former stated that «collective interests means interests which do not include the cumulation of interests of individuals who have been harmed by an infringement» (recital 3, Directive 2009/22/CE). In contrast, the notion of collective interests employed by Directive (EU) 2020/1828 is broader: «the general interest of consumers and, in particular for the purposes of redress measures, the interests of a group of consumers» (art. 3, «Definitions», Directive (EU) 2020/1828).

through representative actions[70]. Indeed, violating the GDPR may harm the collective interests of consumers, such as having adequate information and commercial practices performed in good faith, fairness and loyalty, as well as transparency in contractual relations[71]. An example of harm is the case *Meta Platforms v. The Federal Union* where personal data were processed on the basis of uninformed and invalid consent and the data controller also committed a deceptive practice by not complying with all the informatory duties prescribed by consumer law.
However, the scope of the Directive could also extend further. If group data protection was deemed a collective interest of consumers, then it could be directly enforced through a representative action. This would mean that if the right to data protection of a group of users was violated, a qualified entity could start a representative action under the Directive, without having to prove a contextual violation of other consumer law provisions.
The following section will thus explore the concept of "group data protection" as a collective interest of consumers. Then, the links between art. 80 GDPR and the Directive on representative actions will be analyzed.

6. *Group data protection*: a collective interest?

One may wonder whether data protection can be regarded as a «collective interest of consumers», based on the Directive. The answer to this question is crucial in assessing the possibilities of group actions in this area. It is well known that while in common law «there is no right without a remedy» in civil law jurisdictions (the majority within the EU) «the right is said to precede the remedy»[72]. Since aggregate litigation derogates from certain characteristics of civil law jurisdictions[73], group actions are available only for protecting certain kinds of interests (for example, «individual homogenous rights» in the Italian legal system). Hence, it is vital to ascertain whether data protection might be regarded a collective interest, to establish whether the newly adopted Directive (EU) 2020/1828 could be employed for this purpose.
In data protection law, the use of collective remedies seems to be mandated by actual facts. Not only was this affirmed in the judgment *Meta Platforms,* concerning this matter, but it was also considered in several soft law documents enacted by the Euro-

[70] Annex I, n. 56), Dir (EU) 2020/1828.

[71] N. Helberger-F. Zuiderveen Borgesius-A. Reyna, *The perfect match? A closer look at the relationship between EU consumer law and data protection law,* in *Common Market Law Review,* 5, 2017, 1427 ss.

[72] See G. I. Seidman, *Comparative Civil Procedure,* in C. B. Picker-G. I. Seidman (eds.), *The Dynamism of Civil Procedure - Global Trends and Development*, Berlin, 2016, 8 and H. Dedek, *From Norms to Facts: The Realization of Rights in Common and Civil Private Law,* in *McGill Law Journal*, 1, 2010, 79-80.

[73] See Section 2.

pean Union[74], and in the new Directive (EU) 2020/1828 on representative actions[75]. As noted earlier, digital techniques of mass profiling can lead to discriminatory outcomes, and the collection of (often sensitive) data can, in the event of data breaches, result in the dissemination, theft and destruction of these data. In other words, entire groups of individuals increasingly find themselves deprived of control over their information. These people are harmed by the same unlawful conduct, but are often unaware that they are not alone. In such cases, digital practices can generate not only individual injury, but also real social harm[76].

Moreover, unlawful commercial practices appear to be at odds with the interest in a data-driven economy, where market needs must be balanced and reconciled with individual rights and freedoms. Directive (EU) 2020/1828 explicitly mentions the GDPR as one of the regulatory acts whose violation may have an impact on the collective interests of consumers[77].

The above upholds the existence of a general interest in fair personal data processing, which preserves the fundamental rights and freedoms of groups of individuals subjected to the same digital techniques. This interest goes hand in hand with the individual right to personal data protection, namely the right to control one's personal information and the term "group data protection" encompasses this notion[78].

The dual nature of group data protection, an individual right and a supra-individual interest, is similar to that witnessed in other sectors, for example the right to fair

[74] Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, COM/2020/264 final, part. 2; Commission Recommendation of 11 June 2013 on common principles on injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law, 2013/396/EU, recital 6. See also European Parliament's JURI Committee, *Collective redress,* cit., 262.

[75] Directive (EU) 2020/1828, recital 1 ss. On Directive (EU) 2020/1828, D. Fairgrieve-R. Salim, *Collective Redress in Europe: Moving Forward or Treading Water?,* in *International and Comparative Law Quarterly,* 2, 2022, 465 ss; B. Gsell, *The New European Directive*, cit., 1365 ss.; L. Hornkohl, *Up and Downsides of the New EU Directive on Representative Actions for the Protection of the Collective Interests of Consumers – Comments on Key Aspects*, in *Journal of European Consumer and Market Law*, 5, 2021, 189 ss.

[76] C. Camardi, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Jus Civile*, 3, 2020, 810. As pointed out in recital 75 GDPR: «The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage».

[77] See again Annex I, n. 56), Directive (EU) 2020/1828.

[78] The notion of "group data protection" stems from the concept of "collective data protection", elaborated by Alessandro Mantelero, and inspired by the notion of "group privacy". However, Mantelero focuses mainly on groups created by profiling techniques. Moreover, the Author does not seem to trust private enforcement tools, such as group actions, relying almost exclusively on the role of Supervisory Authorities. He also concludes emphasizing the collective dimension of data protection, as an aggregative interest. See A. Mantelero, *Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection*, in *Computer Law & Security Review,* 2, 2016, 1 ss., 13; A. Mantelero, *From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era,* in L. Floridi-L. Taylor-B. Van der Sloot (eds.), *Group privacy. New challenges of data technologies,* Berlin, 2017, 179 ss. On group privacy, see E. J. Bloustein, *Group Privacy: The Right to Huddle,* in *Rutgers-Camden Law Journal,* 8, 1977, 219 ss.

competition, the proper functioning of the market, fair business practices and correct information[79].
Group data protection would therefore fall under the definition of collective interest provided in the Directive (art. 3, Directive (EU) 2020/1828), and this would consequently allow the European representative action to be used in this sector[80]. Given that an interest as group data protection exists, the focus will now shift to the relationship between Directive (EU) 2020/1828 and art. 80 GDPR.

7. Data protection and consumer law: an integrated enforcement system

Given that users are frequently both consumers and data subjects, Directive (EU) 2020/1828 and art. 80 GDPR may overlap and interfere with each other in the future. When interpreting art. 80 GDPR in the case *Meta Platforms*, the CJEU affirmed that the Directive on representative actions «contains several elements which confirm that art. 80 of the GDPR does not preclude the bringing of additional representative actions in the field of consumer protection»[81]. In fact, recital 11 of the Directive states that representative actions do not replace existing legal provisions on group actions.
At first glance, the provisions of the Directive appear compatible with art. 80 GDPR. As stated above, the GDPR empowers certain legal entities to bring representative actions and claim both injunctive and redress remedies. The CJEU underlined that these entities include consumer associations[82]. For its part, the Directive grants standing to qualified entities that States «designate for that purpose» (art. 4, Directive (EU) 2020/1828). The requirements that qualified entities must meet are set out in art. 4 and are essentially aligned with those of art. 80 GDPR[83].
Overall, representative actions are in line with the GDPR, even considering group data protection as a collective interest. Collective interests such as transparency and fairness in contractual relations fit perfectly with the data privacy of users[84]. For example, collective redress measures could play a role in cases of unfair commercial clauses in terms of services, or unfair business practices, when providers fail to comply with informatory duties and violate the GDPR at the same time, thereby harming consumers. Under this scenario, consumers would have two possible options: namely, to act via EU

[79] P. Helm, *Group Privacy in Times of Big Data. A Literature Review*, in *Digital Culture and Society*, 2, 2016, 144.

[80] On the nature of the "collective interests" recalled by Directive (EU) 2020/1828, see E. Camilleri, *La dir. 1828/2020/UE sulle azioni rappresentative e il "sistema delle prove". La promozione dell'interesse pubblico attraverso la tutela degli interessi collettivi dei consumatori: verso quale modello di enforcement?,* in *Nuove Leggi Civili Commentate,* 4, 2022, 1086 ss.

[81] CJEU, C-319/20, *Meta Platforms,* cit., § 81.

[82] CJEU, C-319/20, *Meta Platforms,* cit., § 65.

[83] Art. 80, para. 1, GDPR.

[84] See P. Rott, *Data protection law as consumer law. How consumer organisations can contribute to the enforcement of data protection law*, in *Journal of European Consumer & Market Law*, 3, 2017, 115 ss.

representative actions or via national class actions, in accordance with art. 80 GDPR[85].

8. Compensatory actions

While the Directive explicitly allows for injunctive and compensatory actions, art. 80 GDPR seems to make a distinction between them. The GDPR allows a qualified entity to ask for compensatory measures if it obtains a mandate from the data subject (art. 80 (1) and art. 82 GDPR). However, when entities exercise data subjects' rights without a mandate (art. 80 (2)) the possibility of claiming damages is debatable[86]. Indeed, art. 80 (2) does not explicitly refer to art. 82. Nor does the recent judgment *Meta Platforms* cover compensatory claims, since the CJEU's ruling covered only injunctive measures. Nevertheless, the wording of art. 80 (2) does not exclude compensatory actions, and the case *Meta Platforms* may also be a point in favor of allowing an entity to ask for redress even without a mandate.

Although art. 80 (2) GDPR does not mention collective compensatory measures, the latter may fall under the broad notion of «effective judicial remedy»[87]. The GDPR is a Regulation, thus providing scope for full harmonization among Member States. However, in *Meta Platforms* the CJEU qualified art. 80 (2) as an «open clause»[88]. It has therefore left room for national laws to implement art. 80 (2) in a manner that best guarantees the rights laid down in the Regulation.

The CJEU referred to effective protection, the need to secure proper redress, and consumers' access to justice. These goals may be achieved more promptly by strengthening collective redress measures[89]. This could be pursued by, for example, expanding the number of eligible entities that can sue a data controller[90], including those who do not have a mandate. Collective redress can, in fact, aggregate small claims, satisfy individual rights and deter companies from engaging in unfair practices. Were a legal system to legitimize collective redress even when the data subjects have not conferred a mandate on the representative entity, the system would be likely to defend the effectiveness and

---

85 F. Gascon Inchausti, *A new European way to collective redress? Representative actions under Directive 2020/1828 of 25 November*, in *Zeitschrift für das Privatrecht der Europäischen Union,* 2, 2021, 66. Cfr. G. De Cristofaro, *Azioni "rappresentative" e tutela degli interessi collettivi dei consumatori. La "lunga marcia" che ha condotto all'approvazione della dir. 2020/1828/UE e i profili problematici del suo recepimento nel diritto italiano*, in *Nuove Leggi Civili Commentate*, 4, 2022, 1022.

86 See F. Casarosa, *Azioni collettive fra tutela dei dati personali e tutela dei consumatori: nuovi strumenti alla prova dei fatti*, in P. Iamiceli (ed.), *Effettività delle tutele e diritto europeo. Un percorso di ricerca per e con la formazione giudiziaria*, Open Access – Università degli Studi Trento, 2020, 439; F. Casarosa, *Transnational collective actions for cross-border data protection violations*, in *Internet Policy Review*, 9, 2020, 5 ss.; A. Pato, *The collective private enforcement of data protection rights in the EU*, in *MPI-IAPL Summer School 3rd ed, Forthcoming*, 2019, 2 ss; A. Pato, *The National Adaptation of Article 80 GDPR, Towards the Effective Private Enforcement of Collective Data Protection Rights,* in K. McCullagh-O. Tambou-S. Bourton (eds.), *National Adaptations of the GDPR,* Series Open Access Book, in *Blogdroiteuropéen*, 2018, 99.

87 Art. 79 GDPR, mentioned in art. 80, para. 2, GDPR.

88 CJEU, C-319/20, *Meta Platforms,* cit., § 57.

89 CJEU, C-319/20, *Meta Platforms,* cit., §§ 73-75.

90 V. Zeno Zencovich - M. C. Paglietti, *Diritto processuale*, cit., 51.

supremacy of EU law.

Furthermore, if Member States already allow collective compensatory mechanisms under their laws, these mechanisms could potentially be used by a legal entity having direct standing to undertake a collective action, in line with art. 80 (2) GDPR[91]. Although the CJEU referred only to injunctive claims in its ruling, there is no reason to maintain that the judgment does not also apply to redress measures in this respect. Ultimately, in representative actions, the Directive allows a legitimate entity to seek redress with or without a mandate from consumers, leaving States free to choose opt-in or opt-out mechanisms (art. 8 (3), Directive (EU) 2020/1828).

9. Private enforcement and data protection: opportunities

In conclusion, group actions are not only a deterrent to businesses engaging in unlawful conducts; more importantly, they may grant individuals effective relief[92]. This is true especially for data protection law. When the right to data privacy is violated on a large scale, collective redress provides a useful procedural tool. The legal basis for this can be found in art. 80 GDPR. This is not the only route. Collective actions may be started, when data subjects are also consumers, through national laws implementing Directive (EU) 2020/1828. Thus, the Directive is taking steps in the right direction to protect consumer rights.

While collective redress poses big challenges, it could certainly be an important tool for the enforcement of digital rights in the era of ICTs. Under the "multi-level" legal order, we need to (re)think our traditional dogmas and categories, such as the right of action, standing and liability. Moreover, the enforcement of these rights should be pursued globally and uniformly, since their dimension is global itself.

Our globalized and digital world also requires heightened awareness of how procedural and substantive law interconnect. Further harmonization and convergence of procedural law rules are essential to achieve a common ground for handling cross-border disputes. Additionally, Member States and EU institutions, including the judiciary, ought to continue to cooperate closely in ensuring a direct and indirect enforcement system that is both multilayered and effective. In such a system, consumer law and data protection law should increasingly interact with each other. Developing group actions can be pivotal in this regard, ensuring the effectiveness of people's fundamental rights, especially their right to data privacy.

[91] See again CJEU, C-319/20, *Meta Platforms,* cit., §§ 60-66.

[92] C. Hodges, *Collective Redress: The Need for New Technologies, in Journal of Consumer Policy*, 2019, 60-61.

Sul crinale tra *data altruism* e *social scoring*: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo*.

Andrea Vigorito

Abstract

L'attuazione della Strategia europea in materia di dati sta cambiando il volto del sistema regolatorio europeo mediante la predisposizione di nuovi strumenti per il governo dei dati, sia (a monte) volti all'incentivazione della loro circolazione sia (a valle) volti al controllo del loro utilizzo. In questo contesto, il presente contributo mira a fornire una prima analisi della concreta portata applicativa di alcuni concetti di recente introduzione quali l'altruismo dei dati (data altruism) e il c.d. punteggio sociale (social scoring). Nel farlo, lo scritto prende le mosse da alcune esperienze pratiche recentemente oggetto di attenzione nell'attività del Garante privacy, con la finalità di identificare delle possibili applicazioni dei nuovi strumenti regolatori nonché di delineare il confine tra iniziative di cittadinanza attiva e di cittadinanza "a punti".
Inglese

As the European Strategy for data is changing the European regulatory framework, new means for data governance are being implemented. These tools are intended to both foster data circulation and control its use. Within this context, the paper offers an overview of the concrete scope of application of some newly-introduced concepts such as data altruism and social scoring. Therefore, the study takes as a basis some practical experiences recently investigated by the Italian Data Protection Authority, in order to identify possible applications of the new regulatory tools and to outline the border between active citizenship and citizen scoring initiatives.

Sommario

1. Nuove frontiere nel sistema europeo di governo dei dati. – 2. Altruismo dei dati. Oltre il recepimento normativo. – 3. Punteggio sociale. Dal modello cinese alle ap-

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

plicazioni europee. – 4. Le istruttorie del Garante privacy: il caso dell'Osservatorio Nazionale *Sharing Mobility*. – 4.1. Alla luce del *Data Governance Act*. – 4.2. Alla luce dell'*Artificial Intelligence Act*. – 5. Osservazioni conclusive: cittadinanza attiva o "a punti" per la *smart city*.

Keywords

governo dei dati – altruismo dei dati – social scoring – punteggio sociale – cittadinanza "a punti"

1. Nuove frontiere nel sistema europeo di governo dei dati

Il processo di adeguamento del modello regolatorio europeo alle trasformazioni in corso nella società basata sui dati ha di recente subìto una decisa sterzata, muovendo verso frontiere nuove e aderendo a un rilevante mutamento di prospettiva[1]. Invero, il graduale manifestarsi delle componenti della Strategia europea in materia di dati[2] sembra preludere alla concretizzazione di un rivisitato modello di gestione e governo dei dati (o, come viene spesso definito, pur nell'ambiguità del termine, di *data governance*)[3]. Più precisamente, nella ricerca di un corretto regime giuridico circa la raccolta, l'elaborazione, l'utilizzo, il governo dei i dati – ciò che, appunto, viene definito *data governance* –, il mutamento concettuale da un paradigma di esclusività sui dati a uno improntato ad accessibilità e condivisione è ora accompagnato da scelte di politica legislativa che paiono sottendere «un modello multipolare, nel quale le istanze di protezione dei dati coesisteranno con pari dignità con quelle di libero accesso e riuso dei dati medesimi»[4]. La libera circolazione dei dati, fulcro dell'innovazione digitale e della creazione di uno

[1] Le esigenze di regolazione dei mercati di dati vengono efficacemente descritte da L. Taylor, H. Mukiri-Smith, T. Petročnik, L. Savolainen, A. Martin, *(Re)making data markets: an exploration of the regulatory challenges*, in *Law, Innovation and Technology*, 2, 2022, 355 ss. La società "datificata", del resto, imponeva una scelta in questo senso: nell'ampia letteratura di riferimento in tema di c.d. *datification*, si rinvia a V. Mayer-Schönberger, K. Cukier, *Big Data: a revolution that will transform how we live, work, and think*, Mariner Books, New York, 2014; L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

[2] Commissione europea, Comunicazione *A European strategy for data*, 19.2.2020 COM(2020).

[3] Per il concetto di *data governance* e la sua evoluzione, vd. T. Streinz, *The Evolution of European Data Law*, in P. Craig e G. de Búrca (a cura di), *The Evolution of EU Law*, Oxford, 2021 (3ª ed.), 902 ss.; S. Viljoen, *A Relational Theory of Data Governance*, in *Yale Law Journal*, 2, 2021, 573 ss.

[4] G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista Trimestrale di Diritto Pubblico*, 4/2022, 975. Sulla dialettica esclusività-accessibilità, si fa riferimento alla ricostruzione di J. Drexl, *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, in *JIPITEC*, 8, 2017, 257 ss.; sul punto, rimangono sempre attuali le parole di S. Rodotà, *Il terribile diritto*, Bologna, 2013 (3ª ed.), 463: «[m]uta lo sguardo sulla proprietà […] si potrebbe dire che *si passa da una proprietà "esclusiva" ad una "inclusiva"*. Più correttamente, questa situazione può essere descritta come riconoscimento della legittimità che al medesimo bene facciano capo soggetti e interessi diversi. *Il discorso sull'esclusione viene tramutato così in quello sull'accessibilità*.».

"spazio comune europeo di dati"[5], viene così a essere stimolata per il tramite di meccanismi di incentivo all'accesso o alla condivisione, assecondando un utilizzo trasversale dei dati che sia volto ad assicurare la creazione di benefici per i cittadini[6]. In linea con quanto descritto finora, lo sviluppo di politiche di apertura nel governo dei dati mira a massimizzare, in particolar modo, la circolazione e l'utilizzo di dati per scopi di utilità e interesse generale (contrasto al cambiamento climatico, prevenzione delle pandemie, miglioramento dei servizi pubblici)[7]. Peraltro, tali iniziative di apertura e sensibilizzazione coinvolgono, nell'intenzione del legislatore europeo, anche gli stessi consociati. Così, valorizzando una visione che da tempo va affermandosi tra gli studiosi e in alcune esperienze applicative, meccanismi di "*data activism*" e forme di cittadinanza attiva possono essere incentivati, contribuendo all'evoluzione del concetto stesso di città, che, nel mondo interconnesso, diviene *smart city*[8].

L'attuale configurazione regolatoria conosce tre atti definiti – *Digital Markets Act* (DMA)[9], *Digital Services Act* (DSA)[10], *Data Governance Act* (DGA)[11] – e due proposte presentate dalla Commissione europea – *Data Act* (DA)[12], *Artificial Intelligence Act* (AIA)[13] –, che costituiscono i pilastri del progetto di predisposizione di un pacchetto digitale intrapreso dall'Unione europea[14]. La frammentazione legislativa cui l'UE si è arresa nel regolare tali fenomeni riflette i molteplici stimoli con i quali il legislatore si deve confrontare e il complesso rapporto tra le varie componenti della *data economy*[15].

Del resto, la complessità del sistema emerge con il solo considerare l'atteggiarsi della sequenza dati-algoritmi (cui, più propriamente, dovrebbe aggiungersi un terzo seg-

[5] M. Minghini - A. Kotsev - C. Granell, *A European Approach to the Establishment of Data Spaces*, in *Data*, 7, 118, 2022.

[6] Riassume tali obiettivi la Strategia europea in materia di dati, di cui il dato trasversale si ricava dalla promozione delle varie tipologie di flussi di dati (B2B, B2G, G2B). Un simile stimolo è richiesto anche dalle risultanze di indagini empiriche, basti pensare all'affermazione secondo la quale circa l'85% dei dati raccolti in Europa non viene riutilizzato (T. Ramge, V. Mayer-Schönberger, *Fuori i dati! Rompere i monopoli delle informazioni per rilanciare il progresso*, Milano, 2021, 39).

[7] Coerentemente con questo disegno, gli strumenti predisposti dal legislatore seguono le medesime finalità: a titolo esemplificativo, l'altruismo dei dati del *Data Governance Act* è previsto "per obiettivi di interesse generale", così come l'accesso forzato dei dati del settore privato da parte del settore pubblico (B2G) proposto nel *Data Act* sarebbe possibile solo "*under exceptional need*".

[8] Sul punto, S. Tranquilli, *Il nuovo citoyen européen nell'epoca del Data governance act*, in *Rivista di Digital Politics*, 1-2, 2022, 180; cfr. anche F. Musella, *Amministrazione 5.0*, in *Rivista di Digital Politics*, 1, 2021, 101.

[9] Regolamento (UE) 2022/1925.

[10] Regolamento (UE) 2022/2065.

[11] Regolamento (UE) 2022/868. D'ora in avanti, DGA.

[12] Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), COM(2022) 68 final.

[13] Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale), COM(2021) 206 final. D'ora in avanti, AIA.

[14] P.G. Picht - H. Richter, *EU Digital Regulation 2022: Data Desiderata*, in *GRUR International*, 5, 2022, 395; G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 971. Per una panoramica delle iniziative previste, si rinvia alla Comunicazione "Strategia europea per i dati" (vd. *supra*, nota 2).

[15] Su alcune implicazioni relative ai rapporti tra gli impianti normativi, vd. S. Tranquilli, *Il nuovo citoyen européen nell'epoca del Data governance act*, cit., 187-189.

mento, relativo alle piattaforme[16]) come elementi attorno ai quali ruota la moderna società informazionale: è riconosciuto che i dati operino allo stesso tempo come *input* e *output* dei processi produttivi che interessano i sistemi di intelligenza artificiale [17]. Da questa fondamentale interazione deriva un nesso inscindibile tra i dueelementi, che ne condiziona la futura operatività come l'uno strettamente dipendente dall'altro.

All'interno di questo disegno, le strategie regolatorie promosse dall'UE in risposta alle esigenze della nuova società digitale descrivono e alimentano – per scelta politica o per necessità tecnica – tale rapporto osmotico tra dati e algoritmi (o, più in generale, tra dati e sistemi di intelligenza artificiale)[18].

Ciò premesso, scopo del presente contributo è mettere in luce la relazione tra i due segmenti della sequenza e, per farlo, si propone di esaminare un esempio di interazione dati-algoritmi e le sue possibili implicazioni sul piano delle tutele dei soggetti coinvolti, facendo ricorso ai nuovi strumenti del pacchetto digitale UE. Dunque, a partire dalle esperienze applicative attualmente presenti in Italia, verrà descritta l'incidenza di alcune norme presenti nell'attuale contesto regolatorio – sia volte all'incentivazione delle nuove pratiche tecnologiche sia dirette ad imporvi dei limiti.

In via di prima approssimazione, è possibile distinguere due piani operativi nei quali l'interazione tra dati e algoritmi si può articolare: a) a monte – il legislatore europeo muove verso la predisposizione di strumenti abilitanti una maggiore circolazione dei dati, anche (e soprattutto) verso il settore pubblico, quali l'altruismo dei dati; b) a valle – la proposta regolatoria complessiva dell'UE vigila sull'utilizzo che di questi dati viene fatto attraverso gli algoritmi, imponendo il rispetto di alcuni principi strumentali a preservare i diritti fondamentali coinvolti e irreggimentando forme di tutela rispetto a pratiche predittive quali l'attribuzione di un punteggio sociale basato sui dati.

In altri termini, tra fenomeni quali l'altruismo dei dati (*data altruism*) e il punteggio sociale (*social scoring*) potrebbe scorgersi un nesso, si potrebbe dire, ipotattico[19]: il primo aspetto attiene alla fonte dei dati e consiste in una modalità di (incentivazione della) circolazione dei dati; il secondo riguarda l'attività sui dati ottenuti e consiste in una modalità di (*rectius*, distorsione nell') utilizzo che di essi viene fatto tramite il possibile ricorso a sistemi di intelligenza artificiale.

Attraverso il richiamo a evidenze empiriche e a prospettive applicative, allora, sarà possibile fornire una prima impressione circa i legami e l'interazione tra le varie com-

---

16 G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, 972.

17 F. Mezzanotte, *Access to Data: The Role of Consent and the Licensing Scheme*, in S. Lohsse, R. Schulze, D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, Oxford/Baden-Baden, 2017, 159 ss.

18 Sulla relazione tra dati e algoritmi, *ex multis*, vedasi V. Mayer-Schönberger, T. Ramge, *Das Digital: Markt, Wertschöpfung und Gerechtigkeit im Daten-kapitalismus*, 2017; WIPO, *WIPO Technology Trends 2019: Artificial Intelligence*, Geneva: World Intellectual Property Organization, 2019; Comunicazione 25.4.2018, *L'intelligenza artificiale per l'Europa*; M. Brkan, *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*, in *International Journal of Law and Information Technology*, 2, 2019, spec. 19 ss.

19 Intendendosi come "proposizione principale" l'attività che con i dati viene svolta dall'IA e come "proposizione subordinata" – e, in questo caso, cronologicamente antecedente – la modalità di raccolta dei dati stessi: la seconda è operata in funzione della prima e rappresenta una sola delle possibili modalità di raccolta dei dati diffuse nella prassi.

ponenti del sistema europeo di governo dei dati che va delineandosi (come combinazione di atti legislativi già approvati e proposte ancora da approvare).
A tal fine, lo studio si soffermerà, in particolare, sull'esperienza dell'Osservatorio Nazionale *Sharing Mobility*, che ha promosso un'indagine sulla mobilità urbana basata sull'analisi statistica di dati relativi agli spostamenti messi a disposizione volontariamente dagli stessi cittadini[20]; di recente, il Garante per la protezione dei dati personali ha avviato un'istruttoria nei confronti di tale iniziativa (accomunandola ad altri progetti) per scongiurare il rischio di quella che ha definito una cittadinanza "a punti", riproponendo la sottolineata (pericolosa) vicinanza tra cittadinanza attiva e rischi di profilazione[21].
Il dato comune alle esperienze interessate dalle istruttorie del Garante risiede nella predisposizione di meccanismi premiali incentivanti la condivisione "volontaria" dei dati (che, in alcuni casi, possono essere accompagnati dalla previsione di provvedimenti *lato sensu* sanzionatori) rispetto ai quali è opportuno compiere gli accertamenti necessari a scongiurare eventuali derive discriminatorie che dall'attribuzione di un punteggio – e dal corrispondente meccanismo di premi e sanzioni – possono scaturire.
Pertanto, dopo una disamina dei tratti caratterizzanti le due pratiche in questione – altruismo dei dati (2.) e punteggio sociale (3.) –, si procederà a un'analisi più dettagliata delle esperienze oggetto delle istruttorie del Garante privacy (in particolare, il caso dell'Osservatorio Nazionale Sharing Mobility) (4.) e della loro compatibilità con il quadro regolatorio europeo in via di formazione – sia vigente, il DGA (4.1.), sia ancora da approvare, l'AIA (4.2.). All'esito di questa trattazione, saranno offerte delle osservazioni conclusive in merito alle implicazioni che la diffusione di simili iniziative può generare nel rapporto tra Stato e cittadino nella società digitale, cercando di individuare dove le stesse si collochino nell'alternativa tra forme di cittadinanza attiva e "a punti" (5.).

2. Altruismo dei dati. Oltre il recepimento normativo

Per quanto riguarda il primo dei due piani operativi sopra individuati – relativo alla raccolta dei dati come oggetto della successiva attività degli algoritmi – la Strategia europea mira a introdurre strumenti idonei a garantire una maggiore condivisione dei dati relativamente a tutti i flussi che possono venire in considerazione nelle prassi applicative (*business-to-business* o B2B, *government-to-business* o G2B, *business-to-government* o B2G).
Recentemente, come forma di reazione alla scarsa predisposizione dei settori privato e pubblico a interagire tra loro, le discussioni in merito all'accrescimento della fiducia circa la condivisione dei dati sono andate intensificandosi. Così, in linea con la diffusione di una cultura di "filantropia digitale"[22], anche la strategia regolatoria europea ha

[20] Le principali informazioni sull'iniziativa sono reperibili sul sito osservatoriosharingmobility.it

[21] Garante Privacy, comunicato stampa 8 giugno 2022, «"Cittadinanza a punti": Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini "virtuosi"».

[22] M. Taddeo, *Data Philanthropy and Individual Rights*, in *Minds and Machines*, 27, 2017, 1–5; cfr. anche R.

cominciato a farsi carico delle suddette istanze: il DGA dedica un intero Capo (il Capo IV) a quello che viene definito come "altruismo dei dati" (*data altruism*)[23].

A livello definitorio, l'art. 2, par. 1, n. 16) DGA spiega come per altruismo dei dati si intenda: «la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».

Gli elencati obiettivi di interesse generale informano, perciò, l'utilizzo dei dati così raccolti. Del resto, la logica sottesa all'altruismo dei dati è in linea con l'obiettivo di superare un sistema in cui la detenzione dei dati si concentra nelle mani di poche imprese private (peraltro non europee) e di consentire di contribuire, volontariamente, al bene comune[24]. In altri termini, la finalità cui questo nuovo strumento mira è «contribuire allo sviluppo di *pool* di dati messi a disposizione sulla base dell'altruismo dei dati, che abbiano dimensioni sufficienti da consentire l'analisi dei dati e l'apprendimento automatico, anche attraverso l'Unione»[25]. Per far sì che ciò avvenga, lo stesso Regolamento rimanda alla definizione di politiche nazionali da parte degli Stati membri che si muovano in questa direzione – agevolando l'altruismo dei dati per mezzo, ad esempio, della previsione di strumenti di facile utilizzo per dare il consenso o l'autorizzazione o di campagne di sensibilizzazione[26].

Dalla lettura del testo normativo, sembrano emergere alcuni elementi costitutivi di particolare rilevanza nelle pratiche di altruismo. Si tratta dei connotati della: a) volontarietà; b) assenza di compenso; c) funzionalizzazione a obiettivi di interesse generale. A questa considerazione si aggiunge il rilievo secondo il quale il reticolato predisposto dal DGA si innesta, in ogni caso, sulle disposizioni del Regolamento generale sulla

Kirkpatrick, *A new type of philanthropy: donating data*, in *Harvard Business Review*, 21 marzo 2013. Se vogliamo, una visione coerente con il bisogno di solidarietà (in questo contesto, una solidarietà 'digitale') fatto proprio da S. Rodotà, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2014. Tuttavia, da parte di alcuni è stato notato come «[l]a scelta del termine "altruismo" risulta altrettanto problematica implicando che non acconsentire alla condivisione dei dati equivalga ad una manifestazione di "egoismo"» (F. Caloprisco, *Data Governance Act. Condivisione e "altruismo" dei dati*, in *I Post di AISDUE*, III, 2021, 5 maggio 2021, 60).

[23] Sul punto, vd. C. Kruesz - F. Zopf, *The Concept of Data Altruism of the Draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU*, in *European Data Protection Law Review*, 4, 2021, 569 ss. Per alcune prime analisi del nuovo regolamento, si rinvia a F. Caloprisco, *Data Governance Act. Condivisione e "altruismo" dei dati*, cit.; S. Tranquilli, *Il nuovo citoyen européen nell'epoca del Data governance act*, cit.; L. Lionello, *La creazione del mercato europeo dei dati: sfide e prospettive*, in *Diritto del commercio internazionale*, 3, 2021, spec. 688-689.

[24] Sul punto, in generale, vd. A. Alemanno, *Data for Good. Unlocking Privately - Held Data to the Benefit of the Many*, in *European Journal of Risk Regulation*, 2, 2018, 183 ss.

[25] Considerando 45 DGA.

[26] Art. 16 e considerando 45 DGA.

protezione dei dati (RGDP o GDPR) ed è condizionato al suo rispetto, in particolare per quanto concerne il tema dell'altruismo dei dati. Difatti, non solo la condivisione volontaria è subordinata a un consenso che deve rispettare le condizioni di liceità poste dal GDPR, ma anche il trattamento dei dati da parte delle organizzazioni dovrà rispettare il medesimo impianto normativo[27]. In quest'ottica, peraltro, il DGA ipotizza l'introduzione di un "modulo europeo comune di consenso all'altruismo dei dati", che, strutturato secondo un approccio modulare che permette una personalizzazione in funzione di settori specifici e finalità diverse, garantirebbe uniformità, nel formato, tra gli Stati membri[28].

Così delineato, l'altruismo intercetterebbe due esigenze: da un lato, l'aspirazione a ridurre la distanza tra i dati a disposizione del settore privato e quelli detenuti dal settore pubblico – sostenuta anche con il tentativo di inserire, nella proposta di *Data Act*, un eccezionale meccanismo di accesso forzato ai dati detenuti dai privati da parte del settore pubblico che si affianchi ai modelli di condivisione volontaria[29]; dall'altro, l'intenzione di coinvolgere i cittadini, concorrendo a garantire una maggiore consapevolezza nella raccolta e nell'utilizzo dei dati che li riguardano (c.d. *self data awareness*).

Lo strumento che il DGA ha individuato come mezzo di incentivazione di queste pratiche è l'istituzione di organismi *ad hoc*. Più precisamente, nell'ottica di aumentare la fiducia nei confronti delle iniziative di condivisione dei dati, il DGA predispone la possibilità di istituire "organizzazioni per l'altruismo dei dati". Tali organismi, che derogano alle disposizioni relative ai servizi di intermediazione del Capo III (art. 15), necessitano del possesso di alcuni requisiti affinché possano essere qualificati come tali. L'art. 18 DGA fissa i requisiti generali per la registrazione presso un registro pubblico di cui all'art. 19 DGA. A tal fine, l'entità deve: «a) svolgere attività di altruismo dei dati; b) essere una persona giuridica costituita a norma del diritto nazionale per conseguire obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile; c) operare senza scopo di lucro ed essere giuridicamente indipendente da qualsiasi entità che operi a scopo di lucro; d) svolgere le proprie attività di altruismo dei dati mediante una struttura funzionalmente separata dalle sue altre attività; e) rispettare il codice di cui all'articolo 22, paragrafo 1, al più tardi entro 18 mesi dopo la data di entrata in vigore

[27] Considerando 50 DGA: «Qualora siano titolari del trattamento o responsabili del trattamento dei dati ai sensi del regolamento (UE) 2016/679, le organizzazioni per l'altruismo dei dati riconosciute dovrebbero rispettare le norme di tale regolamento. L'altruismo dei dati sarebbe basato in genere sul consenso degli interessati ai sensi dell'articolo 6, paragrafo 1, lettera a), e dell'articolo 9, paragrafo 2, lettera a), del regolamento (UE) 2016/679, che dovrebbe rispettare i requisiti per il consenso lecito conformemente agli articoli 7 e 8 di tale regolamento. […]». Quanto alla specificità del consenso, S. Tranquilli, *Il nuovo citoyen européen nell'epoca del Data governance act*, cit., 193 evidenzia come «[u]na descrizione generica, quale, ad esempio, la finalità di rendere i dati disponibili "per il bene pubblico" o "per la ricerca scientifica" sarebbe considerata insufficiente a soddisfare il requisito della specificità del consenso». Vd. Anche Caloprisco, *Data Governance Act. Condivisione e "altruismo" dei dati*, cit., 63.

[28] Art. 25, par. 1 e par. 2.

[29] Tale meccanismo, la cui portata sarebbe da verificare in concreto e sul quale si sono appuntate le prime critiche rispetto alla formulazione del testo legislativo, è contenuto nel Capo V e dev'essere giustificato da necessità eccezionali (*exceptional need*). Sul punto, vedasi H. Richter, *The Law and Policy of Government Access to Private Sector Data (B2G Data Sharing),* in Bundesministerium der Justiz und für Verbraucherschutz, Max-Planck-Institut für Innovation und Wettbewerb (a cura di), *Data Access, Consumer Interests and Public Welfare*, 2021, 529.

degli atti delegati di cui a tale paragrafo»[30].

Ai requisiti generali si aggiungono poi una serie di obblighi: sia di trasparenza (riguardanti le modalità del trattamento dei dati, le persone fisiche e giuridiche che possono accedervi, gli obiettivi di carattere generale perseguiti), sia di assistenza nel prestare o revocare il consenso sia, ancora, di rispetto delle finalità di utilizzo e di garanzia di un elevato livello di sicurezza per la conservazione e il trattamento[31].

In ogni caso, il Regolamento fa salva la possibilità di svolgere attività nell'ambito dell'altruismo dei dati anche a prescindere dalla qualificazione di organizzazione riconosciuta[32].

Una volta registrate, il ruolo di tali organizzazioni pare potersi ricondurre a tre tipologie di attività: a) la raccolta di dati pertinenti direttamente da persone fisiche e giuridiche; b) il trattamento di dati raccolti da terzi; c) lo svolgimento di entrambe le attività, per finalità del trattamento dalle stesse stabilite (in alternativa, saranno soggetti terzi a svolgere il trattamento, per le medesime finalità)[33].

Tuttavia, le nobili intenzioni del testo si scontrano con i limiti degli strumenti che sono stati scelti per attuarle: da più parti è stato sottolineato come la tendenza a un'eccessiva procedimentalizzazione e burocratizzazione, insieme all'assenza di disposizioni di natura sostanziale relative al consenso da prestare, rischino di ridurre l'altruismo a una mera formula vuota, di facciata[34].

Ciononostante, il messaggio comunicativo sembra essere in grado di dispiegare una certa efficacia: alle iniziative che già esistevano in tema di altruismo dei dati (*decode*, *OpenSchufa*)[35], si sono aggiunti numerosi progetti originati dalle necessità legate all'emergenza pandemica (le *app* di *contact tracing*)[36]; inoltre, e soprattutto, le pubbliche amministrazioni hanno, in alcuni casi, accolto questa formula – talvolta in maniera atecnica – con la finalità di sviluppare una proficua collaborazione con i cittadini per il miglioramento di servizi pubblici[37].

In ogni caso, a fronte di una volontaria e "filantropica" cooperazione tra privati e settore pubblico, rimane da verificare il rispetto dei limiti posti all'utilizzo che dei dati

[30] Art. 18 DGA.

[31] Artt. 20 e 21 DGA. Ne danno conto F. Caloprisco, *Data Governance Act. Condivisione e "altruismo" dei dati*, cit., 72; G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 988.

[32] Considerando 48.

[33] Questo è quanto pare derivarsi dal contenuto del considerando 50.

[34] G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 991, in cui si riporta il rischio che si tratti di «un dispositivo di *marketing* normativo privo di significativo impatto operazionale»; similmente, sull'eccessiva burocratizzazione, S. Tranquilli, *Il nuovo citoyen européen nell'epoca del Data governance act*, cit., 194, la quale ivi sottolinea, inoltre, che le disposizioni contenute nel DGA assomigliano più a quelle di una direttiva che non a quelle di un regolamento; cfr. anche, in termini critici sul DGA, W. Veil, *Data altruism*, AlgorithmWatch Discussion Paper #1, 2021.

[35] Sulla prima iniziativa, volta a consentire ai cittadini di controllare se condividere o meno i propri dati, decodeproject.eu; per quanto riguarda la seconda, finalizzata a indagare le pratiche del sistema di punteggio tedesco SCHUFA, openschufa.de. Gli esempi sono tratti da W. Veil, *Data altruism: how the EU is screwing up a good idea*, cit.

[36] Sul punto, si rinvia a V. Zeno-Zencovich, G. Resta, E. Poillot, G. Lenzini, *Data protection in the context of Covid-19. A short (hi)story of tracing applications*, Roma TrE-Press, 2021.

[37] Di alcune di queste esperienze si darà conto *infra*, par. 4.

viene compiuto.

3. Punteggio sociale. Dal modello cinese alle applicazioni europee

Forniti volontariamente dai privati o dai cittadini, acquisiti coattivamente per finalità di interesse pubblico, ottenuti sulla base di contratti o collaborazioni tra esponenti del settore pubblico e del settore privato, i dati alimentano le macchine. E, con una frequenza sempre maggiore, «[a]ziende e governi sfruttano […] le macchine per giudicare le persone, consentendo a chi sviluppa le AI di accumulare un potere enorme. Il potere è la capacità di far compiere a una persona azioni che altrimenti non farebbe»[38]. Dunque, nell'ambito della sequenza dati-algoritmi, i sistemi di intelligenza artificiale si inseriscono a questo punto della catena, utilizzando i dati che li alimentano per generare a loro volta dati come *output*. Nonostante processi di vario genere (predittivi, statistici, di profilazione) siano regolarmente in atto da parte di aziende private, una particolare attenzione dev'essere rivolta all'eventualità che siano soggetti pubblici a servirsi di questo tipo di attività, eventualità sempre più attuale con la proliferazione dei progetti di *smart city*.

In particolare, tra le possibili applicazioni cui la raccolta di dati combinata all'azione degli algoritmi dà luogo, sebbene ancora poco esplorato dagli studiosi (se non con riguardo all'esperienza cinese[39]), il tema dei sistemi idonei ad attribuire un punteggio sociale sulla base dei dati analizzati (*social scoring*) va acquisendo – sia sul piano empirico che a livello di politiche legislative – una rilevanza sempre maggiore, tale da non poter più essere trascurato.

Il *social scoring* costituisce il portato del carattere pervasivo della tecnologia in ogni settore della società e della quotidianità, in grado di incidere, per quello che qui interessa maggiormente, sul rapporto tra pubblico e privato e, più specificamente, sulla relazione Stato-cittadino[40]. Esso consiste nell'azione di sistemi di intelligenza artificiale che, sulla base di dati a vario titolo ottenuti (sia *online input* che *offline input*), attribuiscono un punteggio sociale alle persone. Più precisamente, l'operare congiunto delle nuove tecnologie (sistemi IA, algoritmi, *big data*, riconoscimento facciale, sensori delle *smart city*, …) produce valutazioni (di tipo numerico) classificatorie a partire da comportamenti,

[38] F. Pasquale, *Le nuove leggi della robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale*, Luiss University Press, 2021, 166.

[39] F. Liang - Y. Chen, *The making of "good" citizens: China's Social Credit Systems and infrastructures of social quantification*, in *Policy & Internet*, 14, 2022, 114 ss.; D. Mac Síthigh - M. Siems, *The Chinese social credit system: A model for other countries?*, in *EUI Working Papers*, 1, 2019. Diverso il livello di approfondimento scientifico per quanto riguarda simili sistemi come esperienze legate al mondo creditizio, dove meccanismi di questo tipo sono molto diffusi: sul punto, si rinvia a P. Manes, Credit scoring *assicurativo,* machine learning *e profilo di rischio: nuove prospettive*, in *Contratto e Impresa*, 2, 2021, 469 ss.; per un esame della tematica, a livello comparatistico, nel Regno Unito, si veda N. Aggarwal, *The Norms of Algorithmic Credit Scoring*, in *The Cambridge Law Journal*, 1, 2021, 42 ss.

[40] G. Sciascia, *Reputazione e potere: il* social scoring *tra distopia e realtà*, in *Giornale di diritto amministrativo*, 3, 2021, 318: «Il *social scoring* costituisce un esempio emblematico delle trasformazioni e delle evoluzioni che riguardano i rapporti tra poteri pubblici, nuove tecnologie e libertà».

preferenze, violazioni (e, nelle sue più estreme configurazioni, opinioni espresse sui *social network*). Le analisi operate sulla base di questi elementi generano un punteggio indicativo del grado di affidabilità del singolo, creando dei profili, e rendono possibile la corresponsione di premi o sanzioni rispetto al comportamento di ciascuno[41]. Tali risultati categorizzanti rischiano di generare inaccettabili conseguenze discriminatorie nell'ampliamento o nella restrizione della sfera giuridica individuale[42], soprattutto quando dotate di elevato potenziale in termini di manipolazione inconsapevole delle persone e controllo sociale[43]. Calate nel rapporto tra Stato e cittadino finirebbero, finanche, per delineare un nuovo concetto di cittadinanza, allineato alle peculiarità delle "città intelligenti"[44].

In ultima istanza, «[i] sistemi di credito sociale non sono solo progetti giuridici, ma anche culturali e politici»[45].

Quanto all'origine di questi progetti, generalmente, se ne parla come di derivazioni di sistemi già oggetto di implementazione, a vario livello, nella società cinese: in Cina, il sistema dei crediti sociali (Scs) si concretizza in un costante monitoraggio che, dacché originariamente limitato alle aziende, solo nel 2014 è stato esteso ufficialmente alle persone, quando il Consiglio di Stato cinese ha annunciato delle "linee guida per la promozione di un sistema di credito sociale" basate sulla valutazione della reputazione mediante l'attribuzione di un punteggio[46].

Sul piano storico, gli studiosi che si occupano dell'esperienza cinese spesso avvertono riguardo alle peculiarità che la digitalizzazione assume in Cina, soprattutto quanto al recepimento di certe dinamiche all'interno della società: in questo caso, si afferma, «[i]l sistema dei crediti sociali ha radici antiche nella cultura cinese»[47]. Questo si spiega considerando che il percorso iniziato con la filosofia confuciana, con la quale la morale diveniva parte integrante della nuova società, sembra ora evolversi nei termini in cui sono le nuove tecnologie a consentire di calcolare la moralità dei cittadini[48].

Tuttavia, è bene specificare che il modello di Scs cinese non consiste in un sistema unificato, ma in diversi sistemi (*black list*, *red list*, progetti pilota, …), tutti in fase di sperimentazione e tutti diretti all'attribuzione di un punteggio di affidabilità a cittadini

---

41 S. Pieranni, *Red Mirror. Il nostro futuro si scrive in Cina*, Roma - Bari, 2020, 96.

42 G. Sciascia, *Reputazione e potere*, cit.; K. Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021, 205 laddove l'Autrice aggiunge che spesso questi sistemi (e, in generale, sistemi di controllo da parte dello Stato) vengono testati sulle categorie più deboli, in particolare portando l'esempio dei rifugiati; C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown, 2016, *passim*.

43 Cfr. considerando 15 AIA.

44 S. Pieranni, *Red Mirror*, cit., *passim*; G. Sciascia, *Reputazione e potere*, cit.

45 F. Pasquale, *Le nuove leggi della robotica*, cit., 162.

46 Ivi, 160; S. Pieranni, *Red Mirror*, cit.; peraltro, recentemente è stata divulgata in Cina la bozza di una legge che disciplina l'istituzione del sistema di credito sociale, la quale ne distingue l'operatività in quattro settori (governativo, commerciale, sociale, giudiziario) e ne fornirebbe così una solida base legale.

47 S. Pieranni, *Red Mirror*, cit., 98.

48 *Ibid.*; cfr. rilievi simili in F. Nasi, *Il sistema di credito sociale cinese*, su pandorarivista.it, 28 dicembre 2021che richiama «il concetto di *chéngxìn* (诚信), che può essere tradotto come onestà, affidabilità o integrità».

e aziende sulla base di parametri fissati da Stato o amministrazioni locali[49].

Nella sua configurazione tradizionale, a cavallo tra le varie esperienze globali, il *social scoring* comprende e influenza opportunità di ogni tipo (la possibilità di viaggiare, l'istruzione, l'ottenimento di prestiti, …), rendendole più o meno difficoltose o del tutto inibendole. Di esso, vengono identificati tre elementi caratterizzanti: universalità, effetto a onda e rete di conseguenze[50]. L'universalità concerne la fonte delle informazioni, dal momento che universale, in quanto basata su informazioni di qualsiasi provenienza, è la gamma di dati a disposizione dei Scs. L'effetto a onda fa riferimento alla eterogeneità di conseguenze di una eventuale violazione rispetto al contesto in cui la stessa è stata posta in essere. Infine, la rete di conseguenze interessa gli effetti (positivi o, soprattutto, negativi) che possono prodursi in capo a soggetti diversi rispetto a colui che realizza la condotta.

Il funzionamento del *social scoring* si ispira – come la maggior parte delle applicazioni e dei dispositivi *smart* oggi diffusi – a una logica di *gamification*, che «si verifica quando elementi divertenti simili a quelli di un gioco compaiono in diverse attività, e tutto dipende dal punteggio quantificato»[51]. L'inserimento di premi, incentivi, ma anche punizioni o sanzioni, può avvenire in relazione a qualsiasi tipo di attività e ciò concorre a rendere più coinvolgente l'esperienza legata all'attività in questione, fino ad arrivare potenzialmente a coinvolgere ogni aspetto della vita. In base ai *feedback* che ricevono, gli utenti sono portati a modificare il loro comportamento al fine di migliorare il proprio record o punteggio. In questo modo, è facile presumere che nei cittadini sorga una «personalità algoritmica volta a massimizzare il proprio status»[52], sia individuale che all'interno della collettività. Secondo gli osservatori più critici, gli aspetti 'gamificatori' della sorveglianza nascondono gli algoritmi e «incanalano la soggettività in evoluzione»[53], con l'inevitabile conseguenza di indirizzare l'identità e plasmare i modelli comportamentali secondo una logica di assuefazione ai *feedback*, ai punteggi, ai traguardi personali, senza che l'individuo se ne renda conto, producendo un effetto inconsapevole di autosorveglianza[54].

---

[49] S. Pieranni, *Red Mirror*, cit., 96.

[50] F. Pasquale, *Le nuove leggi della robotica*, cit., 161.

[51] D. Lyon, *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori*, Luiss University Press, 2020, 140.

[52] F. Pasquale, *Le nuove leggi della robotica*, cit.; Id., *The Algorithmic Self*, in *The Hedgehog Review*, 1, 2015; cfr. anche P. de Filippi, *The Social Credit System as a New Regulatory Approach: From 'Code-Based' to 'Market-Based' Regulation*, in *verfassungsblog.de*, 24 giugno 2019.

[53] J. E. Cohen, *The Surveillance-Innovation Complex: The Irony of the Participatory Turn*, in D. Barney - G. Coleman - C. Ross - J. Sterne - T. Tembeck (a cura di) *The Participatory Condition*, University of Minnesota Press, 2015, 5 («*channel evolving subjectivity*»). Riecheggiando, in un certo senso, quanto S. Rodotà, *Protezione dei dati e circolazione delle informazioni*, in Id., *Tecnologie e diritti*, Bologna, 2021 (2ª ed.), 87, anticipava con riguardo agli effetti distorsivi delle tendenze classificatorie, il quale già lucidamente avvertiva circa le possibili conseguenze distorsive in termini sociali quando, anticipando il concetto di 'categorizzazione', affermava che «[l]a categorizzazione di individui e gruppi, inoltre, rischia di annullare la capacità di percepire sfumature sottili, gusti non abituali»; in merito, sulle conseguenze della raccolta di informazioni, cfr. anche Id. *Elaboratori elettronici e controllo sociale*, Bologna, 1973 (ristampa inalterata, Jovene 2018).

[54] D. Lyon, *La cultura della sorveglianza*, cit., 139-140, attuando quello che J. Whitson, *Gaming the quantified self*, in *Surveillance and Society*, 1-2, 2013, definisce «quantificare la cura di sé». Pare utile ricordare che le

Sul piano più prettamente giuridico, un apporto, a livello definitorio, rispetto a simili fenomeni, si rinviene nella recente proposta di regolamento sull'intelligenza artificiale: l'art. 5, I, AIA nel vietare determinate pratiche di intelligenza artificiale secondo un approccio *risk-based*, include soltanto alcune tipologie di *social scoring* e per esso intende il ricorso a «sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste».

Al netto di eventuali considerazioni circa l'effettivo orizzonte applicativo della fattispecie[55], è opportuno sottolineare che la (provvisoria) formulazione si appunta, quindi, sul concetto di "affidabilità" (*trustworthiness*), che, come hanno fatto notare i primi commentatori, innova rispetto a quanto era stato proposto dall'*High Level Expert Group*-AI, nel quale si era, invece, fatto riferimento a valutazioni inerenti alla "personalità" o alla "integrità morale"[56].

L'espressa previsione (nonché, a determinate condizioni, il divieto) dei meccanismi attributivi di un punteggio sociale all'interno dell'impianto normativo che va delineandosi nell'ambito della Strategia europea per i dati rivela una latente preoccupazione circa l'espansione e l'adozione di siffatti sistemi anche in Occidente[57]. Del resto, esistono anche in ambito europeo alcune esperienze applicative già sperimentate e, in taluni casi, non tollerate dagli ordinamenti da esse interessati.

Per fornire, brevemente, alcuni esempi, nel 2014 era stato avviato dal governo olandese SyRI (*System Risk Indication*), un algoritmo di profilazione del rischio (*risk profiling*) finalizzato alla protezione del sistema di assistenza sociale nazionale e ideato per rilevare possibili frodi da parte dei beneficiari di misure di assistenza. Tuttavia, nonostante la presenza di un'espressa previsione normativa come base giuridica, il Tribunale dell'Aja ne ha sancito l'illegittimità alla luce della violazione del diritto alla *privacy* come riconosciuto dall'art. 8 CEDU[58].

Come ulteriore modello di sistema di profilazione di rischio può richiamarsi l'esperienza danese, iniziata nel 2018, relativa al c.d. "*Gladsaxe model*", volto all'individuazione di situazioni di rischio riconducibili a minori in condizioni di particolare vulnerabilità

medesime dinamiche sono indagate in S. Zuboff, *The age of surveillance capitalism*, Profile Books Ltd, 2019. Sugli effetti distorsivi di una "società a punteggio", cfr. anche D. K. Citron, F. Pasquale, *The Scored Society: Due Process for Automated Predictions*, in *Washington Law Review*, 1, 2014, 7 ss.

[55] Che verranno svolte *infra*, par. 4.2.

[56] Lo sottolineano M. Veale - F. Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, in *Computer Law Review International*, 4, 2021, 100 dove rimandano a High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, 34 e High-Level Expert Group on Artificial Intelligence, *Policy and Investment Recommendations for Trustworthy AI*, 2019, 20.

[57] Nell'occuparsi della normativa europea, il presente contributo tralascia l'esperienza americana, rispetto alla quale è però doveroso il rinvio al caso più conosciuto, relativo all'algoritmo COMPAS sul rischio di recidiva e alla famosa controversia *State v. Loomis* che ne è scaturita. Per una disamina completa, vd. H. Liu - C. Lin - Y. Chen, *Beyond* State v. Loomis*: artificial intelligence, government algorithmization and accountability*, in *International Journal of Law and Information Technology*, 2, 2019, 122 ss.

[58] Per un'analisi dettagliata delle implicazioni del caso e della decisione, si rinvia a G. Avanzini, *Intelligenza artificiale e nuovi modelli di vigilanza pubblica in Francia e Olanda*, in *Giornale di diritto amministrativo*, 3, 2022, 322-323.

familiare; il modello, per via delle pressioni provenienti dall'opinione pubblica e dal mondo accademico, nonché a causa della scoperta di un'attività di raccolta di dati molto più intensa di quanto non fosse necessario da parte delle amministrazioni coinvolte, è stato bloccato dallo stesso governo danese[59].

Ancora, in Germania, il progetto *OpenSCHUFA* – di fatto, espressione di una forma di altruismo dei dati già prima della sua espressa previsione – ha fatto luce su alcune criticità esistenti in merito all'operatività del sistema di credito SCHUFA, diretto a stabilire, a fronte di dati raccolti in settori tra loro eterogenei, un punteggio dei cittadini relativo alla loro affidabilità creditizia, e idoneo a influenzare l'accesso a prodotti o servizi[60].

In un siffatto contesto evolutivo, la notizia delle istruttorie avviate dal Garante per la protezione dei dati personali volte a investigare il rischio di una cittadinanza "a punti" deve essere letta come il naturale esito di un processo di avvicinamento tecnologico di simili modelli – che mantengono comunque una significativa distanza dal modello cinese – ormai avviato.

All'esito di queste brevi considerazioni introduttive, occorre chiarire in che modo le iniziative attenzionate dal Garante possano rappresentare esperienze esemplificative della sequenza dati-algoritmi sottesa alle strategie regolatorie aventi ad oggetto le istanze della società digitale.

4. Le istruttorie del Garante privacy: il caso dell'Osservatorio Nazionale *Sharing Mobility*

Il nesso tra altruismo dei dati e punteggio sociale ha trovato una recente manifestazione in una serie di iniziative italiane interessate da alcune istruttorie del Garante per la protezione dei dati personali. Con un comunicato stampa dell'8 giugno 2022, il Garante divulgava la notizia di aver avviato tre istruttorie (che vanno ad aggiungersi a una, precedente e riguardante vicende astrattamente analoghe, resa nota con un comunicato del 3 maggio 2022), aventi ad oggetto «una serie di progetti promossi da soggetti pubblici e privati, che prevedono l'assegnazione di punteggi anche riguardo a raccolte di dati conferiti "volontariamente" dagli interessati»[61], a testimonianza della progressiva diffusione (e, conseguente, attenzione) che simili vicende vanno assumendo anche nell'ordinamento italiano.

La finalità dell'intervento dell'Autorità risiede nel prevenire «rischi connessi a meccanismi di profilazione che comportino una sorta di "cittadinanza a punti" e dai quali possano derivare conseguenze giuridiche negative sui diritti e le libertà degli interes-

[59] Vd. AlgorithmWatch, *Automated Society Report 2020*, Denmark, accessibile presso automatingsociety.algorithmwatch.org. Ne dà conto anche G. Sciascia, *Reputazione e potere*, cit., 321.

[60] In merito, vd. W. Veil, *Data altruism*, cit., 3; cfr. anche E. Brandimarte, *Should we let the algorithms decide? A critical assessment of Automated Decision Making in Europe*, 24-35 (capitolo III), tesi del Master in European Economic Studies presso il College of Europe Bruges, accessibile presso mayerbrown.com.

[61] Garante Privacy, comunicato stampa 8 giugno 2022, cit.

sati, inclusi i soggetti più vulnerabili»[62]. Del resto, le problematiche sottese alla sorveglianza e alle conseguenze che simili iniziative potrebbero avere in termini di profilazione maturano, in particolar modo, ove siano coinvolte pubbliche amministrazioni, la cui attività sarebbe in grado generare forme di sovrapposizione tra pubblico e privato, così incidendo sul rapporto tra Stato cittadino e, più in generale, sul concetto di cittadinanza[63].

Più specificamente, oggetto dell'azione del Garante sono tre progetti: 1) il progetto dell'Osservatorio Nazionale *Sharing Mobility*, in cui è coinvolto il Comune di Bologna, mediante il quale si mira a compiere un'analisi sulla mobilità urbana sulla base di dati volontariamente forniti dai cittadini, i quali potranno conseguentemente ottenere dei benefici (ad esempio, scontistiche); 2) lo "*Smart Citizen Wallet*" del Comune di Bologna, una sorta di "patente digitale" finalizzata, sempre su base volontaria, a individuare i cittadini più virtuosi attribuendo loro un punteggio e dei premi; 3) la "Carta dell'assegnatario" nel Comune di Fidenza, come sistema di valutazione a punti dei nuclei familiari nell'ambito degli alloggi di edilizia residenziale pubblica, che comprende anche la possibilità di determinare, a fronte di comportamenti valutati negativamente, conseguenze pregiudizievoli.

Oltre alle iniziative in questione, occorre richiamare il caso del sistema di *rating* reputazionale, ad opera della piattaforma *Mevaluate*, diretto al calcolo di una reputazione "reale" e "virtuale" di studenti, cui parrebbe aver aderito un istituto di istruzione superiore di Torino, parimenti oggetto di un'istruttoria avviata dall'Autorità[64].

Con un maggior sforzo ricostruttivo, si potrebbe sottolineare come i progetti attenzionati dal Garante, in verità, paiano porsi su una diversa scala di approfondimento nell'attività di attribuzione di un punteggio ai destinatari del servizio. Sarebbe, cioè, possibile distinguere molteplici gradienti di intensità rispetto a iniziative latamente riconducibili al *social scoring*[65]: sistemi che prevedono l'attribuzione di un punteggio, basato su dati provenienti da contesti molto distanti tra loro, e idonei a ricomprendere una vasta gamma di comportamenti si porrebbero al vertice della scala d'intensità; invece, sistemi con un campo di applicazione più circoscritto o privi dell'elemento classificatorio del punteggio si attesterebbero su un livello di intensità più basso. Tuttavia, in assenza di una scelta di politica legislativa netta e di disposizioni che ne individuino un ambito di operatività certo, rimane al momento dubbio ciò che rientra e ciò che

[62] *Ibidem*.

[63] Del resto, Y. Citino, *Cittadinanza "a punti" e social scoring: le pratiche scorrette dell'era dell'intelligenza artificiale*, in *diritticomparati.it*, 22 giugno 2022 ricorda come «si p[ossa] sostenere che all'istituto della cittadinanza si stiano pericolosamente affiancando logiche di mercato, che mirano a targettizzare la popolazione con l'obiettivo di estrarre dati».

[64] Garante Privacy, comunicato stampa 3 maggio 2022, "Scuola: rating reputazionale sotto la lente del Garante privacy. Avviata istruttoria su una piattaforma rivolta agli studenti". Non è la prima volta che un simile sistema privato diventa oggetto dell'attenzione del Garante: relativamente alla medesima azienda, si ricordi il recente pronunciamento della Corte di cassazione, su cui F. Bravo, *Rating reputazionale e trasparenza dell'algoritmo. Il caso "Mevaluate"*, in *Il diritto dell'informazione e dell'informatica*, 6, 2021, 1001 ss.

[65] S. Ianese, *Il social rating cerca di sbarcare in Italia. Ma quanti lo vogliono?*, in *smartius.it*, 19 luglio 2022 ad esempio, suddivide in tre categorie delle iniziative italiane di *social scoring*, alcune oggetto di istruttoria del Garante, definendole, rispettivamente di *citizen science*, di *social rating* "limitato", di *social rating* "puro", operando una distinzione basata, principalmente, sul campo di applicazione di ciascun progetto.

non rientra nel concetto di *social scoring* (del resto, se si dovesse seguire la linea posta dalla definizione resa nella proposta di AIA, rimarrebbero fuori tutti quei sistemi non produttivi di una valutazione sull'affidabilità del soggetto).

Ciò premesso, in generale, sulle istruttorie promosse dal Garante, pare utile soffermarsi su una delle iniziative in particolare, ossia il progetto dell'Osservatorio Nazionale *Sharing Mobility*, in quanto idoneo a illustrare i due piani operativi che il presente contributo è volto ad analizzare più da vicino. Difatti, esso non solo investe il tema dei possibili profili di vicinanza al *social scoring* (sebbene meno intensamente rispetto agli altri progetti coinvolti), ma, per quanto riguarda il momento, cronologicamente anteriore, della raccolta dei dati, l'iniziativa si ispira dichiaratamente a una logica di altruismo dei dati[66].

Per questi motivi, essa è idonea, su un piano prettamente descrittivo, a illustrare i due segmenti in cui è possibile scomporre la sequenza dati-algoritmi caratteristica della società digitale: in un primo momento, simili progetti fanno leva sul carattere volontario della raccolta dei dati, spingendosi fino a invocare forme di altruismo dei dati; in un secondo momento, il potenziale utilizzo che di questi dati viene fatto, connesso al riconoscimento di premi (o sanzioni) a coloro che vi partecipano, deve essere monitorato e, per questo motivo, ha stimolato l'interesse del Garante.

Il progetto dell'Osservatorio Nazionale *Sharing Mobility*, promosso dalla Fondazione per lo sviluppo sostenibile, dal Ministero della transizione ecologica e dal Ministero delle infrastrutture e della mobilità sostenibili, e in cui è coinvolto lo stesso Comune di Bologna, consiste in «un'indagine statistica a carattere sperimentale attraverso la quale il cittadino viene invitato a condividere i propri dati (apparentemente 'in forma anonima'), per consentire un'analisi della mobilità degli abitanti di Bologna [al cui termine] è previsto che il cittadino riceva premi offerti dai partner privati del Progetto»[67]. La finalità principale del trattamento dei dati, quindi, è l'analisi della mobilità delle persone in un determinato territorio per promuovere soluzioni che possano ridurre gli impatti negativi dei trasporti[68].

Alcuni aspetti sono ulteriormente specificati nella *Privacy Policy* del progetto, nella quale si chiarisce che 'Titolare del trattamento' è la Fondazione per lo sviluppo sostenibile e che la base giuridica del trattamento, effettuato dal Titolare, risiede: «a) nell'ambito del ruolo di promotore dell'Osservatorio Nazionale *Sharing Mobility* e di firmatario dell'Accordo di collaborazione con il MiTE registrato il 26/01/2021, ai sensi dell'art. 6 comma 1, lett. e) del GDPR; b) sul consenso che Lei esprime esplicitamente dopo la lettura di questa informativa»[69].

Per quanto riguarda i dati che vengono raccolti, si tratta sia di dati generati dall'applicazione sia di dati forniti tramite questionario dall'utente. Nella prima categoria rien-

[66] La pagina web del progetto spiega infatti che: «I *mobility data*, raccolti da smartphone o veicoli, registrano la posizione di una persona a intervalli regolari tramite GPS. I *mobility data* prendono spesso il nome di *bread-crumb* [e u]tilizzare questi dati per volontà esplicita di chi partecipa all'iniziativa, sotto il suo controllo e per delle finalità condivise, è l'aspetto centrale di questo nuovo tipo d'indagine e di un nuovo approccio all'uso dei dati personali: il *Data Altruism*» in osservatoriosharingmobility.it.

[67] Garante Privacy, comunicato stampa 8 giugno 2022, cit.

[68] Privacy Policy del progetto, accessibile presso *osservatoriosharingmobility.it.*

[69] Ivi, punto 4.

trano: i) dati sulla posizione; ii) dati del dispositivo; iii) dati di utilizzo. Nella seconda sono richieste informazioni eterogenee, quali indirizzo del domicilio, genere, utilizzo di servizi di *sharing*, età, reddito, titolo di studio, disponibilità di veicoli o di abbonamenti al trasporto pubblico, etc.[70]

Infine, è di rilievo la circostanza che tra i soggetti ai quali potranno essere comunicati i dati rientrano sia soggetti privati (erogatori dei premi all'esito della iniziativa) sia enti locali e soggetti pubblici[71].

Al riguardo, il Garante ha chiesto di chiarire alcuni aspetti: a) il ruolo dei soggetti pubblici e privati coinvolti; b) la base giuridica del trattamento; c) le modalità di funzionamento dell'*app* e i trattamenti ad essa connessi.

Sulla base di questi elementi, è possibile effettuare una prima valutazione in merito alla compatibilità di una simile iniziativa con il quadro regolatorio europeo *in fieri*. In altri termini, piuttosto che soffermarsi sulle questioni di cui, verosimilmente, dovrà occuparsi il Garante (relative all'eventuale anonimizzazione dei dati coinvolti, alla legittimità della base giuridica individuata per il trattamento, all'assimilabilità del trattamento a una profilazione vietata *ex* art. 22 GDPR)[72], il presente contributo cercherà di valutare il ruolo delle più recenti componenti del pacchetto digitale rispetto a iniziative quali quella del progetto dell'Osservatorio Nazionale *Sharing Mobility*, in maniera tale da "testare" la tenuta, in queste situazioni, della descritta deviazione di stampo promozionale della circolazione dei dati rispetto all'originario versante limitativo della protezione dei dati, alla cui tutela l'azione del Garante rimane preposta.

4.1. Alla luce del *Data Governance Act*

Quanto all'incidenza del regolamento (UE) 2022/868 (DGA) su iniziative quali il progetto dell'Osservatorio Nazionale *Sharing Mobility*, andrebbero affrontate alcune questioni.

Anzitutto, sarebbe opportuno misurare la principale innovazione operata dal DGA – l'introduzione delle "organizzazioni di altruismo dei dati" – nei termini di una possibile riconduzione dei soggetti promotori del progetto all'interno di tale figura.

In secondo luogo – questione strettamente connessa con la prima –, occorrerebbe valutare la compatibilità del concetto di "altruismo dei dati" con iniziative che prometto no premi e incentivi per facilitare la partecipazione.

Relativamente alla prima questione, deve ricordarsi, preliminarmente, che in dottrina è stato sottolineato il fatto che il DGA non prevede disposizioni puntuali in merito ai rapporti tra chi mette a disposizione i dati volontariamente e le organizzazioni di altruismo né rispetto ai rapporti delle organizzazioni con i terzi destinatari dei dati[73].

[70] Ivi, punto 6.

[71] Ivi, punto 8.

[72] In ragione, da un lato, dell'inopportunità di un'analisi priva di elementi materiali sufficienti, stante la paucità di informazioni rinvenibili riguardo alle iniziative in questione e, dall'altro, della maggiore coerenza rispetto al contesto regolatorio preso in considerazione con il presente scritto.

[73] R. Schildbach, *Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-*

Per questo motivo, l'apporto del DGA si arresta, nel caso di specie, alla possibilità di ricondurre i soggetti coinvolti in simili iniziative all'interno del nuovo paradigma delle organizzazioni altruistiche.

Nel caso dell'iniziativa dell'Osservatorio Nazionale *Sharing Mobility*, verosimilmente, uno 'studio di fattibilità' relativo all'eventuale qualificazione come "organizzazione di altruismo dei dati" andrebbe svolto con riguardo alla Fondazione per lo sviluppo sostenibile in quanto Titolare del trattamento e soggetto al quale vengono trasmessi i dati volontariamente dalle persone fisiche, ruoli che si è visto poter coincidere secondo quanto previsto dal considerando 50 DGA relativamente alle possibili attività delle organizzazioni riconosciute.

La registrazione *ex* art. 19 DGA è subordinata, come analizzato precedentemente, al ricorrere dei requisiti di cui all'art. 18 DGA[74].

Anzitutto, nel caso di specie, è possibile affermare che alcuni dei requisiti in questione potrebbero essere accertati solo in un secondo momento: più precisamente, si tratta delle lett. d) ed e), relative rispettivamente alla creazione di una struttura funzionalmente separata dalle sue altre attività e al rispetto del codice *ex* art. 22 DGA.

Invece, l'assolvimento di altre condizioni parrebbe già in astratto compatibile con il modello civilistico della fondazione di cui agli artt. 14 e ss. c.c. nonché con le caratteristiche statutarie della Fondazione per lo sviluppo sostenibile: le lett. b) e c), difatti, richiedono rispettivamente la forma di persona giuridica che consegue obiettivi di carattere generale e l'assenza di scopo di lucro[75].

Maggiori complicazioni sembrerebbero porre, nel caso di specie, la necessità, stabilita dalla lett. c), di essere giuridicamente indipendente da qualsiasi entità che operi a scopo di lucro e, soprattutto, la richiesta di cui alla lett. a), di svolgere attività di altruismo dei dati.

Su quest'ultimo aspetto si innesta l'ulteriore elemento di criticità che la vicenda in esame presenta: la compatibilità della corresponsione di un premio ai partecipanti all'esito dell'indagine statistica con l'attività di altruismo dei dati.

Difatti, il principale connotato degli strumenti altruistici, in linea con il loro fondamento "filantropico", è – insieme alla volontarietà – la gratuità. In tal senso, il considerando 45 DGA dispone che «[g]li interessati dovrebbero poter ricevere un compenso esclusivamente in relazione ai costi da loro sostenuti nel mettere a disposizione i propri dati per obiettivi di interesse generale». Pertanto, prevedere delle ricompense in cambio della condivisione dei propri dati potrebbe inficiare la pratica stessa di «svol-

Governance-Gesetzes, in *ZD,* 2022, 151; G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 988-989.

[74] Vd. *supra,* par. 2, 7. Non rileva, invece, in questa sede, la natura pubblica o privata del soggetto, diversamente da quanto sarà osservato *infra* (par. 4.2.) relativamente al *social scoring*. Vd. T. Tombal, *Business-to-Government data sharing for environmental purposes*, in *Network Industries Quarterly*, 3, 2022, 7 ss., spec. 8, in cui si afferma che: «*only public and private non-for-profit entities that pursue objectives of general interest and have a legally independent functionally separate structure can be recognised as DAOs*».

[75] Lo stesso statuto della Fondazione afferma che essa non ha uno scopo lucrativo e individua uno scopo di carattere generale quale «la promozione di uno sviluppo sostenibile, di una green economy nonché dello sviluppo tecnologico e dell'alta formazione tecnologica finalizzate all'elevata qualità ecologica». Art. 1 Statuto della Fondazione per lo sviluppo sostenibile, accessibile presso *fondazionesviluppososteni bile.org*.

gere attività di altruismo dei dati» richiesta come condizione per la registrazione delle entità come organizzazioni per l'altruismo.
Per come descritto dal Regolamento, l'espressione «svolgere attività di altruismo», riferita al requisito per la registrazione delle organizzazioni, sembrerebbe ricomprendere sia l'attività di raccogliere dati messi a disposizione volontariamente sia l'attività di operare sugli stessi un trattamento volto a obiettivi di interesse generale (o consentire a terzi di farlo).
Così interpretato il concetto di altruismo, la corresponsione di un premio potrebbe invalidare la natura altruistica della circolazione dei dati soprattutto alla fonte, nel momento della messa a disposizione da parte degli interessati, perché la condivisione dei dati che li riguardano non potrebbe più dirsi disinteressata.
In considerazione di tali rilievi, l'iniziativa promossa dall'Osservatorio Nazionale *Sharing Mobility* – così configurata – finirebbe per non rientrare nell'orizzonte applicativo della nuova disciplina.

4.2. Alla luce dell'*Artificial Intelligence Act*

Ancora, prendendo in considerazione il secondo segmento della sequenza dati-algoritmi, è utile analizzare il progetto dell'Osservatorio Nazionale *Sharing Mobility* e il connesso tema del *social scoring* alla luce della disciplina europea (non ancora in vigore) in materia di intelligenza artificiale.
In altri termini, occorre chiedersi se tale progetto possa rientrare o meno nelle attività vietate di cui all'art. 5 AIA. A tal fine, preliminarmente, è opportuno delimitare il campo di applicazione della norma.
La proposta avente ad oggetto un regolamento sull'intelligenza artificiale – è ormai noto[76] – si fonda su un meccanismo di gestione del rischio orientato alla tutela dei diritti fondamentali e, perciò, in linea con gli attributi del modello regolatorio che l'UE sta tentando di definire come alternativo alla dicotomia Cina-Stati Uniti[77]. Con questa definizione, si intende sottolineare la particolare fisionomia di un testo normativo quando delineato secondo una struttura a geometria variabile, a seconda del livello di rischio che le attività prese in considerazione presentano[78].
In questo contesto, nell'attuale configurazione dell'AIA, i meccanismi di *social scoring* aventi determinate caratteristiche sono inseriti nei sistemi "a rischio inaccettabile" e,

[76] M. Veale - F. Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, cit.; G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Il diritto dell'informazione e dell'informatica*, 2, 2022, 303 ss.; G. Resta, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale?,* in *Il diritto dell'informazione e dell'informatica*, 2, 2022, 323 ss.

[77] A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Faculty Books, 2020. Sui conflitti regolatori su scala globale, si rinvia a M. S. Erie - T. Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, in *New York University Journal of International Law and Politics*, 1, 2021, 1 ss.; E. Chiti - B. Marchetti, *Divergenti? Le strategie di Unione Europea e Stati Uniti in materia di intelligenza artificiale*, in *Rivista della Regolazione dei mercati*, 1, 2020, 29 ss.

[78] G. Resta, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale?*, cit., 339, il quale chiama "piramide del rischio" quella predisposta dal legislatore. La proposta distingue, infatti, tra sistemi vietati (*unacceptable risk*), ad alto rischio (*high risk*), a rischio limitato o minimo (*low or minimal risk*).

quindi, tra le pratiche vietate, in ragione della loro incompatibilità strutturale con la cornice assiologica che l'UE sta cercando di predisporre.

Tuttavia, il divieto non è generalizzato, bensì circoscritto ad alcune tipologie di *social scoring*. Affinché un determinato sistema possa essere o meno considerato rientrante nella portata del (futuro) divieto normativo, occorrerà valutare se tali pratiche comportino «un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche»[79]: a) in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; oppure b) che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità. In quest'ottica, più che a una valutazione in astratto, la riconduzione di questo o quel meccanismo all'interno del divieto predisposto dal legislatore sarebbe demandato a un accertamento in concreto, in considerazione degli effetti che l'intelligenza artificiale potrebbe generare nei confronti degli individui coinvolti (quando, cioè, essa «comporti il verificarsi»[80] di uno dei due scenari vietati). Il che rappresenta, a detta di molti, un ulteriore limite del testo normativo proposto, che non consente di operare una valida selezione *ex ante* dei sistemi IA produttivi di un tale risultato e, quindi, inammissibili; ciò, peraltro, faciliterebbe il sottrarsi dell'autorità coinvolta da responsabilità poiché la stessa potrebbe affermare, a tal fine, che la tecnica di *scoring* non sia stata un fattore determinante nella produzione degli effetti oggetto di divieto[81].

La natura limitata del divieto deriva oltretutto, sul piano soggettivo, dalla perimetrazione dei soggetti utilizzatori di questi tipi di sistemi, che devono essere usati da «un'autorità pubblica o per loro conto»[82] e, sul piano temporale, dal loro utilizzo «per un determinato periodo di tempo». Conseguenza di una tale delimitazione soggettiva – per questo motivo già oggetto di critiche sia in dottrina che a livello istituzionale[83] – è il fatto che la disposizione, nella formulazione attuale, lascia esenti i sistemi privati.

Nel caso del progetto dell'Osservatorio Nazionale *Sharing Mobility*, anche alla luce di queste considerazioni, meglio si comprende l'opportunità di un esame più approfondito – che è infatti parte dell'oggetto dell'istruttoria del Garante – circa il rapporto che sussiste tra i vari soggetti, sia di natura pubblica che privata, coinvolti nell'iniziativa. Ciò, peraltro, alla luce del fatto che è la stessa *Privacy Policy* a giustificare il trattamento facendo richiamo, oltre al consenso espresso dell'interessato, all'art. 6, par. 1, lett. e) GDPR (a tal fine richiamando il documento l'accordo di collaborazione con il MiTE

[79] Art. 5 AIA.

[80] Art. 5 AIA: le critiche si appuntano, nella versione originale, sul verbo "*leading to*".

[81] M. Ebers - V. R. S. Hoch - F. Rosenkranz - H. Ruschemeier - B. Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, in *J*, 4, 2021, 589 ss., spec. 592; dello stesso parere M. Veale - F. Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, cit., 100.

[82] Anche la relazione introduttiva specifica: «[l]a proposta vieta altresì l'attribuzione di un punteggio sociale basato sull'IA per finalità generali da parte di autorità pubbliche» (AIA, pag. 14).

[83] G. Resta, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale?*, cit., 340; M. Veale - F. Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, cit.; M. Ebers - V. R. S. Hoch - F. Rosenkranz - H. Ruschemeier - B. Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act*, cit.; EDPB-GEPD, Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale), punto 29.

del 2021), il quale lo legittima quando «necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento»[84].

In ogni caso, anche a voler qualificare come pubblico l'interlocutore in questione o definire l'attività come svolta per conto di un'autorità pubblica, i limiti nel ricondurre la fattispecie nell'alveo dell'art. 5 AIA si palesano, altresì, su un piano oggettivo: in primo luogo, l'attività in questione non include l'assegnazione di un "punteggio sociale"; in secondo luogo, la nozione di "valutazione dell'affidabilità delle persone fisiche", per quanto indeterminata, non sembra ricomprendere le valutazioni che si sostanziano in indagini con finalità meramente statistiche, senza la creazione di profili classificatori; in terzo luogo, dall'utilizzo dei dati compiuto (cioè, per comparare le abitudini di mobilità di soggetti che si servono o meno della *sharing mobility*) non pare potersi derivare né un trattamento pregiudizievole di natura eterogenea rispetto al contesto generante i dati né un trattamento ingiustificato o sproporzionato.

Peraltro, sembra possibile sostenere questo ragionamento solamente in relazione alle attività statistiche che l'iniziativa si propone di realizzare; invece, nel caso in cui il trattamento dovesse essere utilizzato in maniera tale da incidere significativamente su alcuni gruppi della società – ad esempio, soggetti utilizzatori o non utilizzatori di servizi di *sharing mobility*[85] –, allora il tema potrebbe porsi con una diversa intensità.

Tuttavia, non è da escludere che l'inserimento dell'elemento della corresponsione di un premio possa in astratto avvicinare queste pratiche a quelle che, nell'intenzione del legislatore europeo, sono da vietare. Difatti, la logica premiale è ciò che accomuna operazioni di questo tipo al modello del punteggio sociale – e, più in generale, alla *gamification* di cui esso costituisce espressione – e le discosta dallo strumento dell'altruismo propriamente inteso.

Parimenti, la questione potrebbe essere meritevole di maggiore attenzione qualora le valutazioni in merito alla corresponsione del premio fossero collegate all'attribuzione di un punteggio (anche implicito) o alla corresponsione di sanzioni (in particolare se sproporzionate o avulse dal contesto di raccolta dei dati), come ipotizzato in altri pro-

[84] In merito al contenuto della lett. e), è bene ricordare che la disposizione prevede che siano gli Stati membri a fissare le basi giuridiche del trattamento e che, nel farlo, ne determinino le finalità e gli eventuali adeguamenti alle disposizioni del GDPR. Relativamente all'ordinamento italiano, poi, il Codice in materia di protezione dei dati personali è stato interessato da una recente modifica che, sul punto, ha introdotto il comma 1-*bis* all'interno dell'art. 2-*ter*, che delle basi giuridiche si occupa: in esso viene specificato che il trattamento da parte di un'amministrazione pubblica «è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti». In questo panorama normativo si inserisce, inoltre, un recente provvedimento con il quale il Garante ha precisato che «[a]l fine di adempiere […] "obblighi legali" o "compiti di interesse pubblico o connessi all'esercizio di poteri pubblici", i soggetti pubblici non sono tenuti a chiedere alcun consenso (o autorizzazione) ai soggetti interessati per effettuare il trattamento dei relativi dati personali», anche in considerazione del fatto che lo squilibrio tra interessato e titolare che caratterizza i rapporti con le autorità pubbliche inficerebbe la validità del consenso prestato (considerando 43 GDPR). Per una trattazione dettagliata sul punto, si rinvia a D. Poletti, *sub* Art. 6 regolamento (UE) 2016/679 del 27 aprile 2016 (GDPR), in R. D'Orazio - G.D. Finocchiaro - O. Pollicino - G. Resta (a cura di), *Codice della Privacy e Data Protection*, Milano, 2021, 199 ss.

[85] Per il momento, difatti, i risultati dello studio che sono stati pubblicati evidenziano alcune correlazioni nelle abitudini di queste due categorie di soggetti (ad esempio, relative all'utilizzo dell'automobile); essi sono consultabili presso: *osservatoriosharingmobility.it*.

getti interessati dall'azione del Garante.
Per dovere di completezza, infine, può sottolinearsi un ulteriore aspetto: anche qualora si dovesse ritenere che iniziative di questo tipo non siano riconducibili alle attività vietate dall'art. 5 AIA, un'ulteriore indagine si potrebbe imporre in merito al rispetto dei requisiti, relativi ai dati e al loro trattamento, che la proposta di regolamento richiede per i sistemi di intelligenza artificiale ad alto rischio (Titolo III), nel caso in cui i sistemi considerati dovessero ricadere nell'elenco presente nell'allegato III (si possono ricordare, a titolo esemplificativo, i sistemi di "gestione e funzionamento delle infrastrutture critiche" o di "istruzione e formazione professionale"). In questi casi, come momento intermedio e di congiunzione tra la raccolta dei dati e l'attività che su di essi viene effettuata, occorrerebbe soffermarsi sulla base giuridica identificabile per il trattamento. Anche su questo piano, l'apporto della proposta potrebbe essere significativo, se si considera che una parte della dottrina individua nell'esenzione di cui all'art. 10, par. 5, AIA[86], relativa al divieto di trattamento di particolari categorie di dati, una nuova base giuridica per il trattamento di dati particolari *ex* art. 9 GDPR, correlata alle finalità di '*debiasing*' e correzione delle distorsioni, prodotte dall'utilizzo di categorie di dati limitate, perorate nella proposta per evitare trattamenti algoritmici discriminatori[87].

5. Osservazioni conclusive: cittadinanza attiva o "a punti" per la *smart city*

Seguire il flusso di dati dalla fase della raccolta a quella dell'utilizzo – illustrando così una sequenza dati-algoritmi – permette di osservare come esperienze concrete interagiscano con il quadro regolatorio in divenire e consente, altresì, di svolgere alcune considerazioni conclusive in merito al nesso tra pratiche di *data altruism* e *social scoring*.
Pur attenendo tali fenomeni a due piani diversi (fonte dei dati e attività sui dati), la presenza nelle pratiche di condivisione dei dati di alcuni elementi – ad esempio, come visto, la corresponsione di premi – ne potrebbe determinare, in un certo senso, una sovrapposizione.
Per il momento, le iniziative esaminate si agganciano a due attributi che le mantengono distanti da modelli di *social scoring* veri e propri: a) la volontarietà, che si riflette sulla modalità di ottenimento dei dati da parte delle autorità pubbliche e ne limita la portata

[86] Che recita: «Nella misura in cui ciò sia strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono trattare categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, comprese le limitazioni tecniche all'utilizzo e al riutilizzo delle misure più avanzate di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita».

[87] Questa posizione è sostenuta da M. Ebers - V. R. S. Hoch - F. Rosenkranz - H. Ruschemeier - B. Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act*, cit., 600 e da G. Resta, *Cosa c'è di 'europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale?*, cit., 337; *contra*, vd. EDPB-GEPD, Parere congiunto 5/2021, cit., punto 73.

ai soli dati forniti volontariamente; b) la previsione della sola corresponsione di benefici e l'assenza di sanzioni o dell'attribuzione di un punteggio alle persone.
Tuttavia, l'analisi condotta ha permesso di osservare che anche situazioni di questo tipo possono presentare dei profili di criticità. D'altronde, il fondamento dell'altruismo dei dati – e la sua assimilabilità alla logica del dono[88] – risiede nella natura disinteressata del contributo; al contrario, prevedere la corresponsione di qualsiasi tipo di compenso o premio (per quanto incentivante) formalmente incrina questa logica.
Pertanto, nonostante la condivisione dei dati sia subordinata al requisito della volontarietà, la previsione di forme di compensazione altera il modello del *data altruism* e lo può avvicinare ai meccanismi di *nudging* insiti nel punteggio sociale e nella *gamification* (in cui a uno o più determinati comportamenti possono corrispondere premi, sanzioni o modifiche del punteggio, inducendo così il partecipante a tenere una determinata condotta).
In sintesi, potrebbe affermarsi che stimolare forme di partecipazione attiva da parte dei cittadini per mezzo di tecniche solo latamente riconducibili a una logica di *gamification* non si schiera nettamente né dal lato delle iniziative di *social scoring* né dal lato del *data altruism* e dell'aumento di fiducia verso la circolazione dei dati nei consociati (anzi, rischia di produrre risultati talvolta opposti nell'opinione pubblica[89]). Ciò in quanto, per un verso, la fiducia dei cittadini potrebbe essere ricercata altrove[90] e non in meccanismi premiali per i cittadini "virtuosi" e, per altro verso, le caratteristiche 'gamificatorie' dei progetti esaminati non sono così marcate da poterli considerare tecniche di controllo sociale o cittadinanza "a punti".
In altri termini, nonostante il coinvolgimento diretto dei cittadini nelle attività di raccolta dei dati sia volto a garantire loro una maggiore consapevolezza e fiducia, esso, incidendo direttamente sul rapporto tra cittadini e Stato, sollecita alcune riflessioni e richiede una certa cautela nella sua attuazione, affinché condivisibili iniziative di cittadinanza attiva e di condivisione dei dati non ingenerino dubbi circa la deriva verso una cittadinanza "a punti".
Del resto, il tema dell'individuazione del confine tra cittadinanza attiva e "a punti" come nuove declinazioni del concetto di cittadinanza è tanto più degno di attenzione se si considera che esso intercetta quella esigenza di elaborazione di dati provenienti dagli abitanti e dal contesto pubblico che si pone alla base della realizzazione della

88 G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 989.

89 Ne sono testimonianza gli articoli con cui le testate giornalistiche hanno riportato la notizia delle istruttorie del Garante, giustamente mostrando un certo scetticismo verso iniziative che sottenderebbero rischi di controllo sociale, ma spesso cedendo alla solo apparente vicinanza dei progetti occidentali al modello cinese (citato espressamente o richiamato da contributi grafici). A titolo esemplificativo, si richiamano: *Con la patente a punti per i buoni cittadini rischiamo una deriva cinese*, su *editorialedomani.it*, 4 luglio 2022; *I 3 progetti italiani di "credito sociale" che preoccupano il Garante della privacy*, su *wired.it*, 8 giugno 2022. Sull'accostamento al Scs cinese, oltre a rinviare a quanto visto *supra* (par. 3), utile il richiamo a *How the West Got China's Social Credit System Wrong*, su *wired.com*, 29 luglio 2019.

90 Ad esempio, la figura degli intermediari di dati (*data intermediaries*) ha subìto un notevole sviluppo nelle recenti prospettazioni dottrinarie e legislative. Sul punto, M. Hennemann - L. v. Ditfurth, *Datenintermediäre und Data Governance Act*, in *NJW*, 2022, 1905; F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 1, 2021, 199 ss.; World Economic Forum, *Advancing Digital Agency: The Power of Data Intermediaries*, February 2022.

smart city[91].

Nella formazione e nello sviluppo delle "città intelligenti", condivisione e analisi dei dati costituiscono, infatti, elementi imprescindibili: un simile utilizzo dei dati consentirebbe la risoluzione di problemi collettivi e di questioni di interesse pubblico. Nell'alimentare la *smart city*, nei suoi connotati tipici di connettività e integrazione tra strumenti tecnologici, è naturale che la facilitazione della raccolta dei dati passi attraverso il coinvolgimento dei cittadini, nell'ottica di un miglioramento dei servizi pubblici guidato dall'analisi dei dati. Tuttavia, anche in quest'ambito, l'oscillazione nei modelli tra i due estremi della cittadinanza attiva e della cittadinanza "a punti" ripropone quella tensione tra il desiderio di assicurare un impianto tecnologico al servizio degli abitanti e il rischio di assecondare, così facendo, forme di controllo sociale[92].

In quest'ottica, sono da accogliere con favore i più recenti interventi regolatori dell'UE nelle parti in cui sollecitano nuove sinergie tra pubblico e privato nella società digitale[93], essendo i dati (e la loro circolazione tra i due settori) «capac[i] di ridurre lo squilibrio tra organi potestativi e cittadini»[94].

All'estremo opposto, però, si collocano esperienze quali quella cinese, in cui l'immagazzinamento di dati pare rappresentare uno strumento per creare una "cittadinanza modello" e idonea a popolare le nuove *smart city* perché selezionata secondo le dinamiche del punteggio sociale[95].

Ancora una volta, dunque, il tema risulta essere quello dello sviluppo di una valida alternativa 'europea': non cedere, nel complesso bilanciamento tra efficienza delle funzioni pubbliche e tutela dei diritti dei cittadini[96], verso forme di cittadinanza "a punti", ma predisporre strumenti adatti a facilitare modelli di cittadinanza attiva nel governo dei dati. In questa direzione, sono noti i progetti che promuovono logiche di '*empowerment*' dei cittadini con la funzione di riappropriarsi del controllo sui dati che li riguardano ed evitare le disuguaglianze, la frammentazione e la mancanza di fiducia dettate dalla concentrazione dei dati nelle mani delle principali imprese private[97].

---

[91] In generale, sul tema, si rinvia a A. Decker, *Smart Law for Smart Cities*, in *Fordham Urban Law Journal*, 41, 2014, 1491 ss.; R. Kitchin, *The promise and peril of smart cities*, in *Computers and law: the journal of the Society for Computers and Law*, 2, 2015, 1 ss. Su un piano comparatistico, rispetto al modello cinese, si segnala W. He, W. Li, P. Deng, *Legal Governance in the Smart Cities of China: Functions, Problems, and Solutions*, in *Sustainability*, 14, 2022, 18 ss.

[92] S. Pieranni, *La Cina nuova*, Roma-Bari, 2021, 83.

[93] S. Tranquilli, *Il nuovo citoyen européen nell'epoca del Data governance act*, cit., 183.

[94] F. Musella, *Amministrazione 5.0*, cit., 101.

[95] S. Pieranni, *La Cina nuova,* cit., 122: «lo scopo finale è la creazione di una «cittadinanza modello», ideale per abitare le sfavillanti ed efficienti smart city e […] [i]l sistema dei crediti sociale rappresenta l'acme di questo processo».

[96] F. Musella, *Amministrazione 5.0*, cit., 108.

[97] Per un'analisi approfondita E. Morozov - F. Bria, *Rethinking the Smart City. Democratizing Urban Technology*, New York, 2018, 53 («*Cities and governments have yet to fully grasp that data lies at the heart of most power relations today*»), in cui si propone un modello di gestione dei dati nelle città diverso da quello, imperante, del capitalismo digitale. In particolare, per il caso della città di Barcellona, vd. I. Calzada - E. Almirall, *Barcelona's Grassroots-led Urban Experimentation: Deciphering the 'Data Commons' Policy Scheme*, Conference Data for Policy, 2019, 2; F. Monge - S. Barns - R. Kattel - F. Bria, *A new data deal: the case of Barcelona*, UCL Institute for Innovation and Public Purpose, Working Paper Series n. 02/2022, 8. Ancora, su istanze analoghe si incentra la proposta di J. J. Zygmuntowski - L. Zoboli - P. F. Nemitz,

La spinta verso una diffusione di pratiche più contigue a tali modelli si spiega alla luce del tentativo di allontanarsi dalle logiche proprie del capitalismo della sorveglianza e della società reputazionale, ormai diffuse in ambito privato a partire dall'espansione delle *Big Tech*. Al contrario, adottare questi principi anche in ambito pubblicistico rischierebbe di assecondare definitivamente il «principale pericolo del controllo sociale tramite AI: un mondo irreggimentato»[98].

Embedding European values in data governance: a case for public data commons, in *Internet Policy Review*, 3, 2021, 3.

[98] F. Pasquale, *Le nuove leggi della robotica*, cit., 29. Per contrastare questo pericolo, l'Autore sottolinea l'opportunità di «superare i tentativi di riformare i sistemi di punteggio e cercare di limitarne la portata, assumendo il ruolo di giudici dei limiti della AI [perché il suo uso] non è il solo modo per governare una società e giudicare chi merita oneri o benefit» (ivi, 164-165).

Le modifiche e l'aggiornamento del contenuto digitale e dei servizi digitali nella disciplina di attuazione delle direttive (UE) 770 e 771 del 2019*

Giovanna Capilli

Abstract

Questo contributo esamina l'attuazione delle direttive (UE) 2019/770 e 2019/771 nell'ordinamento italiano con particolare riferimento all'obbligo del venditore e del professionista di fornire gli aggiornamenti nei casi di contratti vendita di beni digitali o di contratti di fornitura di contenuta digitali o servizi digitali. Il saggio si sofferma sulla differenza tra aggiornamenti necessari per il mantenimento della conformità e quelli non necessari, sui presupposti in base ai quali sono consentite modifiche ai contenuti digitali o ai servizi digitali nonché sui possibili rimedi a tutela del consumatore in caso di mancata fornitura dell'aggiornamento o sopravvenuta non conformità dovuta ad un aggiornamento difettoso.

This paper examines the implementation of the directives (EU) 2019/770 and 2019/771 in the Italian consumer code with particular reference to the obligation to supply updates in sale of digital goods or contracts for the supply of digital content or digital services. The essay focuses: on the difference between updates necessary to maintain the conformity and those that are not necessary, on the modifications of the digital content or digital service, and on the consumer's remedies in case of lack of conformity due to defective or incomplete update.

Sommario

1. Introduzione – 2. L'obbligo di fornire gli aggiornamenti – 2.1 Aggiornamenti necessari e aggiornamenti non necessari – 2.2. Differenza tra aggiornamento e modifica– 3. Presupposti per modificare il contenuto digitale e il servizio digitale – 3.1. Il recesso del

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

consumatore – 4. La durata dell'obbligo di fornire gli aggiornamenti – 5. Mancata fornitura dell'aggiornamento e rimedi a tutela del consumatore – 6. Conclusioni

Keywords
tutela dei consumatori – contenuti digitali – servizi digitali – aggiornamenti – upgrade

1. Introduzione

L'Unione europea, per migliorare il funzionamento del mercato interno e per rimanere competitiva sui mercati mondiali, ha cercato di rispondere alle molteplici sfide determinate oggi da un'economia caratterizzata sempre di più dalle tecnologie, attraverso un pacchetto di norme, confluite nelle direttive c.d. "gemelle" del 2019 n. 770 e 771 ed attuate nell'ordinamento italiano alla fine del 2021 con i decreti legislativi nn. 173 e 170[1].

La trasposizione della normativa comunitaria ha comportato una nuova modifica del codice del consumo, in particolare del titolo III unitamente al capo I sulla vendita di beni, nonché l'introduzione del capo I bis sui contratti di fornitura di contenuto digitale e di servizi digitali[2].

L'esame della direttiva (UE) 771/2019 (abbreviata "Direttiva SGD") e del novellato art. 128 del codice del consumo, consente di distinguere tre categorie di beni che rientrano nel suo campo di applicazione (quali oggetti dei contratti disciplinati): a) beni senza elementi digitali, per i quali non vi sono sostanziali novità rispetto agli obblighi del venditore già esistenti ed introdotti con la direttiva 99/44/CE, b) beni con elementi digitali, per i quali il venditore è tenuto a fornire gli aggiornamenti anche dopo la consegna e per il periodo stabilito dalla normativa; c) beni con elementi digitali, per i quali il contratto prevede la fornitura continuativa di contenuti digitali o servizi digitali e il venditore è tenuto a fornire l'aggiornamento del contenuto o del servizio digitale nella misura in cui è necessario per mantenere la funzionalità del bene[3].

[1] Si tratta dei decreti legislativi del 4 novembre 2021 n. 170 e n. 173.

[2] Per alcuni primi commenti alla normativa si rinvia a G. Capilli- R.Torino, *Codice del consumo: le novità per i contratti di vendita e fornitura di beni digitali*, Milano, 2022; A. Luminoso, *La nuova disciplina delle garanzie nella vendita al consumatore (una prima lettura del d. lgs. n. 170/2021),* in *Eur. Dir. Priv.,* 3, 2022, 483; A. Maniaci, *I rapporto tra autonomia privata e disciplina italiana della vendita di beni di consumo dopo il recepimento della direttiva n. 2019/771*, in *Eur. Dir. Priv*., 2, 2022, 237; F. Trubiani, *I contratti di cloud computing: natura, contenuti e qualificazione giuridica*, in *Diritto dell'Informazione e dell'Informatica*, 2, 2022, 395; G. Perfetti, *Beni con elementi digitali e aggiornamenti nella novellata disciplina dei contratti di vendita B2C*, in *juscivile*, 2022, 1, 177 ss.

[3] Per approfondimenti su tale classificazione, si rinvia a H. Schulte-Nolke, *Digital obligations of sellers of smart devices under the Sale of Goods Directive 771/2019*, in S. Lohsse - R. Schulze - D. Staudenmayer (a cura di), *Smart Products*, Münster, 2022, 52, il quale fornisce il seguente esempio: «*a smart lock installed at your front door that can be opened and locked through an app on your mobile phone. This smart lock is certainly a good with digital elements in the sense of article 7 (3) SGD. Whether it is also a good with digital elements where the sales contact provides for a continuous supply of digital content or a digital service over a period of time in the senso of article 10 (2) SGD, depends on the technicalities of the smart lock. The more elaborate smart locks that are actually available on the market are usually connected to a service platform, which is also connected through an app on the user's mobile phone. In such a setting, the operation of the service platform Is crucial for the function of the smart lock. Such a case*

I contratti che prevedono, invece, la fornitura di contenuti digitali o di servizi digitali, che però non sono incorporati o interconnessi con i beni, rientrano nella disciplina di cui alla direttiva (UE) 770/2019 (abbreviata "Direttiva DCSD").

Nelle ipotesi in cui sia incerta la normativa applicare, la linea di demarcazione delle due discipline sopra richiamate è definita dall'art. 3 della direttiva sulla vendita (art. 128, c. 3, cod. cons,.) e dall'art. 3 della direttiva sulla fornitura di contenuti e servizi digitali (art. 135 *novies*, c. 1, cod. cons.) in cui espressamente si stabilisce che dovrà applicarsi la direttiva sulla vendita anche ai contenuti digitali o ai servizi digitali incorporati o interconnessi con i beni e che sono forniti con il bene ai sensi del contratto di vendita. Ciò indipendentemente dal fatto che questi contenuti siano forniti dal venditore o da terzi. Laddove, poi, sia in dubbio la possibilità che la fornitura di un contenuto digitale incorporato o interconnesso o che un servizio digitale incorporato o interconnesso possa fare parte del contratto di vendita o meno, il legislatore ha stabilito una presunzione in base alla quale il contenuto digitale e il servizio digitale vengono fatti rientrare nel contratto di vendita[4].

Circoscrivendo l'analisi al tema degli aggiornamenti e delle modifiche dei contenuti digitali e dei servizi digitali, si cercherà di trattare insieme quanto previsto dalla normativa sulla vendita e sui contratti di fornitura, effettuando ove necessario le opportune differenziazioni.

Secondo il disposto del nuovo art. 129 cod. cons. il venditore deve fornire al consumatore beni che soddisfano i requisiti di cui ai c. 2 e 3, cioè possedere i requisiti di conformità oggettivi e soggettivi[5], nonché rispondere alle previsioni degli artt. 130 e

would fall under article 10 (2) SGD. In connection with article 7 (3) and 10 (1) SGD, the seller of such a smart lock has a full set of digital obligations. Firstly, the seller I also obliged to uphold the functioning of the service platform and the app installed on the user's mobile phone and article 10 (2) SGD. This obligation, of course, also includes providing the necessary updates to the software of the service platform and the app».

[4] Cfr. art. 128, c. 3, e art. 135 *novies* cod. cons.

[5] Per comodità di lettura è opportuno riportare il disposto dell'art. 129 cod. cons.: «2. Per essere conforme al contratto di vendita, il bene deve possedere i seguenti requisiti soggettivi, ove pertinenti:
a) corrispondere alla descrizione, al tipo, alla quantità e alla qualità contrattuali e possedere la funzionalità, la compatibilità, l'interoperabilità e le altre caratteristiche come previste dal contratto di vendita;
b) essere idoneo ad ogni utilizzo particolare voluto dal consumatore, che sia stato da questi portato a conoscenza del venditore al più tardi al momento della conclusione del contratto di vendita e che il venditore abbia accettato;
c) essere fornito assieme a tutti gli accessori, alle istruzioni, anche inerenti all'installazione, previsti dal contratto di vendita; e
d) essere fornito con gli aggiornamenti come previsto dal contratto di vendita.
3. Oltre a rispettare i requisiti soggettivi di conformità, per essere conforme al contratto di vendita il bene deve possedere i seguenti requisiti oggettivi, ove pertinenti:
a) essere idoneo agli scopi per i quali si impiegano di norma beni dello stesso tipo, tenendo eventualmente conto di altre disposizioni dell'ordinamento nazionale e del diritto dell'Unione, delle norme tecniche o, in mancanza di tali norme tecniche, dei codici di condotta dell'industria applicabili allo specifico settore;
b) ove pertinente, possedere la qualità e corrispondere alla descrizione di un campione o modello che il venditore ha messo a disposizione del consumatore prima della conclusione del contratto;
c) ove pertinente essere consegnato assieme agli accessori, compresi imballaggio, istruzioni per l'installazione o altre istruzioni, che il consumatore può ragionevolmente aspettarsi di ricevere; e,
d) essere della quantità e possedere le qualità e altre caratteristiche, anche in termini di durabilità, funzionalità, compatibilità e sicurezza, ordinariamente presenti in un bene del medesimo tipo e che il consumatore può ragionevolmente aspettarsi, tenuto conto della natura del bene e delle dichiarazioni pubbliche fatte dal o per conto del venditore, o da altre persone nell'ambito dei precedenti passaggi

131 in quanto compatibili.

Del pari, in base all'art. 135 *decies* cod. cons., il professionista deve fornire al consumatore il contenuto digitale o il servizio digitale ed entrambi devono rispettare i requisiti soggettivi e oggettivi di conformità.

A questo punto è necessario evidenziare uno degli aspetti innovativi e centrali della novella che ha, indubbiamente, elevato la tutela per il consumatore rispetto alla disciplina previgente: si tratta dell'aggiornamento dei beni con elementi digitali, nonché dell'aggiornamento, e della modifica dei contenuti digitali e dei servizi digitali nei contratti di fornitura.

La finalità delle norme dettate in tema di aggiornamenti, come si preciserà nel prosieguo, è quella di preservare, mantenendola, la conformità di quanto venduto, ossia garantire la funzionalità e la sicurezza IT dei dispositivi elettronici anche dopo la consegna del prodotto e per tutto il tempo che l'acquirente possa aspettarsi, ma non solo[6].

Diventa imprescindibile, quindi, muovere dalle definizioni per esaminare nel dettaglio le implicazioni che tale "ulteriore" obbligo comporta in capo al venditore e al professionista, i quali saranno tenuti non solo informare il consumatore sugli aggiornamenti, ma anche fornirglieli.

Un bene con elementi digitali (*smart product*) viene definito, infatti, come «qualsiasi bene mobile materiale che incorpora o è interconnesso con un contenuto digitale o un servizio digitale in modo tale che la mancanza di detto contenuto digitale o servizio digitale impedirebbe lo svolgimento delle funzioni proprie del bene» (v. art. 128, c. 2, lett. e), n. 2, cod. cons.; art. 135 *octies*, c. 2, lett. c))[7], il «contenuto digitale» consiste nei «dati prodotti o forniti in formato digitale» (v. art. 128 lett. f; art 135 *octies*, c. 2, lett. a)), e il «servizio digitale» è «un servizio che consente al consumatore di creare, trasformare, memorizzare i dati o di accedervi in formato digitale», nonché «un servizio che consente la condivisione di dati in formato digitale caricati o creati dal consumatore o da altri utenti di tale servizio o qualsiasi altra interazione con tali dati» (art. 128, c. 2, lett. g) n. 1 e 2; art. 135 *octies*, c. 2, lett. b, n. 1 e 2).

Necessarie, allora, talune considerazioni preliminari per chiarire meglio le suddette definizioni, muovendo dal considerando 14 della direttiva (UE) 771/2019 in cui si legge che:

---

della catena di transazioni commerciali, compreso il produttore, in particolare nella pubblicità o nell'etichetta».

[6] C. Wenderhorst, *The update obligation*, in S. Lohsse - R. Schulze - D. Staudenmayer (a cura di), *Smart products,* cit., 64, la quale sottolinea come la Direttiva SGD ha introdotto due tipologie di scenari: «*In the first scenario, the trader needs to provide updates in order to maintain the conformity of the digital content or services or of the goods with digital elements with the contract…The second scenario concerns updates and other modifications that are not required to maintain the conformity of the digital content or services with the contact, but which amount to a unilateral change of the performance owed under a long-term contractual relationship and may even be to the detriment of the consumer*».

[7] S. Lohsse - R. Schulze - D. Staudenmayer, *Smart products – A Focal Point for Legal Developments in the Digital Economy,* in S. Lohsse - R. Schulze - D. Staudenmayer (a cura di), *Smart products,* cit., secondo cui: «*the important of smart products is firstly linked to the rise of the Internet of Things (IoT)*», ed evidenziano altresì che l'elevato sviluppo delle IoT correlato al numero delle *smart homes* avrà un forte impatto sulla sempre maggiore diffusione degli *smart products.*

> «Per contenuto digitale incorporato o interconnesso con un bene si può intendere qualsiasi dato prodotto e fornito in forma digitale, come i sistemi operativi, le applicazioni e qualsiasi altro software», ed ancora che «il contenuto digitale può essere preinstallato al momento della conclusione del contratto di vendita o installato successivamente qualora tale contratto lo preveda. Tra i servizi digitali interconnessi con un bene possono figurare servizi che consentono la creazione, la trasformazione o la memorizzazione di dati in formato digitale, nonché l'accesso a tali dati, quali i software come servizio offerti nell'ambiente di *cloud computing*[8], la fornitura continua di dati relativi al traffico in un sistema di navigazione oppure la fornitura continua di programmi di allenamento personalizzati nel caso di uno *smartwatch*».

Deve, altresì, essere apprezzato il considerando 15 in cui si precisa ulteriormente che:

> «Se, ad esempio, nella pubblicità di una smart TV si è fatto riferimento alla presenza di una particolare applicazione video, tale applicazione video dovrebbe essere considerata quale facente parte del contratto di vendita. Ciò si dovrebbe applicare indipendentemente dal fatto che il contenuto digitale o il servizio digitale sia preinstallato nel bene stesso o debba essere successivamente scaricato su un altro dispositivo che sia soltanto interconnesso con il bene in questione. Ad esempio, uno *smartphone* potrebbe essere dotato di applicazioni standard preinstallate fornite secondo il contratto di vendita, quali l'applicazione della sveglia o della fotocamera. Un altro possibile, esempio, è dato dallo *smartwatch*. In tal caso, l'orologio stesso sarebbe considerato il bene con elementi digitali in grado di svolgere le rispettive funzioni solo in combinazione con un'applicazione prevista dal contratto di vendita ma che deve essere scaricata dal consumatore su uno *smartphone*; l'elemento digitale interconnesso sarebbe l'applicazione. Ciò dovrebbe applicarsi anche se il contenuto digitale o un servizio digitale incorporato interconnesso non è fornito direttamente dal venditore ma, conformemente al contratto di vendita e fornito da un terzo».

Da quanto sopra, si può senz'altro trarre che si tratta di "beni" in cui, come possiamo verificare nella quotidianità, gli aggiornamenti hanno un'importanza determinante per il loro funzionamento come anche per i contenuti e servizi digitali[9] giacché senza aggiornamenti, diventerebbero certamente obsoleti[10] e non più utilizzabili efficacemente.

---

[8] F. Trubiani, *I contratti di cloud computing,* cit., 395, il quale con riferimento ai contratti di cloud afferma che: «Proprio nel caso dei contratti di cloud computing, i quali sembrano rientrare a tutti gli effetti nell'ambito della categoria dei contratti di durata, l'obbligo di assicurare la conformità del contenuto o il servizio digitale si estende all'intera durata del contratto: nello specifico il cloud service provider deve fornire la versione più aggiornata del contenuto digitale esistente al momento di conclusione del contratto».

[9] A. Janssen, *The Update Obligation for Smart Products,* in S. Lohsse - R. Schulze - D. Staudenmayer, cit., 93, il quale evidenzia che «*without updates, smart products very quickly become "dumb products" over time, become outdated, lose functionality or develop security gaps. Consumers therefore expect smart products to receive updates at regular intervals, especially if security of smart product is at stake*».

[10] Per un'analisi del sistema di consumo e della obsolescenza dei prodotti dovuta a diverse cause, si

2. L'obbligo di fornire gli aggiornamenti

I beni con elementi digitali, nonché gli stessi contenuti digitali o servizi digitali, sono beni complessi rispetto ai quali l'obbligazione in capo al venditore, così come disciplinata dalla precedente direttiva 99/44/CE, non è più sufficiente, ma si arricchisce ulteriormente rispetto al passato, in quanto il venditore che, prima, era tenuto a consegnare un bene "conforme al contratto", in base alle nuove disposizioni dovrà fornire il bene con gli aggiornamenti del contenuto e del servizio digitale integrato[11] come previsto nel contratto di vendita (v. art. 129, c. 2, lett.d), nonché tenere informato il consumatore sugli aggiornamenti disponibili, anche di sicurezza, necessari al fine di mantenere la conformità dei beni.

Si tratta di un evidente passo avanti rispetto alle regole generali anche di derivazione romanistica che vedevano il venditore obbligato a consegnare il bene trasferendone la proprietà; ma anche rispetto alla direttiva 99/44/CE in virtù della quale il venditore era obbligato non solo a consegnare un bene, ma anche a garantire la conformità di questo al contratto, dovendosi ritenere inadempiente in caso di consegna di bene non conforme.

Con le nuove direttive 771/2019 e 770/2019, i prodotti digitali o le forniture di contenuti e servizi digitali implicano nuovi obblighi che non si esauriscono in un solo momento coincidente con quello della consegna del bene, ma si tratta di obblighi suscettibili di essere continuativi[12] e prolungati nel tempo, e oltre tutto, proprio per la natura del bene, possono riguardare anche soggetti ulteriori rispetto al venditore e al professionista, ma che rimangono estranei al consumatore.

Il venditore/professionista, infatti, sarà l'unico soggetto responsabile ai fini della novella, e ciò anche nell'ipotesi in cui l'obbligo di aggiornamento dipenda da un terzo; e se ciò può essere stato voluto al fine di agevolare il consumatore nell'individuazione del soggetto eventualmente responsabile della mancata conformità, al contempo, come vedremo in seguito, lo limita nell'esperimento dei rimedi nei confronti degli effettivi responsabili della mancanza di conformità.

Diventa centrale, quindi, nella valutazione della conformità del bene e del possibile inadempimento del venditore e del professionista, il rispetto dell'obbligo sia di informare[13] sia quello di fornire gli aggiornamenti, anche di sicurezza[14]. Obbligo che da un

rinvia a S. Latouche, *Usa e getta. Le follie dell'obsolescenza programmata,* Torino, 2012.

[11] Sul tema anche G. Perfetti, *Beni con elementi digitali e aggiornamenti nella novellata disciplina dei contratti di vendita B2C*, cit., 180.

[12] Segue questa impostazione, H. Schulte-Nolke, *Digital obligations of sellers of smart devices under the Sale of Goods Directive 771/2019*, cit., il quale evidenzia che «*The SGD changed this basic principle for smart devices, i.e. goods that contain a digital element or where the sales contract provides for a continuous supply of digital content or a digital service over a period of time*». *Tuttavia, l'Autore evidenzia che «in the case of goods with digital elements, not only the seller but also other persons involved in the digital elements should be liable to the consumer*».

[13] A. Janssen, *The Update Obligation for Smart Products,* cit., 96, il quale sottolinea come: «*the information obligation of the seller about the update is only describe in a rather cryptic way…..In practice, the information about the update will regularly coincide with the supply of the update itself*».

[14] Vale la pena ricordare il nuovo standard di sicurezza minima EN 303 645, che serve come raccomandazione per lo sviluppo sicuro (Security by Design) di dispositivi IoT, accessibile su *etsi.org*. Si legge per esempio in tema di mantenimento aggiornato del software che: «lo sviluppo e la distribuzione

lato è necessario per mantenere la conformità, e dall'altro è esso stesso elemento caratterizzante la conformità stessa del bene posto che è inserito tra i requisiti soggettivi in base al disposto dell'art. 129, c. 2, lett. d) [15].

Questi obblighi, inoltre, devono essere adempiuti nel periodo di tempo durante il quale il contenuto digitale o il servizio digitale deve essere fornito a norma del contratto, se questo prevede una fornitura continua per un determinato periodo di tempo, oppure che il consumatore può ragionevolmente aspettarsi, date la tipologia e la finalità del contenuto digitale o del servizio digitale e tenendo conto delle circostanze della natura del contratto, se questo prevede un unico atto di fornitura o una serie di singoli atti di fornitura (art. 130, c. 2; e art. 135 *undecies* cod. cons.)[16].

Specificatamente, anche con riferimento ai contratti di fornitura di contenuti digitali e servizi digitali, tra i requisiti soggettivi di conformità, in base al disposto dell'art. 135 *decies*, c. 4, lett.d), si prevede che il contenuto digitale o il servizio digitale debba essere "aggiornato come previsto dal contratto"[17].

In entrambi i casi (di vendita di beni con elementi digitali, o di fornitura di contenuti o servizi digitali) il contratto di vendita rappresenta il punto di riferimento per verificare la tipologia degli aggiornamenti che devono essere forniti al consumatore.

Per quanto argomentato fino ad ora, quindi, si può ritenere che un bene con elementi digitali o un contenuto digitale o un servizio digitale per la loro intrinseca natura neces-

---

tempestiva degli aggiornamenti di sicurezza costituisce una delle azioni più importanti che un produttore può intraprendere per proteggere i propri clienti e il più ampio ecosistema tecnico. È buona norma che tutto il software sia mantenuto aggiornato e ben mantenuto; i meccanismi di aggiornamento possono variare dal dispositivo che scarica l'aggiornamento direttamente da un server remoto, trasmesso da un'applicazione mobile o trasferito tramite USB o altra interfaccia fisica; il grado di semplicità dipende dal design e dall'uso previsto del dispositivo. Un aggiornamento semplice da applicare verrà applicato automaticamente, avviato utilizzando un servizio associato (come un'applicazione mobile) o tramite un'interfaccia web sul dispositivo. Se un aggiornamento è difficile da applicare, aumenta la possibilità che un utente rinvii ripetutamente l'aggiornamento del dispositivo, lasciandolo in uno stato vulnerabile; gli aggiornamenti di sicurezza possono essere forniti per i dispositivi in modo preventivo, come parte di aggiornamenti automatici, che possono rimuovere le vulnerabilità di sicurezza prima che vengano sfruttate. La gestione di questo può essere complessa, specialmente se ci sono aggiornamenti del servizio associati paralleli, aggiornamenti del dispositivo e altri aggiornamenti del servizio da gestire. Pertanto, un chiaro piano di gestione e implementazione è vantaggioso per il produttore, così come la trasparenza per i consumatori sullo stato attuale del supporto degli aggiornamenti».

[15] La norma stabilisce che il bene «deve essere fornito con gli aggiornamenti come previsto dal contratto di vendita».

[16] Sul punto con riferimento ai contratti di *cloud computing*: F. Trubiani, *I contratti di cloud computing*, cit., 395 ss., il quale evidenzia che «L'art. 135 undecies cod. cons. disciplina gli obblighi del professionista, con particolare riferimento agli obblighi di informazione che egli ha nei confronti del consumatore in merito agli aggiornamenti (in particolar modo quelli legati agli standard di sicurezza) disponibili per i contenuti o servizi digitali forniti. Proprio nel caso dei contratti di cloud computing, i quali sembrano rientrare a tutti gli effetti nell'ambito della categoria dei contratti di durata, l'obbligo di assicurare la conformità del contenuto o il servizio digitale si estende all'intera durata del contratto: nello specifico il cloud service provider deve fornire la versione più aggiornata del contenuto digitale esistente al momento di conclusione del contratto. Qui il riferimento va di tutta evidenza al tema della c.d. obsolescenza programmata dei beni e/o dei servizi tecnologici».

[17] A tal proposito C. Wendrehorst, *The update obligation*, cit., 66, evidenzia che: «*The update obligation needs to be analysed in relation to four different contractual constellations: (i) single act of supply (or series of individual acts of supply) of digital content or service, (ii) continuous supply of digital content or service over a period of time, (iii) delivery of goods with single act of supply of a digital element (e.g. embedded software), and (iv) delivery of goods with continuous supply of a digital element over a period of time (e.g. user account for the producer's cloud)* ».

sitano di aggiornamenti; questi molto spesso possono essere convenuti nel contratto di vendita con la finalità di migliorare e potenziare l'elemento di contenuto digitale o servizio digitale, ampliarne le funzionalità, adattarlo agli sviluppi tecnici e proteggerlo da eventuali nuove minacce alla sicurezza o servire ad altri scopi[18]. In ogni caso, però, qualora gli aggiornamenti non siano convenuti nel contratto, proprio per la tipologia dei beni, devono essere forniti necessariamente per il mantenimento della conformità.

2.1. Aggiornamenti necessari e aggiornamenti non necessari

Sebbene le direttive non contengano una definizione espressa di "aggiornamento", questa può trarsi dalle stesse disposizioni in esse contenute, ma, soprattutto, verificando quale sia lo scopo degli stessi al fine di differenziarli dalla "modifica" del contenuto digitale o del servizio digitale[19].

Come anticipato, la normativa prevede che nel caso di beni con elementi digitali il venditore debba garantire anche che il consumatore sia informato in relazione agli aggiornamenti e che questi, compresi gli aggiornamenti di sicurezza, gli siano forniti, per il mantenimento della conformità del bene.

Cosicchè, un dato certo è che il venditore debba fornire gli aggiornamenti convenuti contrattualmente (che quindi possono avere finalità ulteriori rispetto al semplice mantenimento della conformità[20]) nonché quelli necessari a garantire che i beni con elementi digitali restino conformi.

Ciò, detto in altre parole, significa che, salva diversa disposizione contrattuale, il venditore ha un obbligo limitato agli aggiornamenti necessari a mantenere la conformità dei beni con i requisiti di conformità oggettivi e soggettivi, ma non ha l'obbligo di fornire versioni aggiornate dei contenuti o dei servizi digitali dei beni, nè tantomeno l'obbligo di migliorare o ampliare le funzionalità dei beni oltre ai requisiti di conformità[21].

---

[18] Vedi considerando 28 della direttiva (UE) 771/2019 che specifica: «La conformità dei beni con contenuti o servizi digitali incorporati o interconnessi con essi dovrebbe pertanto essere valutata altresì in relazione all'eventualità che l'elemento di contenuto digitale o servizio digitale di tali beni sia aggiornato nel modo stabilito nel contratto di vendita».

[19] G. Perfetti, *Beni con elementi digitali e aggiornamenti nella novellata disciplina dei contratti di vendita B2C*, cit., 185 ha richiamato questa definizione di aggiornamento: «messa a disposizione del consumatore utente di un insieme di dati teleologicamente orientati alla rappresentazione di un contenuto digitale o alla fornitura di un servizio digitale da intendersi nell'ambiente digitale del bene compra venduto».

[20] G. Perfetti, *ibid.*, il quale con riferimento agli aggiornamenti contrattualmente convenuti tra le parti, evidenzia che si tratta di aggiornamenti le cui finalità non sono state tipizzate nella direttiva essendo rimesse all'autonomia delle parti.
Si tratta in sostanza degli aggiornamenti di cui parla il considerando 28 della Direttiva SGD in cui si legge: «Gli aggiornamenti convenuti nel contratto di vendita possono migliorare e potenziare l'elemento di contenuto digitale o servizio digitale dei beni, ampliarne le funzionalità, adattarli gli sviluppi tecnici, proteggerli da nuove minacce alla sicurezza o servire ad altri scopi».

[21] È lo stesso considerando 30 a specificare che: «l'obbligo del venditore dovrebbe essere limitato agli aggiornamenti necessari a mantenere la conformità dei beni con i requisiti di conformità oggettivi e soggettivi definiti nella presente direttiva. Salvo diversa disposizione contrattuale, il venditore non dovrebbe avere l'obbligo di fornire versioni aggiornate dei contenuti o servizi digitali dei beni, né di migliorare o ampliare le funzionalità dei beni andando oltre i requisiti di conformità»

Ecco perché è utile distinguere tra aggiornamenti necessari e aggiornamenti non necessari.

I primi, definiti anche "correttivi", in quanto si tratta di aggiornamenti anche di sicurezza che devono evidentemente essere attuati dal professionista per tutta la vita del contratto di fornitura o per tutta la vita del bene con contenuti digitali per mantenere la conformità.

I secondi, definiti anche "evolutivi", perché per loro natura dovrebbero essere reversibili e non dovrebbero ridurre le prestazioni o la capacità di risposta del bene in cui sono incorporati.

È chiaro che la sicurezza informatica[22] assume un ruolo centrale nell'ambito dei requisiti fondamentali che devono essere posseduti dai prodotti o dai servizi digitali[23] e ciò è dovuto al fatto che i rischi che possono scaturire dalla mancanza di sicurezza informatica appropriata del prodotto sono molteplici e possono costituire una minaccia per sé e per gli altri andando ben oltre i profili di responsabilità contrattuale[24].

Occorre, a questo punto, fare alcune ulteriori considerazioni per quanto riguarda gli aggiornamenti non previsti nel contratto.

Potrebbe trattarsi, infatti, di aggiornamenti che il venditore non è obbligato a fornire, ma dei quali deve comunque informare il consumatore e ciò anche nel caso in cui gli aggiornamenti siano forniti da terzi (ipotesi certamente molto frequente nella pratica)[25].

D'altra parte, occorre evidenziare che le direttive e le disposizioni di attuazione indicano nel venditore/professionista l'unico soggetto tenuto a fornire gli aggiornamenti al consumatore, ma è evidente che in considerazione delle tipologie contrattuali che possono caratterizzare i beni digitali o i contratti di fornitura di contenuti digitali o servizi digitali, in cui possono assumere ruoli determinanti, per esempio, le stesse piattaforme, il consumatore potrebbe vedere le sue aspettative di tutela frustrate a causa dell'impossibilità, da un lato, di poter esercitare i rimedi direttamente nei confronti del soggetto che può fornire effettivamente l'aggiornamento e, dall'altro, per l'impossibi-

[22] La definizione di "sicurezza informatica" possiamo riprenderla dal c.d. Cybersecurity Act in cui la "cibersicurezza" viene definita come «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche».

[23] Nel considerando 30 della direttiva (UE) 771/2019 si legge che «oltre agli aggiornamenti convenuti contrattualmente, il venditore dovrebbe altresì fornire aggiornamenti, compresi aggiornamenti di sicurezza, per garantire che beni con elementi digitali restino conformi».
N.E. Vellinga, *Connected and vulnerable: cybersecurity in vehicles,* in *International Review of Law, Computers & Technology*, 36, 2022, 161 ss.; l'A. nell'articolo si occupa della violazione da parte di due hacker dei sistemi wireless dei comandi di un veicolo attraverso il sistema di intrattenimento del veicolo stesso, in tal modo gli hacker hanno determinato un rallentamento del veicolo in autostrada.

[24] In tema di responsabilità per danno da prodotto difettoso si rinvia alla proposta di direttiva COM (2022) 495 final del 28.9. 2022, in cui nella nozione di prodotto difettoso viene indicato anche il prodotto che non offre la sicurezza che il grande pubblico può legittimamente attendersi tenuto conto di tutte le circostanze tra cui (lett. f) «i requisiti di sicurezza del prodotto, compresi i requisiti di cibersicurezza rilevanti per la sicurezza».

[25] Vale la pena osservare che nella ETSI EN 303 645 V2.1.1 (2020-06) viene riportato che in molti casi, la pubblicazione di aggiornamenti software implica molteplici dipendenze da altre organizzazioni come i produttori che producono sottocomponenti; tuttavia, questo non è un motivo per sospendere gli aggiornamenti e può essere utile per il produttore considerare l'intera catena di fornitura del software nello sviluppo e nella distribuzione degli aggiornamenti di sicurezza.

lità per lo stesso venditore di poter "costringere" il terzo a fornirlo.
In tali situazioni al consumatore non resterà altro se non avvalersi del rimedio risolutorio o quello della riduzione del prezzo.
D'altra parte, se è innegabile che la più rilevante novità è rappresentata dalla previsione dell'obbligo di aggiornamento in quanto questo deve essere adempiuto continuamente, anche nel corso degli anni, in ragione del fatto che i beni intelligenti necessitano di aggiornamenti costanti, dall'altra parte il diritto di regresso attribuito al venditore/professionista nei confronti dei precedenti passaggi della catena di transazioni commerciali, qualora la sua responsabilità dovesse scaturire dall'omissione da parte di questi terzi, sarà tuttavia molto difficile da attuare per l'evidente difficoltà per il venditore/professionista di riuscire a provare effettivamente quale soggetto della catena avrebbe dovuto provvedere ad effettuare l'aggiornamento, potendo questo dipendere da diversi fattori, tra cui, per esempio, il fatto che gli aggiornamenti dipendano dal produttore di un sottocomponente del bene medesimo.

2.2. Differenza tra aggiornamento e modifica del contenuto digitale o del servizio digitale

Nel paragrafo che precede si è chiarito che il venditore non è tenuto a fornire al consumatore aggiornamenti che migliorano il bene con elementi digitali o che non siano necessari per mantenere la conformità del bene, ma piuttosto è tenuto a fornire gli aggiornamenti (o upgrade) solo se le parti lo abbiano contemplato nel contratto. In base alla normativa comunitaria il venditore deve assicurare che i beni continuino a funzionare secondo il contratto anche se l'ambiente digitale che li circonda cambia, ma non è tenuto a migliorare il bene digitale[26].
Ecco perché potrebbe diventare rilevante valutare l'entità delle modifiche che vengono apportate alla parte digitale dei beni, in quanto laddove fossero fondamentali non potrebbero essere considerati semplici "upgrade", ma piuttosto si tratterebbe di "update" (come nel caso in cui l'aggiornamento sia volto ad introdurre una nuova funzionalità prima inesistente).
Per comprendere, allora, se si tratti di un "update" o "upgrade" è corretto accertare cosa implichi l'esecuzione dell'aggiornamento, vale a dire se questo determini un ampliamento delle funzionalità dell'elemento digitale o meno[27]. Non sarebbe, infatti,

[26] Si veda anche quanto previsto dal considerando 30 della direttiva (UE) 771/2019: «Salvo diversa disposizione contrattuale, il venditore non dovrebbe avere l'obbligo di fornire versioni aggiornate dei contenuti o servizi digitali dei beni, né di migliorare o ampliare le funzionalità dei beni andando oltre requisiti di conformità».
P. Kalamees, *Goods with Digital Elements and the Seller's Updating Obligation*, in *JIPITEC*, 12, 2021, 131 para 1, il quale riporta il seguente esempio: «*The seller of a fitness tracker is obliged to inform and supply the consumer with updates that keep the application functioning according to the contract and the objective requirements of the SGD for conformity. The seller does not have the obligation to improve the digital elements tied to the goods in any way, e.g. adding functionalities to the application*».

[27] P. Kalamees, ivi, 135, richiamando il caso di un *fitness tracker* evidenzia che: «*To determine whether there is an update or an upgrade, the contents of the update have to be evaluated. If the update is necessary for keeping the goods functioning according to the contract, it is an update. This is the case for example where an update to a fitness tracker is*

sufficiente per integrare "upgrade", il semplice miglioramento della funzionalità già assicurata dal bene, mentre lo sarebbe qualora il consumatore si trovi di fronte ad una nuova versione del bene venduto [28].

L'esatto inquadramento delle fattispecie diventa necessario, quindi, per valutare l'inadempimento del venditore/professionista e garantire, per quanto possibile, l'attuazione del sistema rimediale per il consumatore[29].

Il venditore non sarà tenuto a fornire i cosiddetti upgrade che comportano tendenzialmente rilascio di nuove versioni della componente digitale e implicano non solo rilevanti miglioramenti del software medesimo, si tratta in questo caso di aggiornamenti cosiddetti evolutivi per i quali comunque il consumatore mantiene il suo diritto di rifiuto.

Diversamente il venditore per salvaguardare la conformità del bene con elementi digitali al contratto è tenuto a fornire quelli che abbiamo indicato sopra come "update".

In linea generale, infatti, il consumatore deve accettare l'installazione degli aggiornamenti e comunque decidere se e quando installarli.

Si pone, pertanto, la questione dell'ammissibilità degli aggiornamenti forzati, cioè se sia possibile per i professionisti prevedere che gli aggiornamenti siano installati automaticamente[30].

3. Presupposti per modificare il contenuto digitale e il servizio digitale

In base all'art. 135 *undecies* cod. cons., il professionista è obbligato a tenere informato

provided in order to eliminate some security threats».

[28] C. Camardi, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione dei dati personali*, in *Giust. Civ.*, 3, 2019, 499 ss., la quale evidenzia, con riferimento alla prestazione del venditore e alla sua durata che essi vanno «ragionevolmente dimensionati per rapporto alla versione del bene oggetto dello scambio. Detto altrimenti, fino a quando gli aggiornamenti sono compatibili con la versione del bene oggetto del contratto, essi sono dovuti. Nel momento in cui fosse prodotta una nuova versione del bene, con elementi nuovi di funzionalità, tali da configurare un "altro" bene rispetto a quello venduto, il consumatore non ha titolo a pretendere aggiornamenti che allarghino le funzionalità del bene»; P. Kalamees, *Goods with Digital Elements and the Seller's Updating Obligation*, cit., 135: «*If there is an update that adds some sleep analysis methodology to the fitness tracker's app this should be considered an upgrade if such functionality was not agreed upon in the sales contract*».
I. Barkāne - A. Buka - Z. Dāvida - J. Kārkliņš - S. Kārklis - V. Mantrovs - K. Silionovs, *Digitalais pirkuma objekts*, Latvijas Universitāte, 2022 gli Autori forniscono il seguente esempio: se viene pubblicizzato che un videogioco sarà aggiornato con un nuovo livello una volta all'anno per cinque anni, l'adempimento tempestivo di tale obbligo è generalmente considerato come aggiornamento del contenuto digitale.

[29] Secondo G. Perfetti, *Beni con elementi digitali e aggiornamenti nella novellata disciplina dei contratti di vendita B2C*, cit., 189, «mentre sotto l'impero della dir. 1999/44/CE il venditore si situava in una posizione meramente passiva, in attesa dell'eventuale manifestazione del difetto di conformità, oggi al venditore di un bene con elementi digitali è imposto l'obbligo non solo di eliminare, ma anche di prevenire del difetto, mediante la predisposizione, la notifica e la fornitura al consumatore degli aggiornamenti conformativi».

[30] C. Wenderhorst, *The update obligation*, cit., 72, la quale evidenzia le implicazioni anche sotto il profilo del GDPR dell'eventuale installazione automatica di update in particolare di cybersecurity; M. García Goldar, *The inadequate approach of Directive (EU) 2019/771 towards the circular economy,* in *Maastricht Journal of European and Comparative Law*, 29(1), 2022, 9 ss.

il consumatore sugli aggiornamenti disponibili anche di sicurezza necessari al fine di mantenere la conformità del contenuto digitale e del servizio digitale. Viene ripreso, sostanzialmente, quanto disposto a carico del venditore nelle disposizioni sulla vendita di beni, ma in considerazione del fatto che i contenuti digitali e i servizi digitali sono in costante evoluzione, l'art. 135 *viciessemel* cod. cons. prevede anche la possibilità di modificare il contenuto digitale o il servizio digitale, qualora il contratto disponga che il contenuto digitale o il servizio digitale sia fornito o reso accessibile al consumatore per un certo periodo di tempo oltre a quanto è necessario per mantenere la conformità del contenuto o del servizio digitale.

Quindi, nello specifico caso di contratti di durata aventi ad oggetto la fornitura di contenuti digitali o servizi digitali, le parti contrattuali possono prevedere di effettuare modifiche al contenuto digitale o al servizio digitale.

La modifica implica che viene cambiato o alterato "qualcosa", per cui si potrebbe trattare di una qualsiasi alterazione apportata al codice sorgente, oppure una modifica al software che esegue il servizio; ed ancora la modifica può essere effettuata solo nel *database* del fornitore di servizi, nel sito web dell'host o nel luogo in cui la modifica influisce sul software che viene scaricato e installato nell'apparecchiatura del consumatore. Una modifica potrebbe poi comprendere anche i casi in cui il contenuto digitale, la sua accessibilità, la qualità, la funzionalità, l'interoperabilità con altri servizi, sono influenzate, non solo attraverso modifiche generali al servizio/piattaforma che sono ugualmente applicabili a tutti i consumatori di quel servizio, ma anche modifiche specifiche, che possono riguardare unicamente l'account personale di un determinato consumatore[31].

A differenza poi degli aggiornamenti che il consumatore è libero di installare o meno (fermo restando le conseguenze in ordine alla responsabilità del professionista), salvo abbia autorizzato in sede contrattuale gli aggiornamenti automatici contemplati nelle condizioni generali di contratto[32], le modifiche non necessitano di essere installate dal

[31] Cfr. M. Farinha, *Modifications on the digital content or digital service by the trader in the Directive (EU) 2019/770. Alterações aos conteúdos ou serviços digitais fornecidos pelo profissional na Diretiva (UE) 2019/770,* in *Revista Electrónica De Direito,* 2(25), 2021.

[32] Un esempio può essere utile. Si riporta il messaggio con cui Dropbox comunica l'effettuazione di "aggiornamenti" anche se in realtà come si è spiegato nel testo trattasi di vere e proprie "modifiche":
«Ciao Utente,
Siamo sempre alla ricerca di modi per migliorare l'esperienza di Dropbox e ampliare la nostra offerta di funzionalità. Negli ultimi anni abbiamo accolto HelloSign (ora Dropbox Sign) e DocSend nella famiglia Dropbox, e ora offriremo questi servizi come parte integrante di Dropbox. Se non hai mai utilizzato questi servizi, ora potrai accedervi dal tuo account Dropbox. Stiamo apportando alcuni aggiornamenti ai nostri Termini di servizio e alle nostre Norme sulla privacy in modo che riflettano questi e altri cambiamenti:
Termini di servizio
•Abbiamo aggiunto una lingua per descrivere l'uso dei servizi Dropbox Sign e DocSend.
•Abbiamo aggiunto un linguaggio che chiarisce le tue responsabilità nel caso in cui tu decida di attivare integrazioni di terze parti con Dropbox.
•Ora ci riferiamo ai team Dropbox Business come Team Dropbox e abbiamo aggiornato i Termini di servizio di conseguenza.
Norme sulla privacy
•Abbiamo aggiunto informazioni per spiegare come funziona la raccolta dei dati quando utilizzi DocSend, le informazioni sui contenuti visualizzati in Dropbox o i nostri servizi di firma elettronica.
•Abbiamo aggiunto informazioni per chiarire come utilizziamo i dati quando interagisci con i

consumatore e possono essere effettuate direttamente dal professionista.
Dalla lettura dei considerando 74 e 75 della direttiva (UE) 770/2019 si trae che sebbene alcune modifiche siano spesso suscettibili di avvantaggiare il consumatore in quanto generalmente comportano un miglioramento del contenuto digitale o del servizio digitale, il vantaggio per il consumatore non costituisce un prerequisito necessario per eseguirle, ragione per la quale sono possibili anche modifiche idonee a produrre un impatto negativo per il consumatore se l'operatore economico ha un valido motivo per effettuarle; in queste ipotesi rientrano i casi in cui la modifica è necessaria per adattare il contenuto digitale o il servizio digitale ad un nuovo ambiente tecnico ovvero un numero maggiore di utenti, o per altre ragioni operative rilevanti.
Ricapitolando, quindi, il professionista deve effettuare la modifica per mantenere la conformità, purchè ciò sia consentito dal contratto, tale modifica sia motivata e non siano previsti costi aggiuntivi per il consumatore; quest'ultimo deve, inoltre, essere informato in modo chiaro e comprensibile della modifica e con anticipo ragionevole, su supporto durevole, anche in relazione alla possibilità di recedere dal contratto ovvero alla possibilità di mantenere il contenuto digitale o il servizio digitale senza la modifica.
L'obiettivo del legislatore è evidentemente quello di prescrivere l'obbligo di modifica del servizio digitale o del contenuto in modo da farlo rimanere conforme al contratto imponendo altresì l'ulteriore obbligo di comunicare al consumatore detta modifica; per altre modifiche effettuate dal professionista, che non sono richieste per mantenere la conformità, il contratto deve espressamente consentirle fornendo validi motivi, il consumatore deve essere informato in modo chiaro sulle modalità e sul momento in cui viene effettuata la modifica nonché del suo diritto di recedere dal contratto o di mantenere il contenuto digitale o il servizio digitale senza la modifica.
La *ratio* comune di queste disposizioni sulle modifiche è in realtà di agevole comprensione: informare adeguatamente il consumatore sulla possibilità che possono essere effettuate e costringere il professionista ad adempiere a quanto previsto nel contratto e, quindi, a non discostarsi dai requisiti di conformità, senza poter modificare liberamente il servizio o il contenuto a scapito e all'insaputa del consumatore[33].
L'incidenza negativa, sia degli aggiornamenti che delle modifiche, deve essere accertata obiettivamente tenendo in considerazione la natura, le finalità del contenuto digitale o del servizio digitale, la qualità, la funzionalità, la compatibilità, e altre principali caratteristiche che sono normali per i contenuti digitali o servizi digitali dello stesso tipo. Alcuni esempi possono essere ulteriormente chiarificatori per distinguere corretta-

rappresentanti di Dropbox in determinati contesti di marketing.
•Ora ci riferiamo ai team Dropbox Business come Team Dropbox e abbiamo aggiornato le Norme sulla privacy di conseguenza.
Dai un'occhiata ai Termini di servizio e alle Norme sulla privacy completi, che entreranno in vigore il 3 aprile 2023. Continuando a utilizzare Dropbox dopo questa data, accetti i nuovi termini. Qui puoi trovare anche la versione precedente dei Termini. Per ulteriori informazioni, consulta il Centro assistenza».

[33] I. Barkāne - A. Buka - Z. Dāvida - J. Kārkliņš - S. Kārklis - V. Mantrovs - K. Silionovs, *Digitālais pirkuma objekts*, cit., 98, in cui viene evidenziato che una eventuale riserva nel contratto secondo cui l'operatore può apportare modifiche al contenuto digitale o al servizio digitale, se necessario per il funzionamento del contenuto digitale o del servizio digitale, non sarebbe di per sé sufficiente, in quanto i motivi della modifica devono essere chiari e comprensibili.

mente tra aggiornamento e modifica.

Rientrano nel concetto di modifica le seguenti ipotesi: il cambiamento dell'interfaccia utente per tutti gli utenti del servizio; la modifica dell'algoritmo che regola il modo in cui le pubblicazioni degli utenti vengono visualizzate sul feed dei loro follower (da un ordine cronologico a un ordine percepito di pertinenza calcolato utilizzando l'apprendimento automatico)[34]; il cambiamento della qualità della trasmissione agli utenti premium rispetto agli utenti della versione gratuita; la rimozione di un elemento dall'account di un determinato utente (es. in un videogioco online)[35]. [36]

Se una piattaforma di streaming video stabilisse nelle condizioni generali di contratto di integrare una volta al mese i film disponibili sulla piattaforma con nuovi film, si potrebbe in tal caso parlare di aggiornamenti poiché il professionista adempie all'obbligazione contrattuale; se, invece, la piattaforma offre agli utenti un aggiornamento che prevede cambiamenti del design della piattaforma stessa, allora in questo caso si tratterà di modifica poiché non finalizzata a mantenere il servizio digitale conforme e ciò indipendentemente dal "nomen" che viene fornito nelle condizioni generali di contratto.

Se un sistema operativo per computer fornisce aggiornamenti di sicurezza per gli utenti, le modifiche rientreranno nel concetto di aggiornamento nel momento in cui garantiscono la conformità del sistema operativo[37].

Nel caso in cui una piattaforma di streaming video cambiasse i programmi TV che ha a disposizione per lo streaming ai suoi consumatori, a causa all'acquisizione delle licenze per la distribuzione di detti programmi TV e alla perdita dei diritti per lo streaming di altri Programmi TV, saremmo di fronte ad una modifica che influisce sulla conformità del servizio, causata da terze parti.

Con riferimento a questa ipotesi, il considerando 53 e 54 della direttiva (UE) 770/2019 evidenzia che le restrizioni all'uso del contenuto digitale o del servizio digitale da parte del consumatore, derivanti da limitazioni imposte dal titolare di diritti di proprietà intellettuale in conformità del diritto in materia di proprietà intellettuale, potrebbero

---

[34] Si tratta di una modifica che influisce sul modo in cui il contenuto viene condiviso sulla piattaforma, quindi, si tratta di una modifica, ed è una modifica che riguarda tutti gli utenti.

[35] Si tratta di una modifica del servizio digitale che riguarda un solo utente.

[36] Alcuni di questi esempi sono contenuti nel saggio di M. Farinha, *Modifications on the digital content or digital service,* cit., 93.

[37] È frequente che vengano trovate vulnerabilità di sicurezza dei dispositivi e sia necessario effettuare l'aggiornamento. Si veda per esempio da ultimo l'articolo di P. Tarsitano, *Aggiornamenti Android gennaio 2023, corrette 61 vulnerabilità: mettiamo in sicurezza i device,* in *cybersecurity360.it,* 4 gennaio 2023, in cui si legge: «Tutti gli aggiornamenti dovrebbero essere installati il prima possibile: alcuni o tutti, a seconda del dispositivo, possono essere applicati automaticamente tramite i servizi Google Play; altri, invece, potrebbero essere inviati all'utente sotto forma di un aggiornamento da parte dell'operatore o del produttore del dispositivo, e alcuni potrebbero non essere necessari. I dispositivi Android più economici e meno aggiornati potrebbero non vedere mai gli aggiornamenti»; ed ancora: «Le politiche di aggiornamento di Google prevedono che i dispositivi ricevano aggiornamenti per la versione di Android installata per almeno tre anni dalla data di introduzione sul Google Store, mentre gli aggiornamenti di sicurezza saranno garantiti per tre anni dalla data di introduzione nella versione statunitense del Google Store. Per quanto riguarda, invece, la velocità di rilascio, se i dispositivi sono stati acquistati direttamente sul Google Store allora gli aggiornamenti arriveranno entro un paio di settimane, mentre per i modelli acquistati da rivenditori di terze parti potrebbe volerci più tempo».

violare i requisiti oggettivi di conformità stabiliti dalla direttiva se riguardano caratteristiche che sono abituali di contenuti digitali o servizi digitali dello stesso tipo e che il consumatore può ragionevolmente attendersi. Nel considerando si specifica, altresì, che in queste circostanze il consumatore dovrebbe potersi avvalere dei rimedi previsti per il difetto di conformità e del pari l'operatore economico potrebbe evitare una sua responsabilità soltanto qualora dimostri di avere informato il consumatore, prima della conclusione del contratto, del fatto che una caratteristica particolare del contenuto digitale o del servizio digitale si discosta dai requisiti oggettivi di conformità e il consumatore ha espressamente separatamente accettato tale scostamento.

3.1. Il recesso del consumatore

Si è detto che il professionista ha, per un verso, l'obbligo di aggiornare i contenuti o i servizi digitali per mantenerne la conformità, soprattutto qualora siano forniti o resi accessibili per un certo periodo di tempo e, per altro verso, anche il diritto di apportare modifiche ai contenuti o ai servizi digitali, ma ciò purché ciò sia previsto nel contratto, ne fornisca valida motivazione[38], non vi siano costi aggiuntivi per il consumatore (divieto di nuovi pagamenti per l'accesso al contenuto digitale o al servizio digitale)[39], e

[38] M. Farinha, *Modifications on the digital content or digital service,* cit., 99, riporta alcune "valide ragioni" per apportare modifiche:
«*a) Compliance with legal requirements (from requiring more identification and certification procedures, to comply with data protection law, stop and denounce criminal activity and remove criminal content such as child pornography, among others);*
b) Updating the trademarks of the trader, and changing other aesthetic aspects of digital service and content;
c) Adding features, functionalities and adapt the service or content for a higher degree of interoperability with other services and digital environments;
d) Improving already present features and functionalities;
e) Change algorithms to increase user's engagement with content;
f) Removing content uploaded by the consumers which is protected by intellectual property rights;
g) Removing interoperability with third-party software which is used for malignant reasons – from spyware, malware, to combat the use of bots;
h) Apply sanctions, flag or delete user content which infringes stablished rules on civility and combat misconduct;
i) Patch exploits and bugs that don't cause a lack of conformity;
j) Create, change or diminish space for advertisement;
k) Limiting the platforms and trader's potential liability to third parties».

[39] Ancora sul punto M. Farinha, *Modifications on the digital content or digital service,* cit., 100, evidenzia che, per esempio, se vecchie funzionalità o parti del contenuto stesso che erano precedentemente accessibili al consumatore vengono poste dietro un nuovo *paywall* con l'implementazione di tale modifica, tale modifica viola il disposto concernente la gratuità. Ciò vale sia per i servizi a pagamento (con la creazione di livelli aggiuntivi di consumatori paganti o per nascondere parti di ciò che era disponibile in un "patto di espansione") sia per i contratti "gratuiti" (togliendo contenuti o funzionalità dalla versione gratuita a quella "premium"). L'A., inoltre, evidenzia che oltre al pagamento in denaro, ci potrebbero essere altri costi nascosti per i consumatori e che potrebbero rientrare in questa disposizione: si pensi ad esempio alla necessità di incrementare i requisiti hardware per supportare ed eseguire il servizio digitale. L'implementazione/modifica apportata dal professionista potrebbe impedire a un consumatore di utilizzare il servizio con le sue apparecchiature elettroniche (computer, smartphone...), e ciò contrasterebbe con la disposizione. Questi quindi non solo violerebbero tale condizione ma potrebbero anche costituire un difetto di conformità, qualora i nuovi requisiti minimi hardware fossero superiori a quelli specificati nelle informazioni precontrattuali. Se il consumatore è costretto ad aggiornare la propria attrezzatura, questo tipo di modifica potrebbe bloccare il consumatore dall'accedere al servizio

quest'ultimo sia informato della natura della modifica e dei suoi diritti.
L'obbligo di informazione a carico del professionista in relazione alla modifica da apportare è funzionale al fatto che il consumatore deve comprendere esattamente gli effetti che dalla stessa derivano.
Ecco perché è fondamentale rendersi conto se la modifica sia stata eseguita per mantenere o ripristinare la conformità oppure se sia una modifica discrezionale non idonea a pregiudicare la conformità[40].
Se, infatti, la modifica ha un impatto negativo sull'utilizzo del contenuto digitale o del servizio digitale o sull'accesso allo stesso da parte del consumatore, il consumatore ha diritto di recedere dal contratto entro 30 giorni dal ricevimento delle informazioni fornite o della modifica, se successiva, e se il consumatore sceglie di recedere, il professionista è tenuto a rimborsare al consumatore tutti i pagamenti effettuati per il periodo successivo alla data di risoluzione.
Il diritto di recesso non è contemplato qualora le conseguenze negative della modifica effettuata siano "trascurabili".
Valutazione questa che, nella dinamica contrattuale, è certamente lasciata al consumatore e dipenderà dalla tipologia di modifica o aggiornamento adottato.
Si deve segnalare, in ogni caso, come la problematica sia particolarmente avvertita dai fornitori di contenuti digitali e servizi digitali che sembra stiano procedendo all'adeguamento delle condizioni contrattuali attraverso l'inserimento di clausole volte a prevedere la definizione delle controversie insorte mediante conciliazioni e mediazioni.
Occorre evidenziare che il consumatore non potrà recedere dal contratto anche qualora il professionista gli abbia dato la possibilità di mantenere il contenuto digitale o il servizio nella sua forma esistente, e cioè senza modificarlo e senza alcun costo.
Non si può non segnalare, altresì, che, in questa specifica ipotesi, la maggior parte dei consumatori non sarà in grado di comprendere e valutare in anticipo se la modifica possa determinare problemi e presumibilmente il termine di 30 giorni per esercitare il recesso potrà non essere sufficiente per consentirgli di assumere una decisione consapevole. Qualora, infatti, si acconsenta ad apportare la modifica e poi, questa, dovesse rivelarsi insoddisfacente, oltre il termine indicato il consumatore non avrà altri rimedi se non quelli di diritto comune per potersi svincolare dal contratto. Il consumatore, inoltre, una volta acconsentito alla modifica non avrà il diritto di tornare alla versione originale del contenuto digitale o del servizio.
È possibile che il professionista accompagni le modifiche con un aggiornamento necessario per mantenere conforme il contenuto digitale. In tale circostanza ci si deve interrogare se ciò, senza consentire al consumatore di scegliere separatamente se accettare o meno la ulteriore modifica "non necessaria", possa costituire una pratica commerciale sleale.

e al contenuto digitale, imponendogli costi aggiuntivi vietati dalla norma.

[40] In relazione all'obbligo di aggiornamento e alla sua regolamentazione nei contratti con i consumatori si deve evidenziare che ancora oggi i contratti risultano deficitari.

4. La durata dell'obbligo di fornire gli aggiornamenti

Altra e diversa questione è quella della considerazione del tempo entro il quale il venditore è obbligato a fornire gli aggiornamenti, perché se da una parte la normativa europea limita la responsabilità del venditore alla conformità al contratto del contenuto digitale o del suo servizio digitale integrato per il periodo del biennio, in realtà tale periodo viene superato nel caso in cui sia pattuita una fornitura continuata dell'elemento digitale integrato.

Con riferimento ai beni usati, come nella previgente disciplina, il c. 4 dell'art. 133 cod. cons. consente alle parti di limitare il termine di garanzia ad un periodo comunque non inferiore ad un anno. La novità rispetto al passato è rappresentata dal fatto che tale limitazione può essere prevista anche per il termine di prescrizione dell'azione.

Sotto la vigenza della precedente direttiva 99/44/CE della distinzione tra i termini di garanzia e i termini di prescrizione dell'azione si era occupata la Corte di giustizia nel caso *Ferenschild* del 13 luglio 2017, C-133/16 e proprio con riferimento ai beni usati[41] affermando che il termine biennale con riferimento alla prescrizione dell'azione di garanzia era stato considerato dal legislatore comunitario sufficiente per garantire ai consumatori un livello minimo di tutela e, quindi, da interpretare restrittivamente la disposizione della direttiva ora abrogata che consentiva la pattuizione per i beni usati un termine di garanzia inferiore. In pratica, gli Stati avrebbero potuto prevedere la limitazione della durata del periodo di responsabilità del venditore a un anno dalla consegna del bene nel caso dei beni usati, ma non consentire la possibilità di limitare la durata del termine di prescrizione non ritendo possibile impedire al consumatore di esercitare i rimedi, in caso di difetto di conformità del bene in rapporto al contratto, prima della scadenza del termine di due anni dalla consegna costituendo questo un elemento del modello minimo di tutela dei consumatori garantita dal diritto dell'Unione, anche per quanto riguarda i beni usati.

Con la nuova disposizione contenuta nel c. 4 dell'art. 133 cod. cons. si potrà limitare il termine di garanzia e di prescrizione per i beni usati per un periodo non inferiore ad un anno, e ciò perché è stato ritenuto giustificabile un trattamento differente dei beni di seconda mano; viene incentivata la libertà contrattuale e al contempo assicurato al consumatore di essere informato sia della natura del bene in quanto di seconda mano sia del periodo di responsabilità o del termine di prescrizione abbreviato (cfr. considerando 43).

Le medesime regole contenute nell'art. 133 cod. cons. sono riprese per i contratti di fornitura di contenuti digitali o servizi digitali dal nuovo art. 135 *quaterdecies* cod. cons. ad eccezione, comprensibilmente, della disposizione relativa ai beni usati.

Il momento rilevante per valutare l'eventuale mancata fornitura è quello dell'immediatezza successiva alla conclusione del contratto.

La disposizione trova applicazione sia in caso di fornitura singola, ad esempio nel caso in cui il consumatore scarica un libro elettronico e lo archivia sul proprio dispositivo

[41] Per un approfondimento G. Capilli, *Termini di garanzia e termini di prescrizione nella vendita di beni (anche usati) ai consumatori*, in M. Astone (a cura di), *Il diritto dei consumatori nella giurisprudenza della Corte di Giustizia Europea*, Pisa, 2020, 61.

personale (cfr. considerando 56) oppure di una serie di forniture singole, come nel caso in cui il consumatore riceva un *link* per scaricare un nuovo libro elettronico ogni settimana; sia in modo continuativo per un determinato periodo di tempo, rientrando in questi casi per esempio «la trasmissione in streaming di un videoclip per un determinato periodo di tempo a prescindere dall'effettiva durata del file audiovisivo» oppure «i casi in cui elementi specifici del contenuto digitale o del servizio digitale sono messi a disposizione periodicamente, o in diverse occasioni per la durata determinata del contratto, o per il periodo di validità del contatto a tempo indeterminato» come ad esempio «quando il contratto prevede che una copia del software antivirus possa essere utilizzato per un anno e sia automaticamente aggiornato il primo giorno del mese durante tale periodo, o che l'operatore economico rilasci aggiornamenti ogniqualvolta diventino disponibili nuove caratteristiche di un gioco digitale» (cfr. considerando 57). Anche in questa ipotesi il termine di garanzia è biennale e la prescrizione dell'azione volta a fare valere i difetti emersi nel corso della fornitura e non dolosamente occultati dal professionista è fissata in ventisei mesi dall'ultimo atto di fornitura e ciò vale anche per i contratti di durata.

Un cenno è opportuno farlo ai c.d. beni "ricondizionati" o "rigenerati", termine utilizzato per riferirsi ai prodotti hi-tech, tra cui smartphone, tablet, computer ed elettrodomestici, che vengono riparati ed imballati per essere rimessi in vendita perfettamente funzionanti ad un prezzo decisamente più vantaggioso rispetto ad un prodotto nuovo. Anche per i beni ricondizionati o rigenerati, vale la regola prevista per i beni usati e cioè che la garanzia è quella biennale, salvo che le parti, al momento dell'acquisto, l'abbiano limitata ad un anno.

Il che significa che valgono anche le considerazioni effettuate nel paragrafo precedente in ordine agli aggiornamenti e alle modifiche, e per quanto riguarda i rimedi, si devono considerare i principi statuiti per i beni usati.

Esaminando la questione della durata dell'obbligo del venditore/professionista di fornire gli aggiornamenti, si deve osservare che ovviamente la durata di questo impegno è differente in base al tipo di fornitura del contenuto digitale o del servizio digitale, sia questa singola oppure continuata.

Il nuovo art. 133 cod. cons. con riferimento ai beni con elementi digitali specifica che se il contratto di vendita prevede la fornitura continuativa del contenuto digitale o del servizio digitale per un periodo di tempo, il venditore è responsabile anche per qualsiasi difetto di conformità del contenuto digitale o del servizio digitale che si verifica o si manifesta entro due anni dal momento della consegna dei beni con elementi digitali, e se il contratto prevede una fornitura continuativa per più di due anni il venditore risponde di qualsiasi difetto di conformità del contenuto digitale o del servizio digitale che si verifica o si manifesta nel periodo di tempo durante il quale il contenuto digitale o il servizio digitale deve essere fornito a norma del contratto di vendita; a sua volta l'art. 135 *undecies* cod. cons. specifica che il professionista è obbligato a fornire al consumatore gli aggiornamenti nel periodo di tempo: a) durante il quale il contenuto digitale o il servizio digitale deve essere fornito a norma del contratto, se questo prevede una fornitura continua per un determinato periodo di tempo, oppure, b) che il consumatore può ragionevolmente aspettarsi, data la tipologia e la finalità del con-

tenuto digitale o del servizio digitale e tenendo conto delle circostanze della natura del contratto, se questo prevede un unico atto di fornitura o una serie di singoli atti di fornitura.

Come il legislatore europeo mostra abitualmente, anche nel caso di specie non viene indicato specificatamente un termine preciso che individui il momento in cui il professionista non sia più obbligato a fornire l'aggiornamento, ma piuttosto si fa riferimento al criterio della ragionevolezza da intendersi in senso oggettivo, tant'è vero che si chiarisce che un consumatore dovrebbe normalmente aspettarsi di ricevere gli aggiornamenti per un periodo almeno pari a quello di responsabilità per il difetto di conformità del venditore, mentre in taluni casi la ragionevole aspettativa del consumatore potrebbe estendersi oltre detto periodo, come accade per gli aggiornamenti di sicurezza.

Diversamente, qualora si tratti di beni con elementi digitali le cui finalità sono limitate nel tempo, il venditore sarebbe obbligato solo per quel determinato periodo temporale[42].

È evidente, quindi, che l'obbligo di aggiornamento, può variare considerevolmente nel tempo a seconda del tipo di prodotto, e richiede necessariamente una valutazione che tenga in considerazione la natura del bene e la tipologia del contratto, cosicché si potrebbe verificare il caso per cui tale obbligo si estenda anche oltre il termine di due anni (e quindi oltre il termine di responsabilità)[43].

---

[42] Il considerando 31 della direttiva (UE) 771/2019 precisa che il periodo di tempo durante il quale il consumatore può ragionevolmente aspettarsi di ricevere gli aggiornamenti dovrebbe essere valutato sulla base della tipologia delle finalità dei beni e degli elementi digitali tenendo conto anche delle circostanze e della natura del contratto di vendita, cosicchè un consumatore dovrebbe normalmente aspettarsi di ricevere gli aggiornamenti per un periodo almeno pari a quello della responsabilità per il difetto di conformità del venditore, mentre in altri casi la ragionevole aspettativa del consumatore si potrebbe estendere oltre questo periodo, per esempio nel caso di aggiornamenti di sicurezza; in altre situazioni, ad esempio per i beni con elementi digitali la cui finalità è limitata nel tempo, l'obbligo che incombe al venditore di fornire gli aggiornamenti potrebbe essere limitato a tale periodo.

[43] J. M. Carvalho, *Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771*, in *ssrn.com*, il quale riporta i seguenti esempi: «*Contract concluded between a consumer and Netflix, by which the consumer can access the content made available by that company (continuous supply over a period of time). Article 11(3) of Directive 2019/770 applies, and the digital service (allowing access to the page) must be provided in conformity with the contract as long as the contract remains in force. The nature of this contract points to the possibility for the consumer to access the webpage or application (and the agreed content) for a certain period of time (regardless of whether or not its duration has been previously fixed), and conformity is not relevant at a later date, when the consumer can no longer access the webpage or application; – Sales contract of a car including a GPS application already installed in the car and updates of the application in the first three years. The second part of Article 10(2) of Directive 2019/771 applies, the professional being liable for any lack of conformity that occurs or manifests itself during the three-year period established in the contract. It should be noted that for the car itself the period of two years applies. The consumer will therefore have different deadlines for the lack of conformity to be apparent depending on whether the lack of conformity concerns the car (two years) or the GPS application (three years). If, in the previous example, the parties had agreed on updates within a period of one year, the period of two years would still apply. Although software updates have been agreed on only for a period of one year, the consumer is protected from any lack of conformity in the GPS application that becomes apparent within two years If the consumer has purchased the latest version of the GPS application, without agreeing to updates, the application may be used, in principle, forever, and the trader will be liable for any lack of conformity that becomes apparent within two years. This conclusion is also applicable in the given examples of iTunes and Financial Times – each song and each newspaper file may be used forever, and the trader will be liable for any lack of conformity that becomes apparent within two years*».

A. Janssen, *The Update Obligation for Smart Products*, cit., 102, riporta che il legislatore tedesco in attuazione della direttiva ha previsto nella sezione 475e(2) del German Civil Code che il periodo di responsabilità

A tal proposito, il considerando 64 della direttiva (UE) 770/2019 evidenzia le motivazioni per cui il legislatore ha ritenuto non dover fissare un termine preciso; infatti, data la diversità dei contenuti digitali e dei servizi digitali, non sarebbe stato opportuno indicare termini fissi per l'esercizio dei diritti o il rispetto degli obblighi relativi al contenuto digitale o ai servizi digitali perché tali termini non avrebbero tenuto in considerazione tale diversità e avrebbero potuto, a seconda dei casi, dimostrarsi troppo brevi o troppo lunghi.
Gli elementi che potrebbero essere utili per individuare quali siano le legittime aspettative sulla durata dell'obbligo di aggiornamento sono: dichiarazioni pubblicitarie, trasformazione del prodotto, prezzo, ciclo di vita e se il prodotto continua ad essere venduto sul mercato[44].

5. Mancata fornitura dell'aggiornamento e rimedi a tutela del consumatore

In base al disposto degli artt. 135 *decies* e 135 *viciessemel* cod. cons. il professionista deve ritenersi responsabile nei confronti del consumatore per la mancanza di conformità dovuta alla mancata fornitura dell'aggiornamento. L'attribuzione dell'esclusiva responsabilità al venditore per la fornitura degli aggiornamenti diventa problematica sia per quest'ultimo sia per il consumatore.
Per il venditore, dal momento che generalmente quest'ultimo non ha alcun controllo sugli aggiornamenti e forse neppure informazioni sugli aggiornamenti imminenti. Nonostante ciò, la normativa europea lo individua come unico soggetto responsabile (salvo il diritto di regresso) in caso di aggiornamenti omessi o difettosi[45].
Per il consumatore, in quanto l'avere focalizzato la responsabilità unicamente sul venditore o sul professionista, fa sì che questi possa incontrare difficoltà nell'esperimento dei rimedi volti ad ottenere in maniera coattiva l'aggiornamento, cui sarebbe tenuta una terza parte nei cui confronti il consumatore non ha alcuna azione diretta.
Altra questione riguarda la responsabilità del venditore qualora il bene digitale sia conforme al momento della vendita, ma la mancanza di conformità scaturisca proprio in conseguenza della fornitura di un aggiornamento difettoso o incompleto.
Il considerando 28 della direttiva (UE) 770/2019 su questo aspetto precisa che «la mancata fornitura degli aggiornamenti convenuti nel contratto di vendita dovrebbe essere considerata un difetto di conformità dei beni. Inoltre, gli aggiornamenti difet-

termina decorsi dodici mesi dalla fine dell'obbligo di aggiornamento.
P. Kalamees, *Goods with Digital Elements and the Seller's Updating Obligation*, cit., 137, rileva che, sebbene la mancanza di un termine specifico possa creare delle criticità, la soluzione offerta dalla direttiva debba essere considerata la migliore possibile in quanto, pur lasciando qualche incertezza, allo stesso tempo si presenta flessibile per adattarsi ad un'ampia varietà di beni intelligenti venduti sul mercato.

[44] Hogan Lovells, *The sales law update at the beginning of the year - The update obligations according to §§ 475 b, c German Civil Code ("BGB")*, in *jdsupra.com,* 24 gennaio 2022.

[45] A. Janssen, *The Update Obligation for Smart Products*, cit., 97, il quale prospetta un aumento dei prezzi per i consumatori correlato all'aumento degli obblighi in capo ai venditori e ritiene che l'unica opzione per il venditore potrebbe essere quella di garantire contrattualmente che il produttore del prodotto intelligente o un'altra terza parte informi i consumatori e fornisca gli aggiornamenti.

tosi o incompleti dovrebbero altresì essere considerati come un difetto di conformità dei beni, in quanto ciò significherebbe che tali aggiornamenti non sono eseguiti conformemente alle modalità stabilite nel contratto».
Il considerando 30 aggiunge che «se un aggiornamento fornito dal venditore o da una terza parte che fornisce il contenuto o il servizio digitale in base al contratto di vendita causa un difetto di conformità del bene con elementi digitali, il venditore dovrebbe essere tenuto a rendere nuovamente conforme il bene» e ciò fermo restando che il consumatore deve mantenere la facoltà di scegliere se installare gli aggiornamenti forniti, e qualora decida di non installarli, dovrà essere consapevole che i beni potranno non mantenere la conformità iniziale.
Un'ulteriore chiarificazione si rinviene nel considerando 37 che individua nella consegna il momento rilevante per la valutazione della conformità e ciò anche per i beni che incorporano o sono interconnessi con un contenuto digitale o un servizio digitale fornito tramite una singola fornitura, mentre nel caso in cui il contenuto digitale o il servizio digitale incorporato e interconnesso con i beni debba essere fornito in modo continuativo per un certo periodo di tempo il momento rilevante ai fini della determinazione della conformità coinciderebbe con il periodo di tempo decorrente dal momento della consegna e per motivi di certezza giuridica in generale dovrebbe corrispondere con il periodo durante il quale il venditore è responsabile di un difetto di conformità.
Ciò significa che se il venditore, per esempio, ha accettato di fornire interrottamente un contenuto digitale o un servizio digitale per un periodo superiore al biennio, sarà tenuto anche a fornire gli aggiornamenti e il consumatore avrà diritto ad esperire i rimedi previsti per i difetti di conformità anche oltre il biennio.

6. Conclusioni

L'attuazione delle direttive del 2019 sulla vendita di beni e sui contratti di fornitura di contenuti digitali e servizi digitali ha introdotto il diritto del consumatore di ricevere gli aggiornamenti per gli elementi digitali integrati e per i contenuti e servizi digitali necessari per il funzionamento dei beni acquistati e per la corretta esecuzione dei contratti di fornitura.
In base alla nuova normativa l'unico obbligato nei confronti del consumatore è il venditore o il professionista sebbene in molte situazioni questi non sarà in grado di fornire gli aggiornamenti facenti capo a terze parti, cosicché i diritti dei consumatori potranno risultare frustrati dall'impossibilità di poter esperire un'azione diretta nei confronti di coloro che effettivamente sono in grado di aggiornare i contenuti digitali e i servizi digitali.
Ma un dato è certo. È proprio la tipologia dei beni digitali e dei contratti di fornitura di contenuti e servizi digitali che necessita di più soggetti che interagiscono tra loro ognuno con un compito ben preciso, ma nel sistema concepito dal legislatore comunitario, in molti casi, i consumatori saranno costretti a risolvere il contratto e ottenere la

restituzione delle somme pagate[46] in quanto non potranno disporre di uno strumento coattivo per ottenere l'aggiornamento.

Quindi, sebbene la nuova normativa comunitaria abbia di certo apportato novità significative in tema di tutela dei consumatori che tengono conto delle innovazioni digitali e dei nuovi beni e servizi acquistati dal consumatore, rimangono tuttora insolute alcune questioni fondamentali, cui l'Unione europea, seppur con una frenetica (e non sempre coordinata) produzione normativa, sta cercando di fornire risposte via via introducendo nuove regole che potrebbero cercare di colmare le criticità che ad oggi appaiono irrisolte.

[46] In questo senso anche H. Schulte-Nolke, *Digital obligations of sellers of smart devices under the Sale of Goods Directive 771/2019,* cit., 60-61.

Contrastare l'astensionismo e favorire la partecipazione: il voto elettronico basato sulle tecnologie *Blockchain* e *Distributed Ledger**

Marco Ladu

Abstract

Con il presente saggio si intende offrire qualche spunto di riflessione attorno al dibattito sull'implementazione del voto elettronico, in particolare basato sulle tecnologie *Blockchain e Distributed Ledger*. Proprio attraverso il c.d. *e-voting*, infatti, sembra possibile poter incidere sul fenomeno, sempre crescente, dell'astensionismo (quantomeno di quello involontario) e tentare di rivitalizzare la partecipazione nel contesto democratico. Lo scritto non manca di porre in luce punti di forza e criticità alla base dello studio, della sperimentazione e dell'eventuale introduzione del voto elettronico, sia esso presidiato che non presidiato, tenendo a mente che i caratteri di personalità, eguaglianza, libertà e segretezza del diritto di voto devono sempre fungere da parametri per la verifica dell'efficienza e della compatibilità costituzionale di qualsivoglia meccanismo o modalità del suo esercizio.

The paper aims to offer some insight on the debate concerning the implementation of the electronic voting, particularly based on Blockchain and Distributed Ledger technologies. Indeed, through the so-called "e-voting" it seems possible to tackle the ever-increasing phenomenon of unintentional abstentionism and revitalize participation in the democratic process. The paper highlights strengths and weaknesses that the study, experimentation and introduction of e-voting, both supervised and unsupervised, underlie, bearing in mind that the essential features of personality, equality, freedom and secrecy of the right to vote must always work as parameters of the efficiency and constitutional compliance of any mechanism or way of voting.

Sommario

1. Brevi considerazioni introduttive. – 2. Un richiamo all'articolo 48 della Costituzione italiana quale parametro irrinunciabile per la valutazione delle modalità di esercizio del voto. – 3. L'astensionismo e il c.d. partito del non voto: come favorire la partecipazio-

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

ne politica? – 4. L'insieme delle tecnologie *Blockchain* e *Distributed Ledger* a fondamento del voto elettronico: punti di forza e ricorrenti criticità. – 5. Osservazioni conclusive.

Keywords

Voto elettronico – *Blockchain* – *Distributed Ledger* – astensionismo – partecipazione

1. Brevi considerazioni introduttive

Lo studio e l'implementazione di nuove modalità di voto, basate sulle tecnologie *Blockchain e Distributed Ledger*, continua a coinvolgere buona parte del mondo giuridico, comprese le scienze costituzionalistiche, il cui interesse per il sistema elettorale non può che essere centrale negli studi dei meccanismi di rappresentanza nel contesto democratico. A ciò si affianca, invero, il più ampio tema della partecipazione politica e quello, per converso, della crescente disaffezione rispetto alle dinamiche politico-istituzionali e che sfocia nel fenomeno dell'astensionismo. Aspetti, questi, che innegabilmente coinvolgono differenti discipline e settori di intervento, sia in ambito pubblico che privato, che attengono in particolar modo alla sensibilizzazione e alla formazione delle cittadine e dei cittadini e che in questa sede si ritiene di non approfondire. Il richiamo, tuttavia, appare necessario per delineare la cornice all'interno della quale il dibattito sulle modalità alternative di esercizio del voto, specie di quello elettronico, si svolge da qualche tempo e continua a svolgersi con un crescente interesse, man mano che le tecnologie accrescono.

Al netto di tali problematiche di ordine sociopolitico, in via preliminare occorre tenere conto di quanto l'implementazione di potenti software e tecniche algoritmiche sofisticate nonché lo sviluppo di tecnologie in grado di registrare operazioni con un sempre maggiore livello di sicurezza e attendibilità consentono oggi di studiare nuove modalità di partecipazione, a partire dall'utilizzo di piattaforme digitali e applicativi che assicurino un collegamento diretto tra i vari livelli di governo e la cittadinanza.

In questo contesto, con il presente scritto si intende offrire una panoramica dei punti di forza e delle criticità che seguirebbero all'introduzione di un sistema di voto elettronico generale e, cioè, finalizzato ad essere impiegato per le votazioni locali, nazionali, europee, referendarie e, perché no, meramente consultive. Ci si soffermerà, senza pretesa alcuna di esaustività, sulle caratteristiche tecniche della *Blockchain* (e dei registri distribuiti), valorizzando le potenzialità dei sistemi di voto elettronico in rapporto ad una maggiore partecipazione.

In termini generali, in un discorso complesso che sconta numerose "contaminazioni" tra le novità introdotte dalla rivoluzione digitale e i problemi classici delle democrazie costituzionali, da un lato si collocano le tecnologie e dall'altro la persona umana immersa nel contesto sociale, nella comunità politica alla quale appartiene e presso la quale è chiamata a partecipare. Traducendo queste premesse attraverso un'operazione insiemistica – ove i meccanismi della rappresentanza e della partecipazione politica intersecano l'implementazione delle nuove tecnologie in ambito politico-elettorale – or-

mai da qualche tempo si assiste all'introduzione nel linguaggio corrente di espressioni quali "democrazia 4.0", "democrazia digitale", "democrazia elettronica" e così via.
Tra i compiti del giurista, in questo rinnovato contesto, vi è anzitutto quello di vagliare la compatibilità, la tenuta e la coerenza di eventuali nuovi sistemi di voto rispetto ai parametri legali di natura costituzionale nonché quello di verificare in che modo le nuove tecnologie possano favorire la partecipazione alla vita politica e istituzionale del nostro Paese nel quadro di una rinnovata democrazia parlamentare.

2. Un richiamo all'articolo 48 della Costituzione italiana quale parametro irrinunciabile per la valutazione delle modalità di esercizio del voto

Svolte tali osservazioni di carattere introduttivo, in un certo senso più di metodo che di sostanza, non è possibile prescindere in questa sede da un breve richiamo, di natura teorica, alla funzione e ai parametri costituzionali del voto. Come si vedrà nel prosieguo, infatti, la tenuta di eventuali nuovi modelli e strumenti di esercizio del voto potrà essere verificata solo a fronte del rispetto della disciplina costituzionale in materia. Come è noto, l'art. 48 della Costituzione italiana stabilisce, al secondo comma, che: «Il voto è personale ed eguale, libero e segreto. Il suo esercizio è dovere civico» e proprio i caratteri di personalità, eguaglianza, libertà e segretezza – inscindibilmente legati alle altre disposizioni racchiuse nel medesimo articolo – devono fungere da parametri irrinunciabili per la verifica dell'efficienza e della compatibilità costituzionale di qualsivoglia meccanismo o modalità di esercizio del voto[1].
Il voto, sotto il profilo definitorio, costituisce un mezzo che consente alla volontà popolare (in realtà, alla volontà di chi si è espresso) di diventare decisione politica generale[2]. Attraverso il voto, o meglio attraverso la procedura di voto, la volontà popolare diventa decisione politica generale e, in tal senso, il voto può intendersi come votazione, cioè come processo funzionale all'espressione, alla comunicazione, alla rilevazione e alla conta delle preferenze espresse dai titolari di questo particolare diritto-dovere

[1] Per una ricostruzione della portata dell'art. 49 Cost., si rinvia, tra i vari contributi, a M. Armanno, *Personale, uguale, libero e segreto. Il diritto di voto nell'ordinamento costituzionale italiano*, Napoli, 2018; D. Casanova, *Eguaglianza del voto e sistemi elettorali. I limiti costituzionali alla discrezionalità legislativa*, Napoli, 2020; G. Chiara, *Contributo allo studio del diritto di voto. Appunti delle lezioni*, Milano, 2012; E. Grosso, *Articolo 48* (commento), in R. Bifulco - A. Celotto - M. Olivetti (a cura di), *Commentario alla Costituzione*, Torino, 2006; F. Lanchester, *Voto* (voce), in *Enciclopedia del diritto*, Milano, 1993, 1107 ss.; M. Rubechi, *Il diritto di voto. Profili costituzionali e prospettive evolutive*, Torino, 2016.

[2] Sul punto restano insuperabili le parole di J. J. Rousseau, il quale nella sua opera *Il contratto sociale*, ebbe modo di evidenziare che spesso vi è «molta differenza tra la volontà di tutti e la volontà generale; questa mira unicamente all'interesse comune, l'altra all'interesse privato e non è che una somma di volontà particolari; ma se si toglie da queste stesse volontà il più e il meno che si eliminano reciprocamente, resta, come somma delle differenze, la volontà generale». Inoltre, Rousseau pone quale tema centrale quello della libertà del singolo e della necessità che ciascuno sia debitamente informato. Difatti, «perché si abbia chiaramente l'enunciazione della volontà generale» è fondamentale «che non ci siano società parziali nello Stato e che ogni Cittadino dia il proprio parere pensando solo con la sua testa» (J. J. Rousseau, *Il contratto sociale*, Torino, 1980, 79-80).

civico e politico[3].

Osservando ancor più da vicino la dinamica del voto e della procedura che ne consente l'espressione, è possibile far emergere – come già osservato in dottrina – il principio che sottende al funzionamento delle istituzioni democratiche e all'assunzione delle decisioni politiche, vale a dire il principio maggioritario[4]. In altre parole, nel contesto elettorale, il principio maggioritario diviene la chiave di lettura del voto stesso in quanto sono proprio i risultati ad essere declamati secondo tale principio: l'autonomia che spetta al singolo elettore, mediante il voto, riesce a combinarsi con quella degli altri. A tal proposito, molto efficace risulta un'espressione impiegata in dottrina e secondo la quale il meccanismo di voto consentirebbe di addivenire ad un «autogoverno collettivo egualitario»[5]: un'espressione che attesta l'importanza dell'esercizio del diritto-dovere di voto al fine di esprimere la propria scelta e concorrere, in modo paritario, al governo collettivo della comunità politica. La scelta personale si fonde così con la scelta altrui e, attraverso l'applicazione del principio maggioritario, diviene il governo di tutti[6].

Tanto premesso, operando una scelta di campo, si cercherà di affrontare in questa sede il tema del voto elettronico ragionando parallelamente attorno ai temi dell'astensionismo e della partecipazione politica, tentando di valorizzare come l'utilizzo delle nuove tecnologie possa forse condurre verso un maggior coinvolgimento nei processi di formazione di quella volontà generale alla quale si è poc'anzi fatto riferimento.

La tesi di fondo che si intende sostenere con il presente scritto è quella di ritenere che l'introduzione di eventuali nuove modalità di voto, quali il voto elettronico, possano anzitutto incidere significativamente su alcune sottoclassi dell'astensionismo, di cui si dirà, nonché possano in un certo senso rivitalizzare la partecipazione al contesto de-

[3] Cfr. G. Gometz, *Democrazia elettronica. Teoria e tecniche*, Pisa, 2017, 155.

[4] Si segnala, al riguardo, una recente opera monografica – di taglio comparatistico – con la quale il tema del principio maggioritario viene affrontato nell'ottica di una sua attenuazione in favore di metodi alternativi per la determinazione delle decisioni politiche generali (ad esempio, il metodo del consenso). Si rinvia, pertanto, a M. Frau, *L'attenuazione del principio maggioritario. Istituti e modelli alternativi al principio deliberativo di maggioranza*, Napoli, 2022.

[5] Cit. G. Gometz, *Democrazia elettronica. Teoria e tecniche*, cit., 161. In particolare, si osservi la nota n. 16 per la ricostruzione del concetto sottostante all'espressione impiegata, con riferimenti utili per una ricostruzione anche in chiave storica e filosofica.

[6] Per un approfondimento di queste tematiche si rinvia in particolare al lavoro di Gianmarco Gometz (*Democrazia elettronica. Teoria e tecniche*), il quale, argomentando sul valore democratico del voto elettronico e sull'esigenza di assicurarne l'uguaglianza, l'espressività e la sicurezza, ha avuto modo di evidenziare che «Il nesso strumentale rispetto a un'autentica sovranità popolare è poi palese per la *sicurezza* della tecnologia di voto, sia nella sua declinazione pubblica che in quella privata. La prima, infatti, concerne l'uguaglianza, la regolarità del computo e la genuinità del voto dei cittadini, e si persegue attraverso meccanismi diretti ad assicurare che solo gli aventi diritto votino, soltanto una volta ciascuno (per ogni questione su cui è richiesto il voto) e con sufficienti garanzie di inalterabilità e incancellabilità del proprio voto. Essa consiste insomma nella capacità della tecnologia di favorire il fedele rispecchiamento tra le preferenze politiche di ciascuno dei cittadini e i risultati ufficiali delle consultazioni popolari. La sicurezza privata, d'altro canto, consiste in misure a tutela dell'anonimità e della segretezza, a loro volta strumentali alla libertà del voto, ossia alla protezione della signoria del cittadino di votare come meglio crede, al riparo da qualsiasi controllo, coercizione o ritorsione. Poiché la libertà di voto è consustanziale alla libertà/autonomia dei votanti, possiamo dire che più l'espressione della volontà dei cittadini è genuina ed esente da interferenze e manipolazioni esterne, più essi sono autonomi/sovrani» (G. Gometz, *Democrazia elettronica. Teoria e tecniche*, cit., 162).

mocratico, rinnovando le procedure di voto, senza trascurare l'importanza di garantire un sistema di elezione sicuro, ritenuto affidabile per la collettività e rispettoso, come premesso, dei canoni e dei parametri costituzionali, i quali fungono da filo conduttore in un discorso all'interno del quale si inseriranno parecchie questioni problematiche legate all'effettivo rispetto dei principi di libertà, segretezza, uguaglianza e personalità del voto.

3. L'astensionismo e il c.d. partito del non voto: come favorire la partecipazione politica?

L'astensionismo è da qualche decennio divenuto un fenomeno cronico che, potremmo dire, caratterizza ormai il nostro sistema politico, tanto che si giunge a considerare coloro che si astengono quale un vero e proprio partito, il c.d. partito del non voto[7].
Dalla nota piattaforma *Openpolis*, che funge da valido osservatorio sui temi della democrazia e della partecipazione politica, è possibile trarre tutta una serie di dati – rielaborati da fonti del Ministero dell'Interno – sul fenomeno dell'astensionismo[8].
Partendo dal dato dell'affluenza alle elezioni politiche dal 1948 ad oggi, emerge un calo costante nella partecipazione al voto. Da un'affluenza del 92,23% del 1948, infatti, si è passati ad un'affluenza 63,79% registrata nelle ultime elezioni politiche del 25 settembre 2022[9]. Il dato è sconcertante, ancor più evidente se viene considerato *a contrario*: il 36,21% degli elettori non ha preso parte alle ultime elezioni, ciò significa che quasi quattro persone su dieci oggi si esimono dall'esprimere il proprio voto, per le più svariate ragioni, come a breve si vedrà.
Tornando ai dati e prendendo a campione delle annualità intermedie prima degli anni 2000 per poi concentrarsi sulle ultime legislature, si nota come nel 1976 l'affluenza fosse pari al 93,39%, nel 1987 all'88,83%, nel 1994 all'86,31%, nel 2006 all'83,62%, nel 2008 all'80,51% per poi crollare 75,2% nel 2013, al 72,94 nel 2018 e, come detto, al 63,79% di quest'anno[10], segnando il minimo storico.
Se si osservano i dati, in termini percentuali, con riferimento al partito del non voto[11],

[7] Invero, ragionare attorno all'idea di un "partito" del "non voto" è quasi paradossale, poiché trasformare l'astensionismo in un partito è un'operazione che tradisce il significato e il ruolo costituzionale del partito. Difatti, l'art. 49 Cost. indica i partiti – che, come è noto, sotto il profilo privatistico non sono altro che associazioni non riconosciute – quali strumenti per concorrere con metodo democratico alla determinazione della politica nazionale, dunque un qualcosa di diametralmente opposto al fenomeno dell'astensionismo.

[8] Si rinvia ad un recente report*, L'astensionismo e il partito del non voto* in *openpolis.it*, 11 ottobre 2022.

[9] Sul punto, in dottrina è stato osservato, rispetto all'ultima tornata elettorale, che «Forse ancor più significativo è il registrato aumento dell'astensionismo (poco meno del 64% di votanti) cui si deve comunque aggiungere circa il 4,5% tra voti nulli e schede bianche» (A. D'Andrea, *Il Parlamento e il Governo: le ragioni del rispettivo disallineamento costituzionale (sempre reversibile)*, in *Diritto costituzionale. Rivista quadrimestrale*, 3, 2022, 40).

[10] Tutti i dati riportati sono riferiti all'elezione della Camera dei Deputati.

[11] La percentuale riferita al partito del non voto è il risultato della somma di coloro i quali non si sono recati alle urne e di coloro che non si sono espressi lasciando la scheda bianca. La percentuale è calcolata sull'intero corpo elettorale e prendendo in considerazione le singole liste.

è possibile sottolineare come per la prima volta nel 1996 la percentuale degli astenuti, con il 19,66%, ha superato il primo partito che aveva ottenuto il 16,19% dei voti validamente espressi. Da quel momento in poi, nell'anno 2001, si sono astenuti il 22,05% degli aventi diritto al voto e il primo partito si è attestato al 22,18% (quindi sostanzialmente in posizione equivalente). Il numero degli astenuti è calato nelle annate 2006 e 2008 per poi ricrescere e superare nuovamente il partito più votato nel 2013 (25,65% contro il 18,43%), nel 2018 (27,89% contro il 23,08%) e, da ultimo, nel 2022 (37,28% contro il 15,87%). In particolare, proprio le ultime elezioni, quelle del 25 settembre 2022, si caratterizzano per un notevole *gap* tra il numero di astenuti, pari a 17.159.014, e la prima forza politica, sostenuta da 7.302.517 di elettori.

La situazione, di per sé drammatica e allarmante, deve però spingere, *in primis* la figura del giurista, ad analizzare il contesto all'interno del quale il dato si attesta e, soprattutto, a cercare di trovare delle soluzioni che possano abbattere il fenomeno dell'astensionismo e favorire il più possibile la partecipazione alla vita politica e democratica del nostro Paese.

Anche per queste ragioni, il 14 aprile 2022 è stato presentato, in chiusura dei lavori di una commissione costituita *ad hoc* per indagare le cause dell'astensionismo[12], il libro bianco "Per la partecipazione dei cittadini: come ridurre l'astensionismo e agevolare il voto"[13], che consente di offrire in questa sede utili elementi per ricostruire le cause dell'astensionismo e tentare di approntare delle risposte efficaci al fenomeno.

Anzitutto, lo stesso libro bianco, affronta il tema dell'astensionismo operando una *summa divisio* tra astensionismo "reale" e astensionismo "apparente".

Quanto all'astensionismo "reale", che qui maggiormente interessa a fini argomentativi, è possibile a sua volta individuarne tre differenti classi: l'astensionismo "involontario", determinato dalla impossibilità di recarsi alle urne e che vede soprattutto coinvolti gli anziani, gli infermi, gli ospiti dei presidi sanitari o socio-sanitari, i fuorisede per motivi lavorativi o di studio nonché coloro che non si trovano in sede perché temporaneamente altrove per le più varie ragioni (ad es., per turismo); l'astensionismo "per disinteresse", frutto di una indifferenza rispetto al momento elettorale, alla vita politica in generale o, comunque, di una scarsa considerazione della capacità di incidere sulle decisioni politiche collettive; da ultimo, l'astensionismo "di protesta", quale

[12] Come riportato sul portale del Ministero per le riforme istituzionali e la semplificazione normativa, «Il 22 dicembre 2021 è stata istituita la Commissione di esperti per indagare le cause dell'astensionismo e proporre soluzioni in grado di arginare questo fenomeno, da anni in crescita nel nostro Paese. membri della Commissione, che hanno lavorato a titolo gratuito, sono: Franco Bassanini, professore e costituzionalista che ha coordinato i lavori, Gian Carlo Blangiardo, presidente dell'ISTAT, Alessandra Ferrara ricercatrice dell'ISTAT, Leonardo Morlino, professore di Scienza della politica, Paolo Feltrin, politologo ed esperto in materia elettorale, Cristina De Cesare, consigliera della Camera dei Deputati, Adriana Apostoli ed Elisabetta Lamarque, professoresse di diritto costituzionale, Antonio Floridia, già presidente della Società Italiana di Studi Elettorali, Fabrizio Orano prefetto, direttore del Ministero dell'Interno, Paolo Donzelli, consigliere della Presidenza del Consiglio dei ministri presso il Dipartimento per la trasformazione digitale. Ad essi si sono aggiunti alcuni componenti del Gabinetto del Ministro e del Dipartimento per le riforme istituzionali della Presidenza del Consiglio dei ministri» (v. *Presentato il Libro bianco sull'astensionismo*, comunicato stampa del 2 maggio 2022, disponibile all'indirizzo *riformeistituzionali.gov.it*).

[13] Il documento, in formato e-book, è liberamente consultabile e scaricabile attraverso il portale del Ministero per le riforme istituzionali e la semplificazione normativa (*riformeistituzionali.gov.it*).

espressione massima del proprio dissenso nei confronti della politica in generale o della politica del momento. Un discorso a parte, e che qui si ritiene esclusivamente di dover accennare, può farsi in relazione ai risultati dei sondaggi politici periodici, i quali rischiano di condurre ad un'astensione dal voto sul presupposto che l'elettore maturi l'idea che la sua scelta non possa incidere su un assetto già di per sé determinato. L'astensionismo di questo tipo si colloca, dunque, accanto a quello per disinteresse, manifestandosi perlopiù a seguito dello svilupparsi di un sentimento di arrendevolezza o rassegnazione nell'elettore.

In ogni caso, una volta operate queste distinzioni di carattere meramente teorico, è possibile ritenere che l'implementazione di una nuova modalità di voto elettronico, nel caso di specie basate sull'insieme delle tecnologie *Blockchain* e *Distributed Ledger*, possa apportare dei benefici specialmente in relazione alle problematiche connesse all'astensionismo involontario, con conseguente aumento della partecipazione per alcune categorie[14]. Difatti, immaginare che il voto elettronico possa incentivare la partecipazione di coloro i quali non si recano alle urne per scarsa affezione o in segno di protesta, appare complesso, ma non è del tutto illogico pensare che si possa comunque ingenerare nel sistema un effetto di "trascinamento" secondo il quale al crescere della partecipazione di determinate categorie di soggetti possa comunque conseguire un progressivo coinvolgimento di altri, proprio sulla base di una tendenza virtuosa.

Il presupposto del ragionamento fin qui condotto, dunque, è quello di considerare senza "se" e senza "ma" l'astensionismo (specie involontario, ma non soltanto) come un serio problema del quale è necessario occuparsi. Come poc'anzi sostenuto, quindi, dinanzi a problemi e vecchie o nuove sfide, è doveroso tentare di ragionare su cosa implicherebbe l'introduzione nel nostro Paese di un sistema di voto di tipo elettronico. Naturalmente parliamo in astratto e per ipotesi perché ad oggi, in Italia, non si sono svolte consultazioni con tale modalità, se non in un contesto circoscritto all'attività referendaria consultiva[15]. Ciononostante, nel corso della XVIII legislatura, è stato previsto, nella legge di bilancio 2020[16], un fondo per la sperimentazione del voto elettronico con riferimento alle elezioni europee, nazionali e per i referendum. La sperimentazione, in particolare, dovrebbe coinvolgere gli italiani residenti all'estero e gli elettori temporaneamente si trovano fuori dal comune di residenza per motivi di lavoro, di studio o per ragioni medico-sanitarie.

Con d.l. 77/2021[17] (poi convertito, con modificazioni, nella l. 108/2021) la sperimen-

[14] Naturalmente, come si dirà nel prosieguo, una particolare attenzione dovrà essere dedicata alla categoria degli anziani o degli infermi, per i quali l'introduzione del voto elettronico porterebbe con sé altre problematiche, specialmente connesse alla minore dimestichezza nell'uso delle nuove tecnologie.

[15] Si ricorda la consultazione referendaria lombarda del 22 ottobre 2017 concernente l'attivazione di iniziative istituzionali necessarie per l'attribuzione di ulteriori forme e condizioni particolari di autonomia *ex* art. 116, c. 3, della Costituzione. In questa occasione, infatti, è stato possibile esprimere il proprio voto in una sede presidiata, vale a dire presso le sezioni elettorali regolarmente istituite, mediante però l'utilizzo di tablet.

[16] In particolare, il Fondo è stato istituito dall'art. 1, cc. 627-628, della l. 160/2019 ("Bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022").

[17] A introdurre la disposizione, precisamente, l'art. 38-bis, c. 10, del d.l. 77/2021 ("Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure").

tazione è stata estesa alle elezioni amministrative e regionali, in programma prima per il 2022 e poi, a seguito di rinvio, per il 2023, con integrazione ulteriore del fondo[18]. Con apposito decreto ministeriale del 9 luglio 2021, successivamente integrato da un ulteriore decreto del 21 ottobre 2021, sono state adottate le "Linee guida per la sperimentazione di modalità di espressione del voto in via digitale", come previsto dal provvedimento di istituzione del fondo.

Al di là dell'eventuale introduzione del c.d. voto elettronico per rispondere all'astensionismo involontario, oggetto specifico del successivo paragrafo, quel che preme sottolineare in questa sede, a conclusione del tema dell'astensionismo in generale, è che innegabilmente esso può essere contrastato con tutta un'altra serie di strumenti che puntino a favorire la partecipazione democratica.

All'uopo, le direttrici sulle quali intervenire sembrano essere almeno due: se da un lato resta fermo il tema della sensibilizzazione alla partecipazione politica mediante i partiti o, più in generale, un'attività di sensibilizzazione rispetto alle dinamiche politico-istituzionali del nostro Paese, che pongano ad esempio al centro l'importanza di prendere parte ad occasioni preziose quali le consultazioni elettorali o referendarie, dall'altro lato si dovrebbe maggiormente coltivare l'attenzione nei confronti degli istituti cosiddetti di democrazia diretta, cercando di potenziarli e renderli più efficaci.

Sotto il primo profilo, quello della sensibilizzazione *lato sensu* politica, è chiaro che si tratta di incidere specialmente sul terreno della formazione e dell'insegnamento, così come sul potenziamento di campagne di sensibilizzazione e la sfida non è di certo alla portata del solo giurista, ma coinvolge un intero sistema di competenze e professionalità sia in ambito pubblico che privato.

Sotto il secondo profilo, invece, è necessario guardare al tema della rivitalizzazione della partecipazione politica mediante il potenziamento di istituti di democrazia diretta e, specialmente, delle consultazioni referendarie, le quali oggi risultano condizionate dalla presenza di ostacoli non soltanto di natura procedurale[19]. In questo caso, è interessante notare come alla sperimentazione, già richiamata, delle modalità di voto elettronico, si affianca – con medesimi fondi e stanziamenti – la predisposizione di una piattaforma pubblica per la raccolta digitale delle firme idonee ai sensi dell'art. 75 Cost.[20].

---

[18] Il rinvio e l'integrazione, pari ad un milione di euro, sono stati disposti dal d.l. 41/2022 ("Disposizioni urgenti per lo svolgimento contestuale delle elezioni amministrative e dei referendum previsti dall'art. 75 della Costituzione da tenersi nell'anno 2022, nonché per l'applicazione di modalità operative, precauzionali e di sicurezza ai fini della raccolta del voto").

[19] In proposito è stato di recente messo in luce che la «rimozione di ostacoli alla partecipazione popolare anche attraverso forme di democrazia diretta sembra poter svolgere una funzione di rafforzamento della responsabilità politica dei rappresentanti, l'esercizio del cui mandato sarebbe, proprio attraverso i referendum, verificabile anche prima delle successive elezioni (nelle quali, peraltro, la responsabilità può essere più difficile da far valere). Inoltre, in questo modo gli elettori avrebbero maggiori strumenti per concorrere alla determinazione della politica nazionale, assumendo direttamente alcune decisioni alle quali tengono in particolare laddove i loro rappresentanti esitassero troppo a lungo, come accade, ad esempio, per l'eutanasia. In questo modo – come già detto – ne risulterebbe probabilmente rivitalizzato l'intero circuito democratico» (A. Pertici, *Il referendum abrogativo e il suo procedimento, tra garanzie e ostacoli. Un bilancio complessivo*, in *Quaderni costituzionali*, 3, 2022, 520).

[20] Per un approfondimento del tema si rinvia alla voce *Raccolta digitale delle firme per i referendum* della scheda di lettura, elaborata dal Servizio studi della Camera dei Deputati, *Digitalizzazione del procedimento*

Accanto al tema del referendum abrogativo, sempre nel corso della precedente legislatura, vi è stato poi il tentativo di introdurre un nuovo istituto giuridico nell'ordinamento italiano, vale a dire il cosiddetto referendum propositivo. In relazione a ciò, è stata depositata presso la Camera dei Deputati, in data 21 febbraio 2019, una proposta di modifica dell'art. 71 Cost., poi approvata e trasmessa all'altro ramo del Parlamento in data 22 febbraio 2019. Oggi la proposta è ricompresa nell'A.S. 1089 (che ha assorbito i progetti C. 726, C. 727, C. 987, C. 1447 presentati alla Camera dei Deputati). La proposta, al momento accantonata, contiene l'introduzione dell'istituto del referendum propositivo e, precisamente, all'art. 1, c. 1, del progetto si prevede che: «Quando una proposta di legge è presentata da almeno cinquecentomila elettori e le Camere non la approvano entro diciotto mesi dalla sua presentazione, è indetto un referendum per deliberarne l'approvazione. Se le Camere la approvano con modifiche non meramente formali, il referendum è indetto sulla proposta presentata, ove i promotori non vi rinunzino. La proposta approvata dalle Camere è sottoposta a promulgazione se quella soggetta a referendum non è approvata». Inoltre, al comma terzo del medesimo articolo è stabilito che: «La proposta sottoposta a referendum è approvata se ottiene la maggioranza dei voti validamente espressi, purché superiore a un quarto degli aventi diritto al voto»[21]. Vi sono poi altre disposizioni, che qui si tralasciano, relative ai casi in cui il referendum propositivo non sia ammissibile ovvero relative al giudizio di ammissibilità che la Corte costituzionale sarebbe chiamata a svolgere. Quel che qui appare interessante osservare è che l'istituto in questione consentirebbe, in larga misura, di poter superare le ben note difficoltà, anche tecniche, in relazione allo strumento del referendum abrogativo[22]. Difatti, se da un lato il referendum abrogativo consente di incidere sul piano della legislazione primaria esclusivamente mediante una tecnica ablativa di parti di testo, nel caso in cui nel nostro ordinamento fosse introdotto il referendum propositivo, gli elettori avrebbero modo, al pari dell'iniziativa legislativa (poiché in entrambi i casi si tratta di avviare l'*iter legis*), di presentare un loro testo, articolato e anche complesso, assicurandosi però la determinazione di un voto popolare nel caso in cui entro diciotto mesi il Parlamento si sia dimostrato inerte di fronte alla proposta. In questo si colgono le potenzialità dello strumento del referendum propositivo.

Esaurito, nel perimetro del presente contributo, il riferimento al tema dell'astensionismo e alla più ampia problematica della partecipazione politica nel contesto democratico italiano, è possibile focalizzarsi sul voto elettronico, intendendo tale strumento quale uno dei possibili rimedi ad alcuni dei problemi fin qui esposti e strettamente connesso all'esigenza di assicurare la "qualità" della rappresentanza politica sul presupposto di una ampia partecipazione.

elettorale e sperimentazione del voto elettronico in *camera.it*, 20 settembre 2022

[21] A.S. 1089, Disegno di legge costituzionale, *Disposizioni in materia di iniziativa legislativa popolare e di referendum*, in *senato.it*.

[22] Sull'istituto in questione è recente il significativo contributo di A. Pertici, *Il referendum abrogativo e il suo procedimento, tra garanzie e ostacoli. Un bilancio complessivo*, in *Quaderni costituzionali*, 3, 2022, 499 ss.

4. L'insieme delle tecnologie *Blockchain* e *Distributed Ledger* a fondamento del voto elettronico: punti di forza e ricorrenti criticità

Il dibattito sull'introduzione del cosiddetto *e-voting* o voto elettronico è ormai risalente nel tempo in quanto si è certamente imposta una riflessione sul punto a partire dall'accrescere della fruibilità delle nuove tecnologie nel nuovo millennio[23]. Oggi, in particolare, l'oggetto di studio è strettamente legato alla possibilità di applicare, su larga scala, le tecnologie *Blockchain* e *Distributed Ledger*. Ed è proprio grazie all'insieme delle suddette tecnologie che è possibile sperare nella messa a punto di sistemi di voto elettronico che rispettino tanto i già menzionati parametri costituzionali quanto le esigenze, che potremmo definire di carattere soggettivo, legate alla sicurezza, affidabilità e fiducia che l'elettore ripone nel sistema di voto.

Si parta, però, da una breve e sintetica ricostruzione del meccanismo di funzionamento e delle caratteristiche di fondo delle tecnologie basate sulla *Blockchain* e sui registri distribuiti[24].

La *Blockchain* è, anzitutto, un vero e proprio sistema di tecnologie diverse che è in grado, mediante una totale decentralizzazione, di mettere insieme delle catene di blocchi, i cosiddetti registri distribuiti (*Distributed Ledger*). Una caratteristica tecnica, quest'ultima, fondamentale in relazione all'utilizzo di tale insieme di tecnologie per il voto elettronico in quanto consente di verificare il consenso espresso (nel caso di specie, il voto) su tutti i "nodi" della rete. Per fornire maggiore concretezza a quanto appena espresso, è possibile descrivere le tecnologie *Blockchain* e *Distributed Ledger* attraverso (almeno) sei caratteristiche peculiari.

In primo luogo, come accennato, può trattarsi di un sistema "decentralizzato". Questo aspetto è fondamentale ed è il punto di forza dei sistemi connessi alla *Blockchain*,

[23] Tra i contributi in tema di voto elettronico si rinvia ad A. Agosta – F. Lanchester – A. Spreafico (a cura di), *Elezioni e Automazione. Tutela della regolarità del voto e prospettive di innovazione tecnologica*, Milano, 1989; E. Bettinelli, *La lunga marcia del voto elettronico in Italia*, in *Quaderni dell'osservatorio elettorale*, 1, 2002; E. Caterina – M. Giannelli, *Il voto ai tempi del* blockchain*: per una rinnovata valutazione costituzionale del voto elettronico*, in *Rivista AIC*, 4, 2021; F. Corona, *E-democracy fra sviluppo delle tecnologie e processi partecipativi*, in *Cammino diritto. Rivista di informazione giuridica*, 9, 2020; V. Desantis, *Le nuove prospettive dell'*internet voting *tra avanzamento tecnologico e sostenibilità giuridica*, in *Rivista AIC*, 4, 2022; A. Gratteri, *Il valore del voto. Nuove tecnologie e partecipazione elettorale*, Padova, 2015; Id., *Finalità e problemi del voto elettronico: le prospettive della sua attuazione in Italia*, in *Forum di Quaderni costituzionali*, 25 marzo 2015; G. Gometz, *Democrazia elettronica. Teoria e tecniche*, cit.; G. Gometz - M. T. Folarin, *Voto elettronico presidiato e blockchain*, in *Ragion pratica*, 2, 2018, 318 ss.; A. G. Orofino, *L'e-vote,* in F. Sarzana di S. Ippolito (a cura di), *E-Government. Profili teorici ed applicazioni pratiche del Governo digitale*, Piacenza, 2003, 361 ss.; D. Pitteri, *Democrazia elettronica*, Bari, 2007; A. Randazzo, *Voto elettronico e Costituzione (note sparse su una questione ad oggi controversa)*, in questa *Rivista*, 2, 2022, 49 ss.; M. Rosini, *Il voto elettronico tra standard europei e principi costituzionali, prime riflessioni sulle difficoltà di implementazione dell'*e-voting *nell'ordinamento costituzionale italiano*, in *Rivista AIC*, 1, 2021; M. Rospi, *Internet e diritto di voto*, in M. Nisticò - P. Passaglia (a cura di), *Internet e Costituzione*, Torino, 2014, 263 ss.; A. Sarais, *Democrazia e tecnologie. Il voto elettronico*, Bologna, 2008; L. Trucco, *Il voto elettronico nella prospettiva italiana e comparata*, in *Diritto dell'informazione e dell'informatica*, 1, 2011, 47 ss.; Id., *Il voto elettronico nel quadro della democrazia digitale*, in T. E. Frosini - O. Pollicino - E. Apa - M. Bassini (a cura di), *Diritti e libertà in Internet*, Firenze, 2017, 425 ss.

[24] Per un rapido, ma esaustivo, approfondimento sul tema della *Blockchain*, si rinvia al portale *Osservatori Digital Innovation* del Politecnico di Milano e, in special modo, sia al *Glossario della Blockchain* sia all'articolo *La Blockchain spiegata semplice. Definizioni, funzionamento, applicazioni e potenzialità*, in *blog.osservatori.net*.

nei quali si riscontra una totale assenza di controllo da parte di un nodo centrale e, dunque, di porsi al riparo da una manipolazione o alterazione eterodiretta di quel che avviene nella rete.
Secondo aspetto, vi è una totale "tracciabilità dei trasferimenti" perché ciò che avviene tra un nodo e l'altro – e che viene incasellato all'interno di questi diversi registri distribuiti – è pienamente tracciabile e accessibile, in assenza, come detto, di una centralizzazione del controllo.
All'assenza di centralizzazione e alla tracciabilità dei trasferimenti si affianca la "disintermediazione". Nell'utilizzo dei sistemi *Blockchain* non vi è un intermediario attraverso il quale transitare. Nel caso dell'*e-voting*, tra l'espressione del voto e lo stoccaggio del voto non vi è intermediazione e ciò si traduce nell'assenza di entità o soggetti che si interpongono nel processo di raccolta e conservazione del voto. Vi è, quindi, l'assenza di un controllo tanto *top-down* quanto nei singoli passaggi, orizzontali, di quel che avviene nella rete.
Come quarto aspetto, il sistema garantisce "trasparenza e verificabilità" di ciò che avviene tra i vari nodi e, dunque, oltre alla tracciabilità dei trasferimenti, il sistema assicura l'accesso alla rete consentendo di verificare che tutto funzioni nel modo corretto e che non vi siano state alterazioni o cancellazioni dei dati acquisiti.
Ulteriore caratteristica è "l'immutabilità" del registro, in base alla quale i dati acquisiti non possono essere modificati se non con il consenso della rete, il quale è espresso, come detto, su tutti i singoli nodi.
Da ultimo, è possibile la "programmabilità dei trasferimenti", vale a dire la possibilità di prevedere il compimento di determinate azioni al verificarsi di condizioni preventivamente imposte.
Le caratteristiche ora richiamate, unitamente intese, consentono di ragionare sul tema del voto elettronico impiegando i registri distribuiti e la *Blockchain* sia "prima del voto", per esempio con la possibilità di ridurre notevolmente il rischio di controllo mediatico della campagna elettorale, "durante il voto", elevando le garanzie relative all'identificazione degli elettori, della raccolta e dell'univocità del voto espresso nonché "all'esito del voto", permettendo lo svolgimento di audit che assicurino, in un'ottica di trasparenza e verificabilità, la correttezza del procedimento svolto e l'assenza di violazioni[25].
Le tecnologie in questione, dunque, sembrano essere astrattamente idonee a fungere da base per lo sviluppo di programmi che consentano la votazione per via elettronica. Tuttavia, calandosi nella realtà delle cose, bisogna indagare come in concreto la *Blockchain* possa condurre ad una digitalizzazione delle operazioni di voto.
Occorre perciò anzitutto domandarsi: cosa si intende per digitalizzazione del voto?
L'interrogativo, apparentemente semplice, rivela invece tutta una congerie di problematiche e questioni, delle quali molte aperte e in cerca di una risposta, tanto sotto il

[25] Questi ed altri profili legati all'introduzione della tecnologia *Blockchain* nei più svariati ambiti applicativi sono ben evidenziati da M. Bellini, *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*, in *blockchain4innovation.it,* 28 settembre 2022. Il tema degli audit, tuttavia, resta uno dei principali nodi da risolvere poiché, se sotto il profilo tecnico-informatico è ricorrente l'affermazione secondo la quale sia possibile "interrogare" i sistemi e gli applicativi impiegati al fine di verificarne il corretto funzionamento, in termini pratici non è agevole comprendere chi e in che misura possa effettuare tali controlli e assicurando quale livello di garanzia. Resta dunque centrale un'analisi di tale profilo, che certamente potrà essere oggetto di viva discussione.

profilo tecnico quanto sotto il profilo giuridico.

In primis, sulla scorta di una felice differenziazione che attiene, sotto il profilo linguistico, al mondo anglosassone – la distinzione, cioè, tra *digitization* (la conversione di testi, di audio, di immagini o di video dall'analogico al digitale) e *digitalization* (l'impiego delle tecnologie digitali per sviluppare e implementare nuovi modelli e processi) – bisogna opportunamente distinguere la "digitizzazione" del voto, intesa quale mero passaggio al digitale dei documenti cartacei sulla base delle tradizionali procedure, dalla "digitalizzazione", la quale può consistere in un ripensamento complessivo del processo e, dunque, ad un passaggio al digitale che comporti un parziale o totale stravolgimento delle procedure tradizionali[26]. In altre parole, una cosa è rendere digitale la scheda elettorale, i registri delle elettrici e degli elettori, i verbali e tutta la documentazione necessaria all'espletamento della tornata elettorale, prevedendo l'utilizzo di computer o tablet presso le tradizionali sedi di voto (assicurando, quindi, il voto "presidiato"), altra cosa è immaginare lo sviluppo di software e modalità di voto del tutto differenti, con procedure di identificazione, di espressione del voto, di verbalizzazione del tutto diverse dall'attuale sistema e, magari, giungendo alla soluzione "estrema" di abbandonare i seggi istituiti presso le sezioni elettorali (voto "non presidiato").

Insomma, alla luce di quanto sino ad ora espresso, si rende subito necessario chiarire che la scelta del legislatore che intendesse introdurre il voto elettronico non è di certo una scelta vincolata in un senso o nell'altro, tanto in relazione all'utilizzo del digitale rispetto alla procedura esistente, quanto in relazione alla scelta di continuare ad assicurare che il voto si svolga in modo presidiato o sia viceversa possibile accedere al voto in qualsiasi luogo ci si trovi.

Già soltanto questi primi aspetti divengono, evidentemente, dirimenti se si ragiona di digitalizzazione del diritto di voto sulla base delle tecnologie *Blockchain* e *Distributed Ledger*.

La scelta, in ogni caso, deve essere frutto di un concreto bilanciamento tra i vari interessi e diritti in gioco, siano essi strettamente connessi ad una rigorosa applicazione dell'art. 48 Cost. sia derivanti da un'analisi degli strumenti necessari ad assicurare i principi costituzionali in materia di voto. Se. Infatti, si volesse incentivare al massimo la partecipazione e snellire la procedura, è quasi superfluo sottolineare le enormi potenzialità di una votazione accessibile da un qualsiasi dispositivo elettronico, in qualsiasi tempo, essendo sufficiente una connessione alla rete Internet. Dall'altro lato, la necessità di garantire i canoni di segretezza, personalità, eguaglianza e libertà del voto, nonché la formalità del momento elettorale, la sicurezza e la fiducia che gli elettori devono riporre nel meccanismo di voto, inducono a pensare che, allo stato attuale delle cose, la forma del voto presidiato possa maggiormente assicurare tali esigenze rispetto a un totale decentramento della procedura attraverso modalità elettroniche.

Queste sono alcune delle prime problematiche che sottendono all'introduzione di un sistema elettronico di voto e che, risultano ancor più comprensibili, se si guarda – senza alcuna pretesa di esaustività – alle esperienze di Stati esteri che hanno adottato, talvolta anche abbandonandolo per poi riprenderlo, il voto elettronico.

[26] Sul punto, si veda l'interessante contributo di C. Di Nardo, *Digitizzazione, Digitalizzazione, Trasformazione Digitale: qual è la differenza?*, in *deltalogix.blog* , 3 marzo 2021.

I casi emblematici che saranno qui evocati sono quelli della Svizzera e dell'Estonia[27]. Partendo dalla Svizzera, si deve immediatamente segnalare che, per il momento, il sistema di voto elettronico è stato sospeso ed è in fase di studio per una nuova introduzione[28]. Osservando, però, l'esperienza degli anni passati, in Svizzera in ben dieci Cantoni è stato possibile, fino ai primi mesi del 2019, votare tramite il proprio dispositivo, grazie a due sistemi messi a disposizione l'uno dalla Posta Svizzera e l'altro dal Catone di Ginevra. La fase sperimentale, tuttavia, non si è potuta concludere poiché il Consiglio federale svizzero – a seguito di una consultazione svolta nel 2018[29] – ha deciso di non procedere con la revisione della Legge federale sui diritti politici (LDP)[30], la quale sarebbe dovuta andare nel senso dell'introduzione del voto elettronico quale modalità alternativa di voto. Agli inizi del 2019, come anticipato, prima il sistema messo a disposizione dalla Posta Svizzera – a causa di problemi legati alla sicurezza e attendibilità della raccolta del voto – poi quello del Cantone di Ginevra – per un eccessivo costo della sperimentazione – sono stati dismessi.

In Estonia, invece, il voto elettronico è presente. Si tratta dell'unico Paese europeo che consente di votare per tutti i livelli di governo (locale, nazionale ed europeo). Il sistema è accessibile, a seguito di identificazione mediante carta di identità elettronica o altra identità digitale certificata, esclusivamente da un computer[31]. Almeno tre, in particolare, le peculiarità del voto elettronico estone. In primo luogo, la votazione da remoto resta aperta dalle ore 9 del lunedì della settimana dedicata alle elezioni e si conclude alle ore 20 del sabato seguente, dunque la sera prima del giorno delle elezioni. In secondo luogo, è possibile per l'elettore ripetere il proprio voto: una volta espresso, in-

[27] Ancora una volta si fa riferimento, per la ricostruzione, ai contenuti del libro bianco *Per la partecipazione dei cittadini: come ridurre l'astensionismo e agevolare il voto*, liberamente consultabile e scaricabile attraverso il portale del Ministero per le riforme istituzionali e la semplificazione normativa (*riformeistituzionali.gov.it*). In particolare, le esperienze dei Paesi europei in relazione al voto elettronico (presidiato e non presidiato) sono rinvenibili alle pp. 102-115.

[28] La notizia è contenuta in un comunicato del 21 dicembre 2020, con il quale il Consiglio federale ha rilanciato la sperimentazione. Si legge nel documento che «I Cantoni dovranno poter di nuovo effettuare prove limitate di voto elettronico, impiegando sistemi completamente verificabili. È questo l'obiettivo che persegue il Consiglio federale dando seguito alla sua decisione del 18 dicembre sulla riorganizzazione della fase sperimentale. La sicurezza del voto elettronico sarà garantita da norme di sicurezza più precise, prescrizioni più severe in materia di trasparenza, una collaborazione più stretta con esperti indipendenti e da una verifica efficace effettuata su mandato della Confederazione. L'adeguamento delle basi giuridiche sarà sottoposto a consultazione nel corso del 2021» (*Voto elettronico: il Consiglio federale lancia la riorganizzazione della fase sperimentale*, in *seco.admin.ch*, 21 dicembre 2020).

[29] Secondo il comunicato del Consiglio federale del 27 giugno 2018, «Nella seduta del 27 giugno 2018 il Consiglio federale ha preso atto del rapporto finale "Gruppo di esperti sul voto elettronico", che gli è servito da base per condurre una discussione sul voto elettronico e definire le prossime tappe. Prevede di aprire una consultazione nel corso del secondo semestre 2018 per fare in modo che il voto elettronico diventi il terzo canale di voto ordinario» (*Voto elettronico quale canale di voto ordinario: il Consiglio federale prevede una consultazione per l'autunno 2018*, in *seco.admin.ch*, 27 giugno 2018). La consultazione, tuttavia, non è andata a buon fine e ha condotto alla rinuncia del 2019. Si è trattato di una consultazione promossa ai sensi della Legge federale sulla procedura di consultazione del 18 marzo 2005.

[30] Precisamente, la Legge federale sui diritti politici del 17 dicembre 1976, la cui abbreviazione in LDP è stata invero introdotta dal numero I della Legge federale del 26 settembre del 2014.

[31] Non è quindi possibile esprimere il proprio voto attraverso dispositivi diversi da un computer. Sono esclusi, ad esempio, di smartphone, nonostante essi siano fondamentali per la verifica successiva del voto espresso (si veda la nota successiva).

fatti, il voto può essere annullato e ripetuto ed il sistema terrà in considerazione esclusivamente l'ultima scelta effettuata. In terzo luogo, nel caso in cui l'elettore dovesse comunque recarsi fisicamente alle urne, il voto elettronico espresso non sarà preso in considerazione e prevarrà, invece, la scelta effettuata presso il seggio presidiato. Sotto il profilo della sicurezza e dell'attendibilità dell'operazione, il voto elettronico estone si caratterizza per un sistema di autenticazione attraverso un'applicazione ufficiale resa disponibile a livello istituzionale; da un complesso sistema di crittografia del voto elettronico e, da ultimo, ma non certo per importanza, dalla possibilità per l'elettore di verificare – scaricando "prima" dell'apertura della votazione un'apposita applicazione sul proprio smartphone – che il voto espresso sia stato acquisito dal server[32].

Le due esperienze ora richiamate e, invero, particolarmente l'esperienza estone, offrono molteplici occasioni di riflessione su quelli che possono essere considerati i punti di forza e le criticità del voto elettronico.

Anzitutto, nel caso in cui si dia la possibilità agli elettori di esprimere la propria scelta da remoto, quindi astrattamente in ogni luogo, è fondamentale definire prioritariamente quale sia il dispositivo idoneo all'utilizzo del programma specificamente preposto all'esercizio del voto elettronico. Qualsiasi dispositivo connesso ad Internet? Soltanto i computer, ritenuti maggiormente sicuri, come nel caso estone? Si tratta di una prima e fondamentale scelta. Anzi, bisognerebbe pure interrogarsi sulla possibilità di introdurre meccanismi elettronici di voto senza connessione Internet, i quali, se risultano sicuri perché non attaccabili dall'esterno[33], pongono comunque tutta una serie di problemi ad esempio legati alla comunicabilità in tempo reale dei dati (il caso tipico dell'elettore che dovesse presentarsi più volte alle urne in seggi differenti). Al pari, isolare il sistema dalla rete Internet coinvolge ulteriori aspetti, di cui si dirà tra poco, relativi alla controllabilità dei software utilizzati mediante audit da parte di soggetti terzi autorizzati.

In seconda battuta, non è indifferente la previsione di una maggiore o minore ampiezza della finestra temporale all'interno della quale è consentito votare. Un termine più lungo potrà sicuramente agevolare gli elettori, avendo essi a disposizione più tempo e quindi più occasioni per effettuare la propria scelta, mentre un termine breve, se riduce tali possibilità, consente però un più stringente controllo su eventuali tentativi di intrusione e la riduzione del rischio di "hackeraggio" del sistema di voto.

Ancora, se si considera il sistema di voto elettronico adottato dall'Estonia, non può passare in secondo piano l'opportunità concessa all'elettore di poter annullare il proprio voto e reiterarlo fintanto che le votazioni da remoto risultino aperte. Si tratta, a ben vedere, di una scelta che porta con sé pregi e difetti. Se da un lato, la possibilità di ripetere la votazione è posta a tutela della libertà, segretezza e personalità del voto, potendo essere stata inizialmente coartata la volontà dell'elettore da parte di terzi, dall'altro lato si lascia libero l'elettore di cambiare idea fino all'ultimo momento e ciò consente, quindi, maggiore spazio a tentativi di condizionamento che comunque po-

[32] Nel caso di specie, sulla schermata del computer utilizzato per la votazione compare un codice QR che, se scansionato con l'applicazione preventivamente scaricata sullo smartphone, consente in modo univoco di scaricare il proprio voto crittografato e di poterlo visualizzare previa conferma.

[33] Va da sé, infatti, che senza una connessione Internet il sistema risulterebbe "isolato" e accessibile unicamente se interrogato fisicamente da chi è presente nel luogo in cui il dispositivo è collocato.

trebbero provenire da terzi soggetti, una volta captata l'originaria volontà dell'elettore. Da ultimo, come anticipato, neppure può considerarsi un'opzione intercambiabile quella di perseguire il voto elettronico mantenendo la formalità del presidio elettorale, piuttosto che implementare un sistema di *home-voting*. Infatti, la possibilità per l'elettore di poter esprimere il proprio voto svincolato dalla sede fisica è senz'altro un enorme incentivo alla partecipazione, così come un potenziale strumento utile al superamento di molte criticità legate all'astensionismo volontario. Tuttavia, si deve tenere conto del cosiddetto *digital divide*, vale a dire del divario, soprattutto generazionale, tra chi possiede dispositivi connessi a Internet – e che quindi ha una, maggiore o minore, dimestichezza nel loro utilizzo – rispetto a coloro i quali non hanno accesso a Internet, non possiedono tali dispositivi o non sono in grado di accedervi autonomamente, senza l'ausilio di altri[34]. In questo senso, il sistema attuale di voto consente, al di là delle problematiche legate all'accesso fisico ai seggi, è piuttosto intuitivo e consente a tutti di poter esprimere il proprio voto (apponendo perlopiù una croce su simboli o scritte prestampati).

Questi rilievi conducono ad una medesima conclusione: esistono molti punti di forza derivanti dall'utilizzo del voto elettronico, ma numerose criticità e nodi da sciogliere in un senso piuttosto che in un altro. Assumere delle decisioni di base, in fase di implementazione e sperimentazione, è fondamentale anche al fine contenere i costi degli studi, costi che altrimenti rischierebbero di divenire sprechi di risorse pubbliche se non correttamente impiegati sulla base di attenti e seri studi preventivi di fattibilità.

Ecco, quindi, che se l'Italia o, come qualcuno auspica, l'Europa[35], dovesse riflettere in modo serio sul voto elettronico, non ci si potrebbe esimere dall'affrontare con rigore e precisione tutti i risvolti problematici, valorizzando il più possibile le potenzialità dello strumento, tenendo a mente gli scopi e senza vanificare l'utilizzo delle ingenti risorse economiche necessarie.

Inoltre, aspetti cruciali che determinano l'efficienza oppure no del sistema impiegato per l'espressione del voto elettronico restano la sicurezza del voto e i relativi controlli. Sotto il profilo della sicurezza, si è già fatto riferimento alla circostanza secondo la quale le tecnologie *Blockchain* e *Distributed Ledger* sembrano essere in grado, almeno stando alle rassicurazioni di chi possiede le necessarie conoscenze tecniche[36], di as-

[34] Al riguardo è stato osservato che «l'utilizzazione di sistemi di *e-voting* non deve influire sulla possibilità materiale di espressione della volontà elettorale, né tradursi nell'esclusione di gruppi, socialmente ed economicamente, svantaggiati. Il voto elettronico deve essere nella sua espressione semplice e intuitivo, alla portata di tutti, come lo è tracciare una croce su una scheda cartacea» (M. Rosini, *Il voto elettronico tra standard europei e principi costituzionali, prime riflessioni sulle difficoltà di implementazione dell'e-voting nell'ordinamento costituzionale italiano*, cit., 21).

[35] Sul punto, infatti, è stato messo in evidenza che «La proposta migliore sembra poter essere quella di intraprendere un percorso europeo a fasi, investendo su Istituzioni sempre più informatizzate, attuando esperimenti di voto elettronico presidiato – certamente meno esposto al rischio di violazione del principio di segretezza del voto rispetto all'*home vote* –, introducendo dispositivi digitali nei seggi elettorali, creando, dunque, le condizioni affinché l'elettore superi le remore psicologiche nei confronti dell'*e-voting* e maturi, quindi, una convinta fiducia» (cit. M. Schirripa, *Il voto elettronico nell'esperienza europea tra pregi e criticità*, cit., 248).

[36] Il che pone comunque il giurista in una posizione di secondo piano o quantomeno induce a riflettere sulla sempre crescente necessità di ampliare il proprio orizzonte conoscitivo, puntando su una maggiore dimensione interdisciplinare della conoscenza giuridica.

sicurare degli standard di sicurezza elevati. In effetti, anche in questo caso si rende necessaria una precisazione di carattere metodologico: come non è infallibile il sistema tradizionale di voto, non si può pretendere che sia infallibile neppure il sistema di voto elettronico. Ciò che conta, sotto questo aspetto, è che il meccanismo sia affidabile complessivamente, restituisca cioè un dato accettabile e il più possibile veritiero e sia in grado di meritare la fiducia generalizzata degli elettori. Al netto di ciò, le tecnologie sopramenzionate sembrano fugare il rischio di una "manomissione" del voto grazie alla decentralizzazione del sistema e all'assenza di intermediazione così come pare riescano ad assicurare l'immutabilità del registro e, quindi, una volta che il voto è raccolto, esso è custodito senza il rischio di una sua alterazione o rimozione. Allo stesso modo, non sarebbe possibile introdurre nuovi voti senza autenticazione e autorizzazione preventiva, la quale andrà concessa unicamente agli aventi diritto.
Sotto il profilo dei controlli, invece, è fondamentale che i software impiegati nonché tutti i passaggi e le chiavi di crittografia siano attendibili e in grado di superare il vaglio di audit affidati a soggetti esterni accreditati. Difatti, sempre grazie all'impiego delle tecnologie *Blockchain* e dei registri distribuiti – connotate, come ricordato, da tracciabilità dei trasferimenti, programmabilità degli stessi nonché da trasparenza e verificabilità – sembra essere possibile consentire a soggetti autorizzati di intervenire mediante la fornitura di chiavi *ad hoc* e poter in qualsiasi momento verificare il funzionamento del sistema elettronico.
L'esigenza non è affatto dissimile a quella che oggi è sottesa all'attuale sistema di voto, cambiano soltanto le modalità. Oggi è possibile contare sull'attendibilità e sicurezza delle operazioni di voto a partire dall'individuazione di presidenti di seggio, segretari e scrutatori sul cui operato l'ordinamento ripone la fiducia e prevedendo delle sanzioni, anche particolarmente severe, nel caso di commissione di illeciti. Nonostante ciò, come agiscono tali soggetti resta affidato a procedure che scontano un certo grado di fallibilità, il quale deve comunque restare all'interno di una soglia di tollerabilità.
Innegabile, infine, il vantaggio in termini di efficienza in fase preparatoria e di celerità nell'ottenimento del risultato elettorale. Con il voto elettronico, infatti, non vi sarebbe bisogno di stampare il materiale cartaceo e non vi sarebbero i tanti problemi che spesso si riscontrane nella consegna e restituzione dei materiali. Al pari, l'esito elettorale sarebbe pressoché immediato una volta chiuse le votazioni e si eviterebbero errori nel conteggio delle schede, eliminando il rischio che il materiale venga sottratto, occultato, danneggiato o smarrito.

5. Osservazioni conclusive

Giungere a delle conclusioni, a seguito dei molteplici spunti di riflessione che si è cercato di far emergere, non è semplice, anche tenuto conto del fatto che il ragionamento condotto si basa su dati e valutazioni astratti e rarissime esperienze concrete di Paesi esteri. Inoltre, come ricordato nelle battute introduttive, il tema del voto elettronico interseca ambiti della conoscenza estranei alle scienze giuridiche e soltanto una fruttuosa cooperazione e un mutuo scambio tra professionisti ed esperti delle

diverse discipline può portare a un risultato sodisfacente. In questo, è altresì evidente il "primato" detenuto dalle scienze informatiche, le quali sono chiamate a uno sforzo significativo, cioè quello di rendere fruibili a tutti gli altri interlocutori le conoscenze indispensabili per porre le basi di una proficua sperimentazione.

Onde concludere, si cercherà di riprendere le fila del discorso e porre alcuni punti fermi che possano essere utili nell'impostazione di un ragionamento in tema di studio del voto elettronico. Per fare ciò, si riprenderanno, per prima cosa, i caratteri costituzionali di "eguaglianza, segretezza, personalità e libertà" del voto[37], i quali – come si è detto – non possono che fungere da irrinunciabili parametri valutativi dell'efficienza e legittimità, sotto il profilo costituzionale, di qualsivoglia meccanismo elettorale, ivi compreso quello fondato sul voto elettronico.

Se, difatti, l'eventuale introduzione dell'*e-voting* in occasione delle elezioni politiche nazionali – ma, il discorso, naturalmente si presta ad essere esteso alle votazioni locali, europee e finanche referendarie o meramente consultive – dovesse violare i parametri espressi dall'art. 48 Cost., lo sforzo di implementare un meccanismo alternativo sarebbe reso del tutto vano, divenendo assai arduo superare i dubbi e i rischi di illegittimità.

Sotto il profilo "dell'eguaglianza", la valenza del voto – anche nel caso di voto elettronico – dovrebbe essere garantita poiché ogni singolo voto avrebbe lo stesso valore degli altri. Questo, naturalmente, una volta che il sistema sia predisposto in modo tale da consentire un singolo accesso all'elettore, di esprimere un solo voto e che siano chiarite le modalità di aggregazione e calcolo del risultato. Seguendo questi canoni, infatti, l'aspetto dell'eguaglianza non sembra essere tra i più critici, pur meritando particolare attenzione.

Sotto l'ulteriore profilo della "segretezza"[38], il voto elettronico basato sulla tecnologia *Blockchain* e *Distributed Ledger* dovrebbe essere messo al riparo da eventuali tentativi di intrusione e di associazione del dato acquisito all'identità del soggetto che ha espresso il voto[39]. In questo, a lungo ci si è soffermati sulle caratteristiche delle nuove tecniche informatiche a disposizione e, solo con un'attenta sperimentazione e messa a punto del meccanismo, sarà possibile avere un riscontro sull'effettiva sicurezza del sistema. In termini generali, tuttavia, con i complessi sistemi di crittografia e grazie alla replicazione dei dati sui vari registri distribuiti alla base della tecnologia *Blockchain*, la segretezza del voto pare poter essere assicurata.

---

[37] In dottrina si sono succedute molteplici interpretazioni dell'art. 48 Cost., ma in ogni caso vi è unanimità nel ritenere che «L'esigenza di assicurare appieno il carattere libero delle consultazioni elettorali rende quindi necessario verificare in concreto le modalità di esercizio del diritto di voto e l'effettività delle corrispondenti garanzie costituzionali […]. Il voto è effettivamente uguale e libero soltanto se ogni elettore può votare di persona ed in segreto e può ragionevolmente confidare in un comportamento equivalente di tutti gli altri elettori, che non devono essere oggetto di indebite pressioni. Nessun allontanamento da questi principi dovrebbe essere ammesso, nel pieno rispetto della sostanziale universalità del suffragio» (cit. A. Gratteri, *Il valore del voto. Nuove tecnologie e partecipazione elettorale*, cit., 2-3).

[38] E, nel caso di specie, riferita non tanto ai rapporti tra i privati quanto piuttosto rispetto alla possibilità che dall'esterno si riesca ad accedere ai dati acquisiti e, in modo diretto o indiretto, si riesca ad associare l'elettore alla scelta da esso compiuta.

[39] Si veda, tra gli altri, il recentissimo contributo di C. Chiariello, *Voto elettronico e principio di segretezza tra regola ed eccezioni*, in *Consulta Online*, 1, 2023, 59 ss.

Venendo alla "personalità", anzitutto il sistema di voto elettronico dovrà garantire un'univoca identificazione dell'elettore, verificando che vi sia corrispondenza tra chi esprime il voto mediante il dispositivo e l'effettivo titolare del diritto, in ciò ponendosi un concreto problema rispetto al parametro costituzionale. Si tratta, effettivamente, di uno snodo nel ragionamento attorno all'implementazione di modalità di voto non presidiato. Come secondo aspetto, anche nel caso di introduzione dell'*e-voting*, non si dovrebbe ammettere l'esercizio del diritto per delega e, tuttavia, la maggiore fruibilità della procedura – ferme le considerazioni già espresse sul voto presidiato e non presidiato – dovrebbe poter facilitare la diretta espressione del voto anche da parte di soggetti deboli o temporaneamente fragili.

Molto interessante, infine, il carattere della "libertà" del voto, il quale rischia effettivamente di non essere sufficientemente garantita dal voto elettronico non presidiato. Infatti, consentire l'accesso da qualsiasi dispositivo, in ogni luogo e all'interno di una finestra temporale molto ampia (di cui si è parlato), potrebbe esporre l'elettore a forme di condizionamento o coercizione della propria volontà. Un terzo soggetto, infatti, potrebbe indurre o costringere l'elettore a svolgere la votazione sotto il proprio diretto controllo o richiedendo di dare prova della scelta effettuata. Il problema in questione, però, sembra superabile grazie alla possibilità di concedere la facoltà di reiterare il proprio voto fino al momento della chiusura delle votazioni. In questo modo, l'elettore risulterebbe libero e il controllo da parte di terzi sarebbe possibile solo all'ultimo istante della procedura, con un impiego di risorse quasi inimmaginabile se si pensa al numero degli elettori (e se si vuole incidere significativamente sul risultato), oppur impedendo l'accesso al sistema una volta effettuata la scelta.

Esauriti questi aspetti, legati ai caratteri costituzionali del voto, invero è possibile valutare il sistema anche in base a ulteriori profili e parametri: l'accessibilità, la sicurezza, l'attendibilità, la verificabilità e, da ultimo, la sostenibilità economica.

Quanto all'accessibilità, è innegabile che l'introduzione del voto elettronico su larga scala consentirebbe in astratto un pieno coinvolgimento da parte degli aventi diritto poiché sarebbe sufficiente avere a disposizione un dispositivo connesso alla rete Internet (nel caso di voto non presidiato) ovvero recarsi presso qualsiasi seggio (a prescindere dal luogo di residenza) per esprimere la propria preferenza nel caso di voto presidiato. Le categorie che immediatamente gioverebbero dell'introduzione del voto elettronico sarebbero certamente quelle degli italiani all'estero e di coloro i quali temporaneamente risultano assenti dal luogo di residenza per motivi di studio, di lavoro o sanitari. Non è un caso, infatti, che il fondo italiano destinato alla sperimentazione del voto elettronico, di cui si è parlato, intervenga su queste due direttrici. Sul punto dell'uguaglianza, però, una particolare attenzione dovrà prestarsi alla problematica del diritto all'accesso ad Internet e della piena fruibilità da parte di tutti, soggetti fragili e deboli specialmente, dei dispositivi necessari all'espressione elettronica del voto nel caso di *home voting*; viceversa, nel caso di voto elettronico presidiato, si ripresentano per i soggetti più deboli le problematiche legate all'accessibilità delle urne, ma al contempo si potrebbero implementare, per queste categorie, modalità che consentano di dislocare il seggio, come oggi avviene per quelli appositamente istituiti presso le residenze di cura.

Quanto agli aspetti della sicurezza, dell'attendibilità e della verificabilità, si è avuto modo di soffermarsi nel corso del contributo sulle soluzioni di natura tecnica messe a disposizioni dalle tecnologie dei registri distribuiti e *Blockchain*. La sicurezza, in particolare, dovrebbe essere garantita dall'assenza di un controllo centralizzato della rete, dalla tracciabilità e programmabilità dei trasferimenti, dall'immutabilità dei registri, nonché da elevati standard informatici relativi ai sistemi di crittografia. La sicurezza degli applicativi di identificazione dell'elettore, la piattaforma per l'esercizio del voto, gli algoritmi necessari per l'acquisizione, l'aggregazione e l'elaborazione del risultato dovrà certamente essere garantita e verificata attentamente in fase di sperimentazione del voto elettronico. Il discorso può essere esteso all'attendibilità e verificabilità del sistema e alla controllabilità da parte di soggetti accreditati, attraverso lo strumento dell'audit. Su questi profili si è già detto e in fase conclusiva non può che ribadirsi la necessità di una verifica in concreto del sistema preposto, alla luce delle potenzialità che le nuove tecnologie racchiudono in loro stesse.

Infine, qualche battuta conclusiva e spunto di riflessione per il futuro dibattito sul tema oggetto del contributo.

A fronte di ingenti costi iniziali, che certamente si impongono per la sperimentazione e la messa a punto di un sistema di voto elettronico, appare piuttosto evidente il significato di un investimento a lungo termine. Se, difatti, la fase sperimentale dovesse produrre i frutti sperati, il voto elettronico consentirebbe la possibilità di svolgere delle votazioni, anche di natura meramente consultiva, con maggiore frequenza, con importanti conseguenze sotto il profilo dell'incentivazione della partecipazione nel contesto democratico e, indubbiamente, riducendo quantomeno l'astensionismo involontario. Al riguardo si è già avuto modo di ribadire che non appare del tutto illogico ipotizzare un effetto virtuoso di "trascinamento" secondo il quale al crescere della partecipazione di determinate categorie di soggetti possa comunque conseguire un progressivo coinvolgimento di altri, proprio sulla base di una tendenza crescente.

Il sistema di voto elettronico, una volta acquisiti e aggiornati i dati degli elettori, una volta reso fruibili e disponibile – magari in forma non presidiata – consentirebbe peraltro l'attivazione, con maggiore frequenza, di meccanismi di coinvolgimento del corpo elettorale, anche in relazione a decisioni circoscritte territorialmente.

Infatti, un ultimo aspetto che deve essere considerato nella predisposizione di un efficiente sistema elettronico di voto è la possibilità di andare verso una sostanziale deterritorializzazione nell'espressione della propria scelta. L'elettore, una volta legittimato e messo nelle condizioni di accedere alla piattaforma preposta, può votare in massima libertà a prescindere dal luogo in cui si trova e, sarà una visione utopistica, ma potrebbe persino essere chiamato a esprimersi rispetto a scelte che investono tanto le politiche locali, quanto quelle nazionali o sovranazionali ogniqualvolta lo si reputasse necessario.

Un'avvertenza, però: quale che sia la strada che il legislatore italiano (e magari europeo) intenderà perseguire, sarà fondamentale fissare degli obiettivi chiari e concreti, tenendo a mente le peculiarità dell'attuale sistema democratico italiano, l'importante funzione della rappresentanza politica nonché la necessità di ridurre l'astensionismo e incrementare la partecipazione e il coinvolgimento dell'elettore. Aspetti, tutti insieme

considerati, che pongono il sistema politico e istituzionale di fronte a una sfida tutt'altro che semplice da affrontare, ma che – forse proprio per questo – merita di essere accettata e portata avanti fino in fondo.

Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai *deepfakes**

Martina Cazzaniga

Abstract

Il contributo mira ad esaminare il "*deepfake*", un'innovativa tecnica basata sull'Intelligenza Artificiale che può essere utilizzata anche per veicolare disinformazione. Dopo alcune considerazioni preliminari di carattere costituzionale, si procede con un'analisi della posizione assunta dall'Unione europea in materia di *deepfake*, approfondendo quanto previsto all'interno dello *Strengthened Code of Practice on Disinformation* e della proposta di Regolamento sull'Intelligenza Artificiale. Infine, si cerca di riflettere sulle implicazioni sul piano costituzionale di una regolamentazione del *deepfake*.

The paper aims to examine the so-called "deepfake", an innovative technique based on Artificial Intelligence that can be used to convey disinformation. After some preliminary constitutional considerations, the paper focuses on the European Union approach to deepfakes by analyzing the Strengthened Code of Practice on Disinformation and the proposed Regulation on Artificial Intelligence. Finally, it presents a reflection about the constitutional implications of a deepfake regulation.

Sommario

1. Cosa sono i *deepfakes*: la manipolazione alla portata di tutti, anche a scopo disinformativo. – 2. Una riflessione circa la compatibilità costituzionale di un divieto assoluto di creazione e diffusione di *deepfakes*. – 3. Lo stato dell'arte della regolazione dei *deepfakes* nell'Unione europea: i primi passi tra *Strengthened Code of Practice on Disinformation* e la proposta di Regolamento sull'Intelligenza Artificiale. – 4. Quali prospettive per il *deepfake*?

Keywords

deepfake – disinformazione – falso - Intelligenza Artificiale - Unione europea

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1. Cosa sono i *deepfakes*: la manipolazione alla portata di tutti, anche a scopo disinformativo

Nel marzo 2023, Donald Trump ed Emmanuel Macron sono i protagonisti di alcune immagini condivise sul *web* che in pochissimo tempo sono state visualizzate da milioni di utenti[1]. I fatti che riportano destano evidente stupore: nella prima serie di scatti fotografici, l'ex Presidente degli Stati Uniti appare in balìa di alcuni poliziotti nell'atto di arrestarlo, mentre nella seconda il Presidente francese si trova in strada, tra manifestanti e forze dell'ordine, durante le proteste organizzate contro la riforma del sistema pensionistico[2]. Nonostante il realismo che le caratterizza, queste immagini sono false. Divulgare informazioni fuorvianti o menzognere non è mai stato così facile, dato che è possibile veicolare disinformazione ricorrendo a molteplici tecniche: è proprio su una di queste, il "*deepfake*", utilizzata per creare le immagini false di Trump e Macron[3], che si intende concentrare l'attenzione.

La divulgazione di tali contenuti manipolati ha iniziato a "smuovere le coscienze", aprendo una discussione circa l'utilizzo del *deepfake* con finalità disinformative. Tuttavia, prima di affrontare questo tema è necessario fare "un passo indietro" per comprendere almeno a grandi linee questa nuova tecnologia.

La parola inglese "*deepfake*" nasce nel 2017 e deriva dal *nickname* di un utente di Reddit conosciuto su questo sito *web* per la sua "abilità" di produrre video pornografici del tutto "originali": questi filmati venivano creati "ritagliando" i volti degli attori che veramente avevano recitato per la realizzazione del video e sostituendoli con i volti di vari personaggi – soprattutto donne – di fama mondiale. Il termine *deepfake*, il quale fino a qualche anno fa indicava semplicemente il *nickname* scelto da questo utente, è oggi utilizzato per riferirsi a questa particolare tecnica di intelligenza artificiale che permette di creare contenuti falsi e manipolati.

Chiunque provasse a digitare questa parola nella barra di ricerca di un qualsiasi *browser*, si accorgerebbe facilmente che sono sempre più numerose le notizie, provenienti da tutto il mondo, che riguardano il *deepfake*. Infatti, anche se in molti probabilmente non sono al corrente dell'esistenza di questa particolare tecnica, la sua diffusione è sempre più ampia: secondo i dati riportati da *Sensity*[4] nel dicembre 2020 i *deepfakes* presenti *online* erano già più di ottantacinquemila[5] e nell'ultimo biennio si è registrata una crescita esponenziale.

Ma che cosa è un *deepfake*? Nel dicembre 2020, il Garante per la Protezione dei Dati Personali ha fornito la seguente definizione della tecnologia del *deepfake*: «I *deepfake* sono foto, video e audio creati grazie a *software* di intelligenza artificiale (IA) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo

[1] E. Franceschini, *Trump in manette e Macron tra i manifestanti: quelle foto false dei leader viste da milioni di utenti*, in *La Repubblica*, 23 marzo 2023.

[2] *Ibidem*.

[3] *L'arresto di Trump simulato dall'intelligenza artificiale: è bufera sulla foto fake*, in *La Stampa*, 23 marzo 2023,

[4] Si tratta di una società con sede ad Amsterdam che si occupa anche di rilevare e tracciare i *deepfakes online*. Cfr. Europol Innovation Lab, *Facing reality? Law enforcement and the challenge of deepfakes*, 2022, 11.

[5] *How to Detect a Deepfake Online: Image Forensics and Analysis of Deepfake Videos*, in *Sensity*, 2021.

estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce»[6].

La parola è composta da due diversi concetti: difatti, si tratta di un neologismo[7] formato dall'unione del termine *fake*, che nella lingua inglese significa comunemente "falso", e *deep*, il quale fa invece riferimento ad una particolare tecnologia di intelligenza artificiale[8]. Infatti, con queste tecniche[9] ultra-innovative è possibile manipolare audio, immagini e video autentici[10], al fine di creare dei contenuti multimediali falsi e distorti[11]: bastano alcune immagini e una connessione Internet per "incollare" il viso di una persona al corpo di un'altra e farle dire e fare ciò che, nella realtà, non ha mai detto o fatto.

Il diffondersi di tecnologie in grado di imitare in modo così fedele la realtà non deve stupire: secondo quanto riportato dalla Commissione per le libertà civili, la giustizia e gli affari interni presso il Parlamento europeo, in futuro sarà possibile creare falsificazioni estremamente realistiche grazie a tecnologie sempre più sofisticate, delle quali ne

---

[6] Garante per la protezione dei dati personali, *Deepfake. Il falso che ti «ruba» la faccia e la privacy*, 28 dicembre 2020.

[7] *Ibidem*.

[8] Il termine "*deep*" a sua volta rimanda al concetto di *Deep Learning*. Il *Deep Learning*, la cui traduzione letterale è "apprendimento profondo", costituisce una sottocategoria del *Machine Learning* (letteralmente "apprendimento automatico") e indica quella branca dell'intelligenza artificiale che fa riferimento agli algoritmi ispirati alla struttura e alla funzione del cervello, chiamati "reti neurali artificiali". Cfr. N. Boldrini, *Deep Learning, cos'è l'apprendimento profondo, come funziona e quali sono i casi di applicazione*, in *Ai4business.it*, 26 settembre 2022.

[9] Le tecnologie di *deep learning* principalmente utilizzate per la creazione di *deepfakes* sono due. La prima è quella a cui i creatori di *deepfakes* ricorrono più spesso: essa prende il nome di *Generative Adversarial Networks* (meglio conosciuta con l'acronimo GAN), cioè il sistema con il quale è possibile realizzare le sostituzioni facciali. Il funzionamento della tecnologia GAN può essere riassunto nel modo che segue: un primo algoritmo è in grado di individuare i frammenti in cui i due soggetti (quello che prende il posto dell'originale e quello che viene sostituito con il volto altrui) hanno espressioni simili; a questo punto interviene un secondo algoritmo che svolge il successivo passaggio di posizionamento facciale, ovvero sovrappone concretamente i due volti in questione. Sostanzialmente, questi algoritmi di apprendimento automatico analizzano il materiale multimediale a disposizione e sono in grado di crearne uno altrettanto di qualità paragonabile. La seconda tecnologia prende invece il nome di *Autoencoders*: si tratta di un tipo di rete neurale che è in grado di estrarre informazioni sulle caratteristiche facciali apprese da immagini e utilizzarle per crearne delle altre con espressioni diverse. Cfr. F. Bertoni, *Deepfake, ovvero Manipola et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*, in *Ciberspazio e diritto*, 20, 62, 2019, 15-16; M. van Huijstee et al., *Tackling deepfakes in European policy*, European Parliamentary Research Service, 2021, 7-8.

[10] Oltre ai filmati, i quali costituiscono sicuramente la forma più nota di *deepfakes*, possono essere diffusi anche *deepfakes* realizzati con tecnologie di c.d. *voice cloning*, le quali permettono di ricreare la voce umana (in questo caso il *deepfake* consiste in una *clip* audio); in alcuni casi invece non viene realizzato un filmato ma una immagine statica, ovvero le c.d. *deepfake images* (ad esempio per creare immagini false da usare come foto del profilo dei *social network*); infine, sono anche da menzionare le tecnologie che permettono di realizzare delle sintesi testuali dato che può essere utile creare anche dei testi falsi in grado di imitare il modo pressoché unico che il *target* ha di parlare e scrivere, considerando anche il suo vocabolario. Su questo tema cfr. T. C. Helmus, *Artificial intelligence, deepfakes, and disinformation. A primer*, in *Rand.org*, 2022, 4-6; M. van Huijstee et al., *Tackling deepfakes in European policy,* cit., 7-15.

[11] Commissione europea, *Technology and democracy. Understanding the influence of online technologies on political behaviour and decision-making*, JRC Science for policy report, agosto 2020, 111.

è un esempio anche la realtà aumentata[12].

Il *deepfake* trova le sue origini proprio nel contesto della pornografia non consensuale[13]: spesso questi materiali sono utilizzati per compiere atti di *revenge porn* ai danni di soggetti fragili – principalmente di sesso femminile – o anche come mezzo di *sextortion*. Ancora oggi, oltre il 95% dei *deepfakes* presenti *online* è costituito proprio da video non consensuali a sfondo pornografico[14].

Sulla base di questi dati, non sorprende il fatto che i *deepfakes* vengano spesso presentati innanzitutto – o esclusivamente – come una nuova "minaccia" da limitare il più possibile. Ad alimentare i timori legati al *deepfake*, si aggiunge il fatto che questi contenuti multimediali manipolati possono essere altresì utilizzati per la commissione di reati (quali, ad esempio, estorsioni, diffamazioni, furti d'identità, frodi informatiche), e, inoltre, possono costituire una vera e propria "nuova frontiera" della disinformazione in grado di mettere a rischio l'assetto democratico[15].

Dunque, il tema del *deepfake* interseca anche quello della disinformazione *online*[16]: con l'avvento di Internet e dei *social network*, la proliferazione di notizie false è notevolmente aumentata, tanto che la disinformazione costituisce oggi un fenomeno dalle molteplici (e quasi infinite) sfaccettature, anche considerato che il suo impatto dipende da tecnologie interessate da celeri processi evolutivi[17], proprio come nel caso dei *deepfakes*. Infatti, sarebbe paradossale pensare che il modo di disinformare possa rimanere il medesimo per sempre: così come era diverso in passato[18] rispetto ad oggi, lo stesso varrà per il futuro.

Perché, dunque, concentrare l'attenzione sui *deepfakes* disinformativi? Quali effetti potrebbero conseguire dall'impiego di questa tecnologia come mezzo di disinformazione, ad esempio in ambito politico? I *deepfakes* raffiguranti Trump e Macron sono la dimostrazione di come questa tecnica possa essere impiegata per diffondere notizie

---

[12] J. Bayer et al., *Disinformazione e propaganda – impatto sul funzionamento dello Stato di diritto nell'Ue e nei suoi Stati membri*, Commissione LIBE presso il Parlamento europeo, marzo 2019, 6.

[13] F. Bertoni, *Deepfake, ovvero Manipola et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*, cit., 13.

[14] Europol Innovation Lab, *Facing reality? Law enforcement and the challenge of deepfakes*, 11.

[15] I rischi associati ai *deepfakes* sono stati approfonditi anche nello studio dell'*European Parliamentary Research Service* dedicato a questa tecnologia. Cfr. M. van Huijstee et al., *Tackling deepfakes in European policy*, 29-35.

[16] Quello della disinformazione è un tema di estrema attualità. Il concetto di *fake news* raggiunge il suo apice di "popolarità" nel 2016, anno della Brexit ma anche delle elezioni presidenziali negli Stati Uniti. Da quel momento, il fenomeno è oggetto di una costante attenzione, tanto che alcuni studiosi hanno dedicato al tema interessanti approfondimenti. Cfr., *ex multis*, C. Hassan-C. Pinelli, *Disinformazione e democrazia. Populismo, rete e regolazione*, Venezia, 2022; S. Sassi, *Disinformazione contro costituzionalismo*, Napoli, 2021; A. Nicita, *Il mercato delle verità,* Bologna, 2021.

[17] P. Cesarini, *The Digital Services Act: a silver bullet to fight disinformation?*, in *MediaLaws.eu*, 2021. L'autore del contributo spiega che «[…] *disinformation is a multi-faceted phenomenon whose impact depends on fast-evolving technologies, service-specific vulnerabilities and constant shifts in manipulative tactics*».

[18] La disinformazione non è sicuramente un fenomeno nato a seguito della rivoluzione digitale, dato che episodi di strategica disinformazione risalgono ad epoche anche molto antiche. Per alcuni esempi cfr. C. Valditara, *Fake news: regolamentazione e rimedi*, in *Diritto dell'informazione e dell'informatica*, 2, 2021, 257 ss; C. Pinelli, *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, in *Diritto pubblico*, 1, 2022, 173 ss.

non veritiere ma anche per finalità satiriche, specie nei casi, come quelli sopra descritti, ove il lettore medio comprende agevolmente che si tratta di un falso.

Ciò premesso, è evidente che *deepfakes* "politici", diffusi specie durante il periodo elettorale, possono costituire uno strumento di distorsione del dibattito pubblico e di manipolazione dei meccanismi di formazione del consenso[19].

La condivisione di un filmato compromettente (in realtà falso), probabilmente più convincente di una notizia solo letta[20], specie se divulgato a ridosso della fine della campagna elettorale, potrebbe incidere sull'esito delle elezioni, soprattutto qualora il soggetto leso non abbia, il tempo per smentirlo efficacemente[21].

Un ulteriore esempio concreto circa l'uso del *deepfake* come mezzo di disinformazione – anche se nel contesto bellico[22] – riguarda lo scontro militare che vede contrapposte la Federazione Russa e l'Ucraina a seguito dell'invasione di quest'ultima da parte del Cremlino avvenuta il 24 febbraio 2022. Il conflitto in corso è noto anche per essere a tutti gli effetti una guerra "mediatica", seppur non la prima nella storia[23], dato che i *social media* sono divenuti luogo privilegiato per la diffusione di informazioni riguardanti le ostilità. Inoltre, in questo caso la disinformazione deve essere considerata una componente essenziale dello scontro in atto: la diffusione di notizie false e fuorvianti è divenuta una vera e propria strategia per combattere il nemico, anche ricorrendo alla tecnica del *deepfake*.

Infatti, dopo circa un mese dall'inizio delle ostilità, divenne virale un video nel quale l'attuale Presidente ucraino Volodymyr Zelens'kyj dichiara a gran voce la resa del popolo ucraino e ordina ai propri soldati di deporre le armi[24]. Il video falso, realizzato appunto tramite la tecnica del *deepfake*, non venne creduto come vero[25], considerato anche il fatto che poco dopo Zelens'kyj smentì ufficialmente la notizia in prima persona[26]. E, in questo caso, i principali *social network*, i quali normalmente intervengono con

---

[19] M. Pawelec, *Deefakes and democracy (theory): how synthetic audio-visual media for disinformation and hate speech threaten core democratic functions*, in *Digital Society*, 1:19, 2022, 15.

[20] T. Dobber-N. Helberger-N. Metoui-D. Trilling-C. de Vreese, *Do (microtargeted) deepfakes have real effects on policital attitudes?*, in *International Journal of Press/Politics*, 26, 2021.

[21] B. Chesney-D. Citron, *Deep fakes: a looming challenge for privacy, democracy and national* security, in *California Law Review*, 107, 2019, 1178.

[22] Oltreché in ambito politico, la disinformazione può avere impatti non indifferenti sull'andamento degli scontri militari. Per un interessante approfondimento sulla disinformazione e sui *deepfakes* nei periodi bellici cfr. M. Mezzanotte, *Fake news, deepfake e sovranità digitale nei periodi bellici*, in *Federalismi.it*, 33, 2022.

[23] P. Suciu, *Is Russia's invasion of Ukraine the first social media war?*, in *Forbes*, 1 marzo 2022; K. Tiffany, *The myth of the first "Tik tok war"*, in *The Atlantic*, 10 marzo 2022.

[24] S. Burgess, *Ukraine war: deepfake video of Zelensky telling Ukrainians to "lay down arms" debunked*, in *SkyNews*, 17 marzo 2022.

[25] In realtà, soffermandosi più attentamente sul video, si può notare che lo stesso non fu realizzato con una precisione tale da renderlo particolarmente credibile: la testa di Zelens'kyj è troppo grande e sproporzionata rispetto al resto del corpo, quest'ultimo ha una risoluzione minore e appare più sgranato in rapporto al viso e, infine, la voce risulta essere più "profonda" rispetto all'originale. Cfr. J. Wakefield, *Deepfake presidents used in Russia-Ukraine war*, in *BBC News*, 18 marzo 2022.

[26] *Ibidem*. Secondo quanto riportato da BBC, il Presidente ucraino definì questa mossa una «*childish provocation*».

l'eliminazione del contenuto falso solo in casi circoscritti[27], procedettero prontamente alla rimozione del video[28].

Tra l'altro, poco tempo dopo non tardò ad arrivare il "contrattacco" ucraino: infatti, venne diffuso un video del Presidente russo Vladimir Putin mentre afferma di aver raggiunto un accordo di pace con lo Stato ucraino[29]. Anche in questo caso le principali piattaforme indicarono il contenuto come manipolato.

Tali esempi aiutano a comprendere le capacità di alterazione dell'opinione pubblica di questi video manipolati. Anche se finora i casi più eclatanti di *deepfakes* politici hanno coinvolto più che altro paesi stranieri[30], si tratta di una «forma di manipolazione dell'informazione [che] è destinata a verificarsi anche sul nostro territorio»[31] o che comunque non è escluso che possa verificarsi. Tra l'altro, Federica Bertoni sottolinea anche il fatto che quando in passato il legislatore italiano è intervenuto in ambito tecnologico, l'ha spesso fatto con normative d'urgenza e basate su una sorta di «onda emozionale»[32]: per questo motivo, ragionare in anticipo sul tema permette probabilmente di formulare delle valutazioni che sperano di essere più equilibrate.

2. Una riflessione circa la compatibilità costituzionale di un divieto assoluto di creazione e diffusione di *deepfakes*

In un futuro prossimo, la possibilità di creare *deepfakes* realistici potrebbe davvero divenire alla portata di tutti a causa del processo di «*democratization of deepfakes*»[33], in realtà già in atto da qualche anno: infatti, molti strumenti sono disponibili presso il pubblico per la realizzazione di *deepfakes*, tecnica ormai non più accessibile solo ad esperti informatici. Di conseguenza, non è irrealistico prospettare che chiunque potrebbe in tempi brevi divenire capace di creare questo tipo di contenuti, anche attraverso l'uso di

[27] Facendo riferimento ad esempio a Facebook, la piattaforma rimuove i contenuti falsi solo quando questi violano le proprie *policies*; in generale per le notizie false al posto della rimozione si prediligono misure più *soft* quali la riduzione della distribuzione del contenuto oppure l'informazione viene corredata di un contesto più completo per permettere agli utenti di decidere in modo autonomo quali contenuti ritenere affidabili. Tuttavia, uno dei casi che giustifica la rimozione è proprio quello dei contenuti multimediali manipolati nel caso in cui la manipolazione non sia evidente. Cfr. *facebook.com/combating-misinfo*; *transparency.fb.com/it-it/policies/community-standards/misinformation/*.

[28] *Meta e YouTube rimuovono video "deepfake" Zelensky*, in *Ansa.it*, 25 marzo 2022.

[29] *Il deepfake di Putin che dichiara la pace con l'Ucraina*, in *La Stampa*, 18 marzo 2022.

[30] Oltre ai *deepfakes* di Trump e Macron richiamati in apertura, ad oggi altri casi eclatanti hanno riguardo Stati come il Gabon, la Malesia e l'India. Cfr., rispettivamente, S. Cahlan, *How Misinformation Helped Spark an Attempted Coup in Gabon*, in *The Washington Post*, 13 febbraio 2020; H. Ajder-F. Cavalli-L. Cullen-G. Patrini, *The state of deepfakes: landscape, threats and impact*, Deeptrace lab, 2019, 10; C. Jee, *An Indian politiciain is using deepfake technology to win new voters*, in *MIT Technology Review*, 19 febbraio 2020.

[31] F. Bertoni, *Deepfake, ovvero Manipola et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*, cit., 23.

[32] *Ibidem*. Federica Bertoni si riferisce soprattutto agli interventi volti a disciplinare fenomeni come il *cyberbullismo* ma anche l'utilizzo di strumenti come i captatori informatici.

[33] P. Jurcys-J. Kalpokiene-A. Liaudanskas-E. Meskys, *Regulating deep fakes: legal ad ethical considerations*, in *Journal of Intellectual Property Law and Practice*, 15(1), 2020, 24.

semplici applicazioni[34]: ad esempio, le immagini *deepfake* di Trump in arresto non sono state create da un abile informatico ma da un giornalista[35].

Non è un caso che alcuni ordinamenti stanno intervenendo per disciplinare l'utilizzo di questa nuova tecnica, muovendo così i primi passi nella regolamentazione del settore. Proprio in quest'ottica è interessante svolgere alcune riflessioni preliminari di carattere costituzionale.

Il primo tema che si pone è sicuramente quello del falso. Ogni *deepfake*, infatti, è oggettivamente un falso: ciascun contenuto creato attraverso questa nuova tecnologia risulta essere intrinsecamente simulatore, dato che si tratta di video (nella maggior parte dei casi) le cui immagini e i cui suoni sono rielaborati e adattati ad un contesto differente rispetto a quello originario e autentico.

Dunque, i *deepfakes* devono essere ritenuti in sé illeciti perché falsi? L'interrogativo rimanda, nel contesto italiano, alla ben nota questione circa la protezione costituzionale del discorso falso e, sul punto, ritengo di poter aderire a quell'indirizzo secondo cui il c.d. subiettivamente falso, pur non rientrando nella tutela costituzionale della libertà di parola[36], non debba essere considerato illecito in quanto tale[37] ma solo qualora determini la lesione di beni giuridici di rilievo costituzionale[38].

Una tutela ancora più ampia del discorso falso è riconosciuta dalla giurisprudenza della Corte Suprema degli Stati Uniti d'America, la quale ha ricondotto all'ambito di applicazione del Primo Emendamento anche le affermazioni false[39], persino quando

[34] Le più famose sono *Reface*, *FaceApp*, *ZaoApp* e anche *Fakeyou*. Nei confronti di quest'ultima il Garante per la Protezione dei Dati Personali ha aperto una istruttoria nell'ottobre 2022. Cfr. *Deepfake: Garante avvia istruttoria su app che falsifica le voci*, 12 ottobre 2022.

[35] E. Franceschini, *Trump in manette e Macron tra i manifestanti: quelle foto false dei leader viste da milioni di utenti*, cit. L'Autore dell'articolo spiega: «Talvolta c'è qualche dettaglio rivelatore che si tratta di una finzione. In una delle immagini su Trump arrestato dalla polizia newyorchese, l'ex-presidente sembra avere tre gambe. In maniera simile, una precedente immagine diventata virale sul web, quella di un poliziotto francese che abbracciava una manifestante, l'indizio era la mano guantata dell'agente, che aveva sei dita. Ma in altre foto tutto appare veritiero e reale».

[36] Secondo Carlo Esposito, dato che la Costituzione italiana tutela le espressioni del «proprio» pensiero, non si dovrebbero considerare riconducibili all'art. 21 le informazioni che l'autore sa essere false. Cfr. C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, in *Rivista italiana per le scienze giuridiche*, IX, serie III anni 1957-1958, 84-85.

[37] Secondo la lezione di Paolo Barile, «neppure la diffusione di notizie false può essere considerata illecita in sé e per sé»: anche se si dovesse propendere per una non riconducibilità dell'affermazione subiettivamente falsa tra il novero delle manifestazioni del pensiero costituzionalmente tutelate, questo non comporterebbe automaticamente la sua illiceità. P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, 229; in questo senso anche A. Pace-M. Manetti, *Commentario della Costituzione. Rapporti civili. Art. 21. La libertà di manifestazione del proprio pensiero,* Bologna, 2006, 89; M. Bassini-G.E. Vigevani, *Primi appunti su fake news e dintorni*, in questa *Rivista*, 1, 2017, 21.

[38] Così, tra i molti, M. Bassini-G.E. Vigevani, *op. ult. cit.*, 15, dove si fa riferimento alla c.d. «teoria del bene giuridico costituzionalmente protetto». Sul tema, cfr. anche C. Melzi d'Eril, *Fake news e responsabilità: paradigmi classici e tendenze incriminatrici*, in questa *Rivista*, 1, 2017, 64.

[39] La sentenza cardine in tema di *false speech* nel contesto statunitense è sicuramente il caso, anche relativamente recente, *United States v. Alvarez*, nel quale la Corte si pronunciò sulla conformità del c.d. *Stolen Valor Act* rispetto al Primo Emendamento escludendone la legittimità costituzionale: l'atto non venne considerato conforme a Costituzione poiché puniva la dichiarazione falsa in quanto tale, senza dare nessuna importanza alla finalità del falso e all'eventuale perseguimento di un interesse o profitto. Cfr. *United States v. Alvarez*, 567 U.S. 709 (2012); O. Pollicino, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in questa *Rivista*, 1, 2018, 75.

l'autore ne sia consapevole.
In questa prospettiva si può ritenere che i *deepfakes* non possano essere vietati a priori ma possano essere ritenuti illeciti solo sulla base di un giudizio *ex post*, in caso di lesione di altri interessi di rilevanza costituzionale.
Tuttavia, proprio perché i *deepfakes* possono causare dei danni sia alla persona (anche dal punto di vista psicologico) che alla società (soprattutto se utilizzati come mezzo di disinformazione) è comunque opportuno interrogarsi sull'introduzione di specifici limiti in grado di circoscrivere la possibilità del concretizzarsi di questi rischi o, comunque, di fornire un adeguato rimedio qualora questi si verifichino.
Bisogna però precisare che ogni intervento regolatorio in materia necessita di tenere in considerazione il fatto che la tecnica del *deepfake* può avere – e concretamente ha, anche se questo aspetto fa molto meno "rumore" – delle applicazioni positive[40], ovviamente a patto che la stessa venga utilizzata nel modo corretto. Richiamare questo aspetto è importante ai fini di un ragionamento giuridico, perché nel momento in cui si prospetta una normativa in materia bisognerà fare attenzione a non ostacolare i risvolti positivi del *deepfake*[41], i quali non solo sono leciti ma altresì incoraggiabili.
Per citare alcuni casi di "usi benefici" del *deepfake*, si può richiamare il possibile impiego nel settore cinematografico[42], pubblicitario e della moda[43], nonché in quello educativo[44] e anche per la realizzazione di opere d'arte[45]: se utilizzato in questo senso, il *deepfake* può essere considerato a tutti gli effetti uno strumento per esprimere la propria creatività[46]. Inoltre, questa tecnologia può anche essere utilizzata per fare satira, parodia o comunque per creare altri tipi di contenuti ricompresi nell'alveo di protezione della libertà di manifestazione del pensiero[47]. Un ulteriore ambito fondamentale in cui l'utilizzo del *deepfake* può davvero agevolare molto la ricerca è quello medico[48].
Proprio perché sono molti i settori in cui il *deepfake* può essere utilizzato con finalità meritevoli, prospettare un divieto assoluto e indiscriminato di ricorrere a questa tecnologia pare sproporzionato oltreché insostenibile sul piano costituzionale, anche perché di per sé la manipolazione informatica non può essere considerata un'attività illecita in quanto tale[49]. Una proibizione totale non solo limiterebbe eccessivamente la libera manifestazione del pensiero ma, più in generale, la sperimentazione in molti ambiti, da

[40] Europol Innovation Lab, *Facing reality? Law enforcement and the challenge of deepfakes*, 5.

[41] M. Feeney, *Deepfake laws risk creating more problems than they solve*, rilasciato dal *Regulatory transparency project of the Federalist Society*, 1° marzo 2021, 5.

[42] B. Chesney-D. Citron, *Deep fakes: a looming challenge for privacy, democracy and national* security, cit., 1770.

[43] D. Yadav-S. Salmani, *Deepfake: A Survey on Facial Forgery Technique Using Generative Adversarial Network*, *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, Madurai, India, 2019, 854.

[44] B. Chesney-D. Citron, *Deep fakes,* cit., 1769.

[45] P. Jurcys-J. Kalpokiene-A. Liaudanskas-E. Meskys, *Regulating deep fakes: legal ad ethical considerations*, cit., 29.

[46] *Ibidem*.

[47] M. Feeney, *Deepfake laws risk creating more problems than they solve,* cit., 5.

[48] M. van Huijstee et al., *Tackling deepfakes in European policy*, cit., 28-29.

[49] B. Chesney-D. Citron, *Deep fakes,* cit., 1788.

quello artistico fino a quello medico[50].
Da queste considerazioni ne discende che l'operazione di bilanciamento tra i vari diritti e interessi sarà delicata e, di conseguenza, da svolgere con cautela.

3. Lo stato dell'arte della regolazione dei *deepfakes* nell'Unione europea: i primi passi tra *Strengthened Code of Practice on Disinformation* e la proposta di Regolamento sull'Intelligenza Artificiale

La diffusione di questa tecnica sta sollevando quesiti tanto giuridici quanto di tipo etico e sociale in molte aree del mondo: ci si domanda quale approccio debba assumere un ordinamento democratico, se sia necessario un intervento normativo e, inoltre, quale sarebbe eventualmente la disciplina più adatta[51].
L'ordinamento italiano non prevede alcuna disciplina in materia di *deepfakes*[52] – e, tra l'altro, nemmeno in materia di disinformazione più in generale[53] – probabilmente anche perché ad oggi casi clamorosi di *deepfakes* concernenti personaggi pubblici italiani non ve ne sono stati.
Se negli Stati Uniti il culmine di attenzione circa questo tema risale soprattutto al periodo che va dal 2018 fino circa al 2021[54], quando alcuni Stati hanno adottato normative sul tema, l'Unione europea, invece, sta muovendo i primi passi per affrontare i *deepfakes* proprio in questo ultimo triennio.

[50] Ivi, 1789.

[51] P. Jurcys-J. Kalpokiene-A. Liaudanskas-E. Meskys, *Regulating deep fakes: legal ad ethical considerations*, cit., 24.

[52] Se il legislatore italiano ancora non si è avvicinato a questo tema, lo ha fatto però in alcune occasioni il Garante per la Protezione dei Dati personali. Il primo caso riguarda la pubblicazione, a dicembre 2020, di un *vademecum* intitolato «*Deepfake*, il falso che ti "ruba" la faccia e la *privacy*», nel quale viene illustrata la tecnica, i principali rischi e alcune raccomandazioni su come proteggersi dai *deepfakes*. Il Garante per la Protezione dei Dati Personali torna però ad occuparsi di *deepfakes* più recentemente, a quasi due anni di distanza dalla pubblicazione del *vademecum*: infatti, con un comunicato stampa rilasciato a Roma il 12 ottobre 2022, annunciò l'avvio di una istruttoria nei confronti della società *The Storyteller Company*, proprietaria dell'applicazione *Fakeyou*, la quale permette di fare pronunciare *file* di testo a voci false – anche se realistiche – di numerosi personaggi famosi, compresi politici italiani. Cfr. Garante per la protezione dei dati personali, *Deepfake. Il falso che ti «ruba» la faccia e la privacy*, 28 dicembre 2020; *Deepfake: Garante avvia istruttoria su app che falsifica le voci*, 12 ottobre 2022.

[53] In passato si sono verificati due tentativi di intervento in materia, entrambi falliti nonché molto discutibili. Ci si riferisce a due proposte di legge, ambedue depositate nell'ultimo anno di lavori della XVII legislatura: la prima data 7 febbraio 2017 (Atto Senato n. 2688 comunicato alla Presidenza il 7 febbraio 2017 – *Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica* – disegno di legge Gambaro e altri), la seconda, invece, risale al dicembre dello stesso anno ed è stata presentata dai Senatori Zanda e Filippin (Atto Senato n. 3001 comunicato alla Presidenza il 14 dicembre 2017 – *Norme generali in materia di social network e per il contrasto della diffusione su internet di contenuti illeciti e delle fake news* – disegno di legge Zanda-Filippin).

[54] A livello statale, prevedono una legislazione positiva in materia la Virginia, il Texas, la California, lo Stato di Washington, quello di New York e, infine, il Massachusetts. A livello federale si nota un approccio più cauto: le poche disposizioni vigenti, infatti, delineano solo obblighi di studio e ricerca in materia. Ovviamente sono stati depositati anche disegni di legge più incisivi, i quali, tuttavia, hanno trovato un'accoglienza assai critica.

L'Unione europea non ha adottato una normativa specifica di contrasto ai *deepfakes*[55]. Tuttavia, questo non è sintomo di uno scarso interesse delle istituzioni europee rispetto al fenomeno: al contrario, soprattutto il Parlamento europeo da anni tiene alta l'attenzione rispetto ai potenziali effetti negativi dei *deepfakes*, ovviamente non trascurando i benefici che il ricorso a questa tecnica può comportare. Infatti, in numerose raccomandazioni e risoluzioni del Parlamento europeo è stato fatto riferimento a questa problematica anche in relazione al tema della propaganda politica e della disinformazione[56].

Alcune previsioni relative ai *deepfakes* sono contenute nello *Strengthened Code of Practice on Disinformation* del 2022[57]: questo codice costituisce un atto di *soft-law* che prevede una serie di impegni e misure specifiche che i firmatari[58] si impegnano a rispettare al fine di limitare la circolazione di notizie false *online*. Nella sezione denominata *Integrity of services*[59] i *deepfakes* vengono richiamati come caso di *manipulative behaviours* da contrastare.

Infatti, il *commitment* numero 14[60] stabilisce che, allo scopo di limitare i comportamenti non consentiti, i sottoscrittori debbano mettere a punto – oppure a rafforzare se le prevedevano già prima della firma del codice – *policies* di contrasto alla disinformazione veicolata attraverso l'utilizzo di queste tecnologie di recente sviluppo.

Il 9 febbraio 2023, ovvero sei mesi dopo la firma del "codice rafforzato", sono stati pubblicati dal neoistituito Centro per la trasparenza i primi *report*[61] presentati dai firmatari, i quali illustrano le misure adottate da ciascuno di loro per rispettare gli impegni assunti.

---

55 M. Liu-X. Zhang, *Deepfake technology and current legal status of it*, in *Proceedings of the 2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022)*, 2022, 1311.

56 L'Istituzione da sempre più interessata al tema è indubbiamente il Parlamento europeo, il quale ancora prima di dedicare a questa tecnologia un apposito studio del Servizio di Ricerca nel 2021 (più volte citato) ha richiamato i *deepfakes* in plurime raccomandazioni e risoluzioni. Cfr., *ex multis*, Raccomandazione del Parlamento europeo del 13 marzo 2019 al Consiglio e al vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza sul bilancio del seguito dato dal SEAE a due anni dalla relazione del PE sulla comunicazione strategica dell'UE per contrastare la propaganda nei suoi confronti da parte di terzi, P8_TA(2019)0187, 13 marzo 2019; Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale, P8_TA (2019)0081, 12 febbraio 2019, Nr. 178; Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale, PE653.860v02-00, 4 gennaio 2021.

57 Il testo completo dello *Strengthened Code of Practice on Disinformation* del 2022 è reperibile all'indirizzo https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

58 Nella versione del 2018 firmatari erano principalmente piattaforme digitali e motori di ricerca con un elevato numero di internauti (come Facebook, Twitter, Tik Tok, Google e Mozilla) insieme ad alcuni attori del settore pubblicitario. Oggi, invece, il *Code of practice on disinformation* conta trentaquattro firmatari, tra cui anche organizzazioni di *fact-cheking* indipendenti, associazioni di categoria e persino membri della società civile.

59 *Strengthened Code of Practice on Disinformation*, 15.

60 Ivi, 15-16.

61 Commissione europea, *I firmatari del codice di buone pratiche sulla disinformazione presentano le loro prime relazioni di riferimento presso il Centro per la trasparenza*, 9 febbraio 2023.

Quello che si può constatare da questi *report* è che in realtà le piattaforme non hanno modificato le normative interne in tema di contenuti multimediali manipolati dopo l'introduzione del codice. Ad esempio, Meta[62] richiama le proprie *policies*[63] e, nonostante non siano previste per il prossimo futuro modifiche sostanziali, dichiara di aver intrapreso uno studio insieme all'Università dello Stato del Michigan al fine di predisporre dei sistemi di *reverse engineering* in grado di rilevare i contenuti manipolati, *deepfakes* compresi[64].

Molto più scarne le parti dedicate alle misure di contrasto ai *deepfakes* all'interno dei *report* di Twitter e Google.

Per quanto riguarda Twitter[65], la disciplina in materia di contenuti multimediali manipolati viene completamente riportata nella relazione[66] quasi con un "*copy and paste*" della propria pagina *web* dedicata[67], senza effettivamente aggiungere altre indicazioni. Alle altre domande, ovvero quelle che interrogano il firmatario circa le misure che intende intraprendere in futuro, Twitter non fornisce alcuna risposta[68].

Google[69], invece, richiama in maniera più specifica le sole regole previste per YouTube, anche se in modo molto schematico ed approssimativo, rispondendo negativamente all'interrogativo circa la volontà di implementare gli sforzi in questo settore per il futuro[70].

La conclusione che si può trarre, per lo meno per quanto riguarda il tema dei *deepfakes*, è che l'adozione del codice non pare essere stata particolarmente influente e in grado di orientare in modo decisivo le scelte delle piattaforme in questo settore.

Anche la proposta di Regolamento sull'Intelligenza Artificiale tratta il tema dei *deepfakes* delineando una disciplina minimale ma comunque rilevante. Bisogna ricordare che i *deepfakes* vengono realizzati attraverso tecniche di Intelligenza Artificiale e proprio per questa ragione la proposta concernente questa materia non ne tralascia un riferimento[71]. La disciplina dei *deepfakes* è presentata in due "punti" diversi della proposta, ovvero nell'art. 52 e nell'Allegato III.

Esaminando l'art. 52, par. 3,[72] si può subito notare che nella proposta non si opta

---

62 *Code of Practice on Disinformation – Meta Baseline Report*, disponibile all'url *disinfocode.eu*.

63 Ivi, 55. Sia rispetto a Facebook che a Instagram, il *report* spiega che «*we remove videos under this policy if specific criteria are met: (1) the video has been edited or synthesized, beyond adjustments for clarity or quality, in ways that are not apparent to an average person, and would likely mislead an average person to believe a subject of the video said words that they did not say; and (2) the video is the product of artificial intelligence or machine learning*».

64 Ivi, 66.

65 *Code of Pratice on Disinformation – Report of Twitter for the period H2 2022*, disponibile in *disinfocode.eu*.

66 Ivi, 24-27.

67 Cfr. Twitter, *Norme sui contenuti multimediali artificiosi e manipolati*.

68 *Code of Pratice on Disinformation – Report of Twitter for the period H2 2022*, 27.

69 *Code of Practice on Disinformation – Report of Google for the period 1 July 2022 – 30 September 2022*, sempre disponibile in *disinfocode.eu*.

70 Ivi, 79-80.

71 M. van Huijstee et al., *Tackling deepfakes in European policy*, cit., 37.

72 Art. 52, par. 3: «Gli utenti di un sistema di IA che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ("*deep fake*") sono tenuti a rendere

per un generale divieto di creazione e divulgazione di *deepfakes*[73]: infatti, ciò che viene imposto a coloro che utilizzano i sistemi di Intelligenza Artificiale che generano *deepfakes* è "solamente" un generale obbligo di trasparenza, cioè di rendere palese che il contenuto multimediale è stato generato o manipolato attraverso queste tecnologie. Si tratta, dunque, di un dovere di tipo informativo. Il fatto che siano previsti unicamente degli obblighi di segnalazione è una conseguenza della non inclusione dei *deepfakes* nei sistemi a rischio inaccettabile o alto ma, invece, della loro riconducibilità in quelli a rischio limitato[74].

Rispetto alla scelta di prevedere un obbligo di questo tipo sorgono alcune perplessità, espresse anche dalla dottrina statunitense in relazione al c.d. *Deepfakes Accountability Act*[75], il quale delineava un dovere simile.

Innanzitutto, bisogna considerare che se il creatore del *deepfake* è disposto a far sapere che il contenuto che sta diffondendo è falso, ne discende che questo non sarà quasi sicuramente il tipo di utente di cui "preoccuparsi", dato che con tutta probabilità non avrà delle intenzioni nocive, proprio perché disposto a "smascherare" la manomissione[76]. Effettivamente, se chi realizza questi materiali alterati ha l'intenzione di recare danni ad un soggetto preciso o alla società, conoscerà sicuramente anche delle tecniche per non svelare la propria identità[77], optando per divulgare il contenuto tramite un *account* falso o un *bot*. Di conseguenza, non sarebbe poi facilmente identificabile un soggetto in capo a cui ricondurre la responsabilità. In definitiva, una previsione di questo tipo non sembra essere idonea a costituire un deterrente tale da demotivare gli autori di *deepfakes* nocivi[78].

L'art. 52, par. 3, delinea anche delle eccezioni a questo dovere di "etichettamento" del *deepfake* come tale, le quali corrispondono ai casi di esercizio della libertà di manifestazione del pensiero ma non solo, dato che viene fatto riferimento anche alla libertà delle arti e delle scienze e all'uso autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati. La previsione di deroghe al generale obbligo appena analizzato è opportuna proprio per evitare di gravare eccessivamente i creatori di *deepfakes* legittimi.

Alla posizione che l'Unione europea intenderebbe assumere in tema di *deepfake* non sono state risparmiate critiche da parte della dottrina, dato che alcuni commentatori

noto che il contenuto è stato generato o manipolato artificialmente. Tuttavia, il primo comma non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati o se è necessario per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantito dalla Carta dei diritti fondamentali dell'UE, e fatte salve le tutele adeguate per i diritti e le libertà dei terzi».

[73] A. Del Ninno, *La proposta di Regolamento UE sull'Intelligenza Artificiale: i profili operativi del nuovo quadro normativo europeo – Parte Quarta*, in *Diritto e Giustizia*, 2021, 12.

[74] Camera dei deputati Ufficio Rapporti con l'Unione europea, *Legge sull'intelligenza artificiale*, dossier n. 57, 12 novembre 2021, 10.

[75] Questo disegno di legge venne presentato dalla componente della *House of Representatives* degli Stati Uniti Yvette Clarke nel 2021 ma risulta ancora al solo stato di "*introduced*". U. S. Congress H.R. 2395, *Deepfakes Accountability Act*, 2021.

[76] D. Coldewey, *Deepfakes Accountability Act wuold impose unenforceable rules – but it's a start*, in *TechCrunch*, 13 giugno 2019.

[77] M. van Huijstee et al., *Tackling deepfakes in European policy*, cit., 46.

[78] M. Feeney, *Deepfake laws risk creating more problems than they solve*, cit., 9.

hanno palesato più di un dubbio circa queste previsioni[79]. In generale, soprattutto chi vede i *deepfakes* più come una minaccia che come un beneficio, lamenta l'eccessiva "timidezza" di questa normativa[80].

Tra l'altro, la proposta nella sua originaria formulazione lasciava del tutto irrisolte alcune questioni, come quelle relative a come dovesse avvenire la *disclosure* delle informazioni richieste. Effettivamente, il testo dell'art. 52, par. 3, così come proposto non presentava alcuna indicazione circa la messa in pratica di questo dovere di trasparenza, con la conseguenza che la sua applicazione avrebbe potuto risultare concretamente complicata: l'assenza di una disciplina sul punto non permetteva di comprendere se fosse sufficiente una indicazione generale oppure se ne fosse necessaria una di carattere più specifico[81].

Alcuni profili critici vengono sottolineati anche nello studio dedicato al tema dei *deepfakes* condotto dallo *European Parliamentary Research Service*, nel quale vengono forniti alcuni "suggerimenti" su come migliorare la prospettata disciplina in materia[82].

Oltre che nell'art. 52, par. 3, i *deepfakes* sono richiamati anche all'interno dell'Allegato III[83] così come originariamente proposto, il quale elenca i sistemi ad alto rischio: al punto n. 6 lettera c) sono previsti anche «i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per individuare i "*deep fake*" di cui all'articolo 52, paragrafo 3». La ragione di questa scelta iniziale risiede nel fatto che si riteneva che i *detection softwares* potessero costituire un rischio per i diritti e le libertà dei singoli individui, decidendo di permetterne l'utilizzo solo nel rispetto di rigorose garanzie[84].

Tuttavia, le previsioni circa i *deepfakes* hanno subìto modifiche con gli emendamenti presentati dal Consiglio[85]: come già osservato, sono due le situazioni nelle quali il *deepfake* viene richiamato nella proposta ed entrambe sono state oggetto di emendamenti. Questo fa riflettere circa la rilevanza del tema, soprattutto se si considera che probabilmente le tecniche per realizzare i *deepfakes* saranno sempre più affinate negli anni a venire e che si tratta di un settore molto controverso.

---

79 D. Messina, *La proposta di regolamento europeo in materia di Intelligenza Artificiale: verso una "discutibile" tutela individuale di tipo consumer-centric nella società dominata dal "pensiero artificiale"*, in questa *Rivista*, 2, 2022, 220. Ad esempio, l'Autore sottolinea che i sistemi con i quali si realizzano i *deepfakes* non sembrano da considerare a rischio elevato, dato che assenti nell'elenco dell'Allegato III. Tuttavia, il par. 4 dell'art. 52 precisa che i paragrafi precedenti «lasciano impregiudicati i requisiti e gli obblighi di cui al Titolo III del presente regolamento», il quale riguarda i sistemi ad alto rischio.

80 A. Del Ninno, *La proposta di Regolamento UE sull'Intelligenza Artificiale: i profili operativi del nuovo quadro normativo europeo – Parte Quarta*, cit., 12.

81 B. van der Sloot-Y. Wagensveld, *Deepfakes: regulatory challenges for synthetic society*, in *Computer Law and Security Review*, 46, 2022, 7.

82 M. van Huijstee et al., *Tackling deepfakes in European policy*, cit., 59. Tra i suggerimenti forniti si possono richiamare i seguenti: chiarire più precisamente quali pratiche sono da considerare proibite, proposta avanzata anche dall'Europol (cfr. Europol Innovation Lab, *Facing reality? Law enforcement and the challenge of deepfakes*, cit., 22); prevedere obblighi non solo in capo ai creatori di *deepfakes* ma anche ai fornitori di queste tecnologie; classificare la tecnologia nella categoria dell'alto rischio.

83 Allegati della Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, SEC(2021) 167 final - SWD(2021) 84 final - SWD(2021) 85 final, 21 aprile 2021.

84 Europol Innovation Lab, *Facing reality? Law enforcement and the challenge of deepfakes*, cit., 21.

85 Per visionare il nuovo testo così come proposto dal Consiglio cfr. *data.consilium.europa.eu*.

Da un lato, è stato variato l'elenco dei sistemi di Intelligenza Artificiale ad alto rischio previsto dall'Allegato III: infatti, i sistemi impiegati dalle autorità per individuare i *deepfakes* sono stati rimossi da questo novero, scomparendo così ogni riferimento a questa tecnica tra i sistemi *high risk*, dato che viene completamente eliminata la lettera c) dal punto n. 6.
D'altro lato, anche l'art. 52 della proposta di regolamento ha subìto cambiamenti[86]. La prima parte del par. 3 rimane immutata, mentre sulla seconda il Consiglio è intervenuto proponendo una modifica dei casi in cui il creatore di *deepfakes* è sollevato dall'obbligo di etichettamento: viene rimosso il riferimento ai *deepfakes* che rientrano nell'esercizio della libertà della scienza, mentre sussiste l'esonero nel caso di opere e programmi manifestatamente creativi, satirici, artistici o fittizi e quando l'uso è autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati.
Oltre a intervenire sul novero delle eccezioni, viene anche aggiunto un par. 3-*bis* all'art. 52, il quale prevede che «le informazioni di cui ai paragrafi da 1 a 3 sono fornite alle persone fisiche in maniera chiara e distinguibile al più tardi al momento della prima interazione o esposizione».
La disposizione appena riportata aggiunge qualche informazione circa i tempi e le modalità con i quali dovrebbe avvenire la rivelazione della manipolazione. Tuttavia, le indicazioni fornite risultano eccessivamente vaghe, dato che è solo richiesto che le informazioni siano chiare, distinguibili e fornite al massimo entro il momento del primo "contatto" con il contenuto. Questa aggiunta non risolve il problema di come debba essere concretamente adempiuto l'obbligo informativo di cui al par. 3.
Questo è lo stato dell'arte della disciplina europea in materia di *deepfakes* nei primi mesi del 2023. Si tratta di un approccio prudente: da un lato, la scelta di evitare obblighi troppo stringenti o divieti è apprezzabile perché in questo modo si scongiura il rischio di un *chilling effect* nei confronti del ricorso a questa tecnologia anche a scopi benefici; dall'altro, tuttavia, l'incognita concerne il comprendere se un dovere di trasparenza così configurato sarà effettivamente rispettato oppure, al contrario, spesso disatteso.
Le riflessioni tratteggiate sono formulate pur sempre sulla base di un quadro giuridico ancora incerto e rispetto ad un settore ancora in divenire: proprio per questo motivo sarà utile monitorare il lavoro delle istituzioni europee nei prossimi mesi in modo da comprendere quale sarà la posizione definitiva sul punto, se e quando l'atto entrerà in vigore.

4. Quali prospettive per il *deepfake*?

Lo stato dell'arte, sotto il profilo sia tecnologico che giuridico, non consente certo di

[86] Proposta di nuovo testo per l'art. 52, par. 3: «Gli utenti di un sistema di IA che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ("*deep fake*") sono tenuti a rendere noto che il contenuto è stato generato o manipolato artificialmente. Tuttavia, il primo comma non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati o se il contenuto fa parte di un'opera o di un programma manifestamente creativo, satirico, artistico o fittizio, fatte salve le tutele adeguate per i diritti e le libertà dei terzi».

prospettare soluzioni a questioni complesse e in divenire. Sia concessa, tuttavia, una riflessione finale sulle implicazioni sul piano costituzionale di una regolamentazione del fenomeno nonché sui confini che i principi in materia di libertà di espressione pongono al legislatore, sia esso europeo o nazionale.

Innanzitutto, come si è già cercato di dimostrare, la previsione di un divieto generale di diffusione dei *deepfakes* sembra porsi in palese contrasto con il diritto a manifestare il pensiero. Tuttavia, ciò non esclude l'ipotesi di interventi "chirurgici" che mirino a contrastare la distorsione del dibattito pubblico, senza comunque precludere lo sviluppo di questa tecnologia.

Un'altra via di intervento, che pone più di una perplessità, è quella che prevede la creazione di nuove fattispecie di reato per perseguire i creatori di *deepfakes* disinformativi[87]. Questa strada è stata percorsa, ad esempio, dallo Stato del Texas, la cui legge in materia criminalizza la creazione e la diffusione di *deepfakes videos* aventi l'intento di nuocere un candidato politico o di influenzare l'esito delle elezioni[88]. Questa scelta fu criticata da alcuni studiosi, tra cui Orin Samuel Kerr, che mostrarono un notevole scetticismo nei confronti della possibilità di perseguire queste condotte ricorrendo allo strumento penale[89].

In generale, la prospettiva di un intervento normativo limitativo dell'uso di questa tecnologia costituisce indubbiamente un terreno scivoloso, proprio come nel contesto della regolamentazione della disinformazione in generale. Rispetto alle altre modalità di divulgazione di notizie false, probabilmente i *deepfakes* possono giustificare un intervento maggiormente stringente, soprattutto se si accoglie la teoria per cui questi contenuti manipolati sono effettivamente maggiormente persuasivi e in grado di condizionare in modo più incisivo l'opinione pubblica[90]. Sono esempio di questa linea di approccio al *deepfake* le *policies* dei principali *social network*: con riguardo ai contenuti disinformativi in generale tendenzialmente le piattaforme preferiscono evitare di fare ricorso a misure "drastiche" e fortemente limitative come la rimozione del contenuto, mentre sembrano più inclini a ricorrere alla cancellazione in relazione ai contenuti manipolati con la tecnica in esame.

Come è stato accennato, i *deepfakes* disinformativi sono maggiormente percepiti come una potenziale minaccia durante il periodo delle elezioni. Proprio in quest'ottica, una opzione regolatoria che alcuni ordinamenti – come la California e il Texas nel contesto statunitense – prediligono è quella di vietare i *deepfakes* "politici" solo durante il periodo elettorale[91], proprio perché questo rappresenta uno dei momenti fondamentali della

[87] La valutazione di non opportunità di un ricorso allo strumento penale riguarda i *deepfakes* disinformativi. Invece, nel caso di quelli a contenuto sessualmente esplicito non consensuali oppure che permettono la commissione di illeciti, il ricorso allo strumento penale non va escluso a priori anche alla luce dei diversi beni giuridici coinvolti.

[88] Texas Senate Bill, *Relating to the creation of a criminal offense for fabricating a deceptive video with intente to influence the outcome of an election*, in *LegiScan.com*, 2019-2020.

[89] O. S. Kerr, *Should Congress pass a "deep fakes" law?*, in *The Volokh Conspiracy*, 31 gennaio 2019.

[90] Cfr. T. Dobber-N. Helberger-N. Metoui-D. Trilling-C. de Vreese, *Do (microtargeted) deepfakes have real effects on policital attitudes?*, cit.

[91] California Assembly Bill-730: *Elections: deceptive audio or visual media*, in *California Legislative Information*, 2019-2020; Texas Senate Bill, *Relating to the creation of a criminal offense for fabricating a deceptive video with*

"vita" democratica, durante il quale molto spesso si verifica una maggiore circolazione di notizie false. Questa scelta, ad esempio, è stata adottata anche in Francia in materia di disinformazione in generale: difatti, la legislazione circoscrive la durata degli obblighi più stringenti in capo alle piattaforme proprio al periodo elettorale[92].

Un'altra tematica centrale in relazione alle possibili misure di contrasto alla disinformazione – e anche a quella veicolata attraverso i *deepfakes* – è quella della trasparenza[93]. Effettivamente, quello contenuto nell'art. 52, par. 3, della proposta di Regolamento sull'Intelligenza Artificiale è un obbligo di trasparenza, poiché impone al creatore del *deepfake* di rivelare che non si tratta di un contenuto autentico. Come già sottolineato, il problema di questa prescrizione riguarda la sua concreta effettività, dato che è molto probabile che venga disattesa per le ragioni già esposte.

Il ragionamento si sposta allora sulla trasparenza della fonte, dato che è ragionevole pensare che i *deepfakes* siano parte di campagne sistematiche di disinformazione e siano diffusi da *account* appartenenti a utenti la cui vera identità rimane sconosciuta. Il tema dell'anonimato in rete è complesso: da un lato, assicurarlo permette a tutti di poter esprimere in modo libero pensieri e opinioni senza il timore spesso legato al doversi esporre personalmente[94]; tuttavia, l'anonimato contribuisce ad un vero processo di deresponsabilizzazione dell'autore dei contenuti[95], il quale, "nascosto" dietro un profilo adespoto, si sente legittimato a veicolare contenuti manipolati e distorsivi.

Per non giungere a negare completamente l'anonimato, in dottrina emergono alcune posizioni propense ad elaborare delle soluzioni di compromesso: ad esempio, una possibilità potrebbe essere quella di permettere agli utenti di partecipare al dibattito pubblico *online* tramite uno pseudonimo, facendo però conoscere la propria identità almeno al gestore della piattaforma e, dunque, fornendo i propri dati personali autentici in sede di iscrizione[96].

Tuttavia, al di là della discussione su come porsi nei confronti dell'anonimato, si potrebbe richiedere alle piattaforme di fornire più informazioni circa la provenienza dei

intente to influence the outcome of an election, in *LegiScan.com*, 2019-2020.

92 Legge organica n. 1201 del 22 dicembre 2018 relativa alla lotta contro la manipolazione dell'informazione; Legge ordinaria n. 1202 del 22 dicembre 2018 relativa alla lotta contro la manipolazione dell'informazione.

93 Su questo valore cardine si basano sia il *Digital Services Act* che anche il Codice rafforzato di buone pratiche sulla disinformazione.

94 M. Lamanuzzi, *Il problema della disinformazione in rete: i limiti del diritto penale e le potenzialità del nuovo Codice rafforzato di buone pratiche dell'UE*, in *medialaws.eu*, 2022.

95 In questo senso si esprime da tempo Giulio Enea Vigevani, il quale in un recente contributo afferma che «il principio di trasparenza sulla provenienza dei contenuti – ricavabile dall'interpretazione sistematica dell'art. 21 Cost., commi 3 e 5, che conduce a valorizzare i principi di responsabilità personale di chi diffonde informazioni o idee ed esclude le manifestazioni del pensiero in forma anonima dall'alveo della tutela costituzionale – consentirebbe al legislatore (nazionale o europeo) di imporre alle piattaforme di accertare e indicare se un contenuto proviene da una persona fisica, una persona giuridica, un organo governativo, un programma automatico, di segnalare da quale paese deriva, etc. Si tratterebbe di uno strumento in grado di frenare quell'inquinamento dello spazio dell'informazione, specie da parte di potenze straniere, che finisce per rendere l'esercizio di un "controllo sugli altri poteri", missione fondamentale dell'attività informativa, subalterno a logiche del tutto diverse». Cfr. G.E. Vigevani, *Piattaforme digitali private, potere pubblico e libertà di espressione*, in *Rivista di Diritto Costituzionale*, 1, 2023, 59.

96 M. Lamanuzzi, *Il problema della disinformazione in rete,* cit.

contenuti[97]: un'idea potrebbe essere quella di investire su algoritmi in grado di stabilire quando un contenuto viene, ad esempio, condiviso da un *bot* e non da un utente "umano". In questo caso, anche qualora il contenuto multimediale fosse un *deepfake*, non sarebbe di per sé vietata completamente la pubblicazione – e non sarebbe nemmeno vietato l'anonimato – ma una etichetta avviserebbe circa quale tipo di *account* l'ha condiviso. Ad esempio, se l'utente sapesse che il contenuto che sta visualizzando è stato condiviso da un *bot*[98], sarebbe probabilmente propenso ad una sua valutazione più critica e prudente.

Dal punto di vista delle soluzioni non propriamente giuridiche, è importante richiamare lo spirito critico che ogni utente dovrebbe "mettere in campo" quando si imbatte in contenuti pubblicati sul *web*: in questo senso appare particolarmente persuasivo Guido Scorza, quando, commentando il fenomeno dei *deepfakes*, sostiene che in vista del progressivo aumento della diffusione di queste tecnologie è necessario iniziare a «sviluppare quantità industriali di spirito critico»[99], che deve essere "allenato" già in età scolastica.

E in questa prospettiva anche educativa, sembrano nel complesso condivisibili le raccomandazioni formulate dagli studiosi della *Alliance of Democracies*[100], i quali si sono occupati proprio del rapporto tra *deepfake* e disinformazione[101].

Dopo una approfondita analisi di questa tematica, vengono appunto formulate alcune *recommendations* finali, le quali possono essere così riassunte[102]: intensificare la collaborazione tra Stati e piattaforme in modo da evitare che queste, soggetti privati, possano decidere in autonomia come bilanciare i diritti rilevanti in questi settori; considerare la trasparenza l'elemento "chiave" nella regolazione della disinformazione *online*; definire coerentemente i casi di rimozione dei contenuti manipolati, in modo da evitare il rischio di *over-removal*; infine, accompagnare la legislazione e le restrizioni da parte delle piattaforme con l'educazione mediatica.

In definitiva, il termine "*deepfake*" ha assunto una connotazione intrinsecamente negativa proprio perché i rischi tendono ad oscurare i benefici che possono derivare dal ricorso a questa tecnica[103]. Questo approccio ai *deepfakes*, conseguenza di una spesso diffusa inquietudine nei confronti di ciò che è nuovo o ignoto, rischia di intaccare il

---

97 In questo senso cfr. N. Diakopoulos-D. G. Johnson, *Anticipating and addressing the ethical implications of deepfakes in the context of elections*, 2020, disponibile in *ssrn.com*.

98 Ad esempio, dal 1° luglio 2019 nello Stato della California vige una legge che impone il dovere per i *social network* di etichettare i *bots* in modo da renderli riconoscibili agli utenti. Cfr. California State Senate, Bill no. 1001, chapter 892, 2018 (c.d. *Bolstering online transparency act*).

99 *La app Fakeyou, i falsificatori si innovano: tempi duri per la verità – Intervento di Guido Scorza*, 20 ottobre 2022.

100 La *Alliance of Democracies Foundation* è una organizzazione no profit fondata nel 2017 dall'ex Primo Ministro danese nonché ex Segretario Generale NATO Anders Fogh Rasmussen. L'organizzazione si dedica al progresso della democrazia e del libero mercato in tutto il mondo. Secondo quanto riportato dalla stessa organizzazione, la stessa mira a divenire «*the world's leading megaphone for the cause of democracy*».

101 C. Waldemarsson, *Disinformation, deepfakes and democracy. The european response to election interference in the digital age*, Alliance of Democracies, 2020.

102 Ivi, 21-22.

103 M. van Huijstee et al., *Tackling deepfakes in European policy*, cit., 49.

«colore di per sé neutro che [lo] strumento ha quando vede la luce»[104], creando così un pregiudizio nei confronti della tecnica stessa che potrebbe influenzare una eventuale regolamentazione. Proprio per questo motivo, si è cercato di tracciare le linee generali di un approccio giuridico ai *deepfakes* che sia rispettoso dei diritti fondamentali: una regolamentazione specifica in materia di *deepfake* può essere benvenuta, purché sia ragionata, frutto di un corretto bilanciamento tra diritti e in grado di cogliere la complessità del fenomeno.

Non resta ora che attendere gli sviluppi futuri in questo settore, i quali riguarderanno tanto l'evoluzione della tecnologia quanto quella della normativa.

[104] F. Bertoni, *Deepfake, ovvero Manipola et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*, cit., 13.

Trasformazione digitale del settore finanziario e *Open Finance*: quali prospettive per un credito "sostenibile"? Prime riflessioni*

Maria-Teresa Paracampo

Abstract

La prossima sfida dell'innovazione digitale va sotto il nome di *Open Finance*. Concepita nell'ambito della Strategia europea per la Finanza Digitale, la nuova rivoluzione nel settore dei dati rappresenta l'evoluzione dell'Open Banking esteso a tutto il settore finanziario. Mira a valorizzare i dati del cliente attraverso una maggiore condivisione e riutilizzo degli stessi in funzione di prodotti e servizi finanziari personalizzati per i consumatori e per le PMI.
I diversi steps per la trasformazione digitale del settore finanziario devono tener conto anche delle spinte provenienti dal parallelo processo di transizione verso l'economia sostenibile. Entrambi i percorsi stanno a cuore della Commissione europea in vista di un'Europa digitale e sostenibile.
Alla luce di queste premesse, il contributo mira ad offrire alcune coordinate normative su possibili sviluppi derivanti dalla sinergia tra i percorsi dell'innovazione digitale e della sostenibilità. In particolare, si propone di fornire prime riflessioni sui mutui green e sulle opportunità di accesso al credito di consumatori e PMI nell'ambito di un ecosistema finanziario aperto.

Open Finance is the next digital innovation challenge. Conceived as part of the European Digital Finance Strategy, the new data revolution represents the evolution of Open Banking across the financial sector. It aims at enhancing the value of customer data through increased data sharing and re-use for customised financial products and services for consumers and SMEs.
The different steps for the digital transformation of the financial sector must also take into account the impulses coming from the parallel process of transition to a sustainable economy. Both paths are at the heart of the European Commission's vision of

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco" Il testo del presente contributo sviluppa, amplia e aggiorna le considerazioni svolte nel corso del Convegno organizzato dall'Associazione Europea per il Diritto Bancario e Finanziario (AEDBF) in tema di "Prospettive di credito per una ripresa sostenibile", tenutosi il 25 novembre 2022 presso la Banca d'Italia, nella sede di Milano..

a digital and sustainable Europe.
Against this background, the contribution aims to offer some regulatory coordinates on possible developments resulting from the synergy between the paths of digital innovation and sustainability. In particular, it aims to provide initial reflections on green mortgages and credit access opportunities for consumers and SMEs within an open financial ecosystem.

Sommario

1. Il percorso dell'innovazione tra tecnologia e sostenibilità. Profili introduttivi – 2. L'*Open Finance* e la prossima sfida dell'innovazione digitale: uno sguardo d'insieme – 2.1. La ricostruzione delle coordinate di nascita e di sviluppo dell'*Open Finance* tra percorsi verticali, intersezioni orizzontali e obiettivi ambiziosi: una strada di lunga percorrenza – 3. Il credito "sostenibile": il ruolo ambivalente di un aggettivo - 4. Sostenibilità e credito: verso una disciplina dei mutui e prestiti green? – 5. *Open Finance* e credito sostenibile: lavori in corso all'insegna di un merito creditizio sostenibile o di un *green credit scoring*? Qualche osservazione conclusiva.

Keywords

finanza digitale - open finance – condivisione dati – credito sostenibile – mutui green

1. Il percorso dell'innovazione tra tecnologia e sostenibilità. Profili introduttivi

Da alcuni anni i temi della digitalizzazione e della sostenibilità hanno assunto un carattere *mainstream* nelle politiche attivate o programmate dalla Commissione europea per il prossimo futuro.
La strada di lunga percorrenza in direzione di un quadro europeo adeguato all'era digitale e alla sostenibilità è guidata dalle molteplici finalità sottese alle diverse azioni messe in campo per favorire la trasformazione digitale e la transizione verde[1], da in-

[1] Il lavoro rientra tra le attività di ricerca del gruppo UNIBA affiliato allo Spoke 4 "Sustainable Finance", relative al Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3, Partenariato Esteso "GRINS – Growing Resilient, INclusive and Sustainable", tematica "9. Economic and financial sustainability of systems and territories", (CUP n. H73C22000930001), finanziato dall'Unione europea – NextGenerationEU.
Tanto deriva dalle dichiarazioni programmatiche della Presidente Ursula von der Leyen, oggetto del discorso tenuto il 16 settembre 2020 su "*Lo Stato dell'Unione 2020. La Commissione von der Leyer: un anno dopo*" e traslate nei documenti europei pubblicati a partire dal *Green Deal* europeo (cfr. Commissione europea, *Il Green Deal europeo* [COM(2019) 640 final – 11 dicembre 2019, *eur-lex.europa.eu*] sino alla Nuova Agenda dei Consumatori (Commissione europea, *Nuova agenda dei consumatori. Rafforzare la resilienza dei consumatori per una ripresa sostenibile* [COM(2020) 696 final, 13 novembre 2020, *ec.europa.eu*].
Un chiaro invito a tracciare la rotta per il prossimo futuro nel duplice senso indicato proviene *inter alia* da: L. Floridi, *Il verde e il blu. Idee ingenue per migliorare la politica*, Milano, 2020; S. Epifani, *Sostenibilità digitale. Perché la sostenibilità non può fare a meno della trasformazione digitale*, Roma, 2020.

tendersi ormai quali sfide indissolubili[2].
Un connubio, quello da ultimo indicato, che nel tempo si è trasformato in una simbiosi di percorsi i quali, pur nel rispetto delle specificità proprie di ciascuno, si sono congiunti nell'oggetto principale della strategia operativa del nuovo corso della Commissione europea, all'insegna di un'Europa sostenibile e digitale[3].
Il disegno europeo è divenuto così il risultato di un'azione sinergica tesa a valorizzare le potenzialità sottese a ciascuno dei due versanti indicati[4].
Difatti, il carattere biunivoco degli obiettivi da raggiungere fa sì che il riferimento alla sostenibilità non si esaurisca solo nella promozione dello sviluppo sostenibile attraverso il ricorso alla tecnologia, bensì si estenda sino a garantire nel contempo un uso sostenibile della stessa tecnologia[5].
La duplice funzionalità dei predetti obiettivi ha contribuito in tal modo a creare un varco – a mo' di passaggio quasi obbligato - dal quale devono transitare tutte le azioni e le misure messe in campo all'insegna tanto del rilancio e della crescita dei Paesi, quanto, nell'ambito di una visione più ampia, del rafforzamento della coesione e del ruolo dell'Unione Europea in un contesto globale.
Trattasi di un progetto ambizioso, rafforzatosi a seguito della pandemia e della conseguente emersione dei diversi punti deboli che hanno a lungo penalizzato il sistema economico-finanziario del Paese, sui quali sono state adottate misure emergenziali di varia natura (a cominciare dal credito)[6].
A livello europeo poi la Commissione, cavalcando l'onda dell'accelerazione del processo di digitalizzazione – rispetto alla quale la pandemia e le misure di restrizione hanno svolto un effetto di detonatore – ha intensificato il suo lavoro, dapprima mappando le aree da attenzionare, poi adottando la Strategia europea per la finanza digitale[7] che ha selezionato le prossime sfide da affrontare.
Sfide che, come anticipato, andranno valutate anche alla luce dei criteri di sostenibilità, che, già oggetto della Strategia per il finanziamento della transizione verso un'econo-

[2] In tal senso anche la comunicazione della Commissione europea, "*Shaping Europe's digital future*", COM(2020) 67 final, 19 febbraio 2020, in *commission.europa.eu*.

[3] Cfr. Commissione europea, *Una strategia per le PMI per un'Europa sostenibile e digitale*, COM(2020) 103 final del 10 marzo 2020, in *ec.europa.eu*.

[4] Sul rapporto tra i percorsi attivati su entrambi i versanti sia consentito rinviare a M.T. Paracampo, *FinTech e la Strategia europea per il mercato unico tecnologico dei servizi finanziari*, in M.T. Paracampo (a cura di), FINTECH. *Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino, 2021, vol. I, 22 ss.

[5] A titolo esemplificativo si segnala, da ultimo, l'approvazione il 20 aprile scorso - da parte del Parlamento europeo - del testo *relativo alla proposta di regolamento europeo relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937*, che nel corso dell'*iter* normativo ha annoverato *inter alia* anche significative integrazioni con riguardo all'impatto ambientale della tecnologia sottostante alle cripto-attività.

[6] Il profluvio di interventi, dettati dall'emergenza sanitaria, è oggetto dei diversi contributi raccolti nel volume di A. Sciarrone Alibrandi - U. Malvagna (a cura di), *Sistema produttivo e finanziario post Covid 19: dall'efficienza alla sostenibilità. Voci dal diritto dell'economia*, Pisa, 2021, nonché in quello a cura di D. Rossano, *Covid 19. Emergenza sanitaria ed economia. Rimedi e prospettive*, Bari, 2020.

[7] Cfr. Commissione europea, *Strategia in materia di finanza digitale per l'UE* [COM(2020) 591 final, 24 settembre 2020, *ec.europa.eu*].

mia sostenibile[8], a sua volta ha acquisito rilevanza trasversale, tanto da assurgere a filo conduttore delle azioni messe in campo tanto in ambito finanziario[9], quanto – più in generale – in tema di trasformazione digitale[10].

Hanno cominciato così a profilarsi diverse tematiche di frontiera, che coniugano le sfide e le potenzialità rivenienti dalla transizione digitale e da quella sostenibile, su cui possono convergere più obiettivi politici della Commissione europea, creando percorsi paralleli e nel contempo complementari.

In questo contesto si inserisce appieno il connubio tra *Open Finance* e credito "sostenibile", quale oggetto di ricerca che trae spunto da una pletora di interventi europei, taluni in corso di definizione, altri solo preannunciati e di prossima consultazione con riguardo ad un altro obiettivo ambizioso, che il legislatore europeo si sta impegnando a realizzare entro il 2024.

Il tema trae origine dal crescente processo di valorizzazione dei dati[11] – di cui peraltro il settore finanziario è particolarmente ricco - che può tradursi in molteplici opportunità per consumatori, imprese e *players* del mercato, in funzione della creazione di un ecosistema finanziario aperto (i.e. *Open Finance*), sostenibile e resiliente[12].

Di tal ché se sul primo versante si avvicina l'appuntamento con la pubblicazione di una bozza di *framework* in materia di *Open Finance*[13], sul secondo versante l'elemento *green*[14]

---

[8] Cfr. COM(2021) 390 final, 6 luglio 2021, in *eur-lex.europa.eu.*

[9] Il connubio trova espressione nella locuzione "*Green FinTech*", su cui si segnala la guida curata da The Green Fintech Network, *Harnessing the Power of Digital Finance for Sustainable Financial Markets. Green fintech action plan: 16 proposals for the Swiss financial centre*, April 2021, in *backend.finance.swiss.*

Al riguardo si rammenta anche come il *Green FinTech* costituisca obiettivo dichiarato dell'ESMA, incluso nel suo programma di lavoro per il prossimo futuro (cfr. *Sustainable Finance Roadmap 2022-2024*, 10 February 2022, ESMA30-379-1051, in *esma.europa.eu).*

L'Autorità europea, nella prospettiva di promuovere una supervisione effettiva e coerente in ordine alla sostenibilità relativa all'innovazione, ha richiamato sul punto i gruppi appositamente creati nell'ambito della stessa Autorità, unitamente al lavoro dell'EFIF, i quali congiuntamente dovranno:

« - Identify use cases of innovative technologies that help channel investments into sustainable objectives and assist transition to a greener economy ('green FinTech') and invite firms to present case studies at EFIF meetings;

- Include sessions on green FinTech and sandboxes in EFIF meeting to collect evidence on their interactions and recent trends».

[10] Sugli ultimi sviluppi a livello internazionale si segnalano: E. Feyen - H. Natarajan - M. Saal, *FinTech and the future of finance. Markets and policy implication*, The World Bank Group, 2023, *documents.worldbank.org,* nonché E. Feyen - J. Frost - L. Gambacorta - H. Natarajan - M. Saal, *Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy. Fintech and the Future of Finance*, Flagship Technical Note, in *documents.worldbank.org,* 2022.

[11] Cfr. D.W. Arner - R.P. Buckley - D.A. Zetzsche, *Open Banking, Open Data and Open Finance: Lessons from the European Union*, March 2022, in *researchgate.net;* N. Lauridsen, *Unlock the value of data: from open banking to open finance, the role of regulation*, 2 November 2022, in *fbf.eui.eu* ; OECD, *Personal Data Use in Financial Services and the Role of Financial Education: A Consumer-Centric Analysis,* in *oecd.org,* 2020.

[12] D. W. Arner - R.P. Buckley - D.A. Zetsche, *FinTech and the Four Horsemen of the Apocalypse*, University of Hong Kong Faculty of Law Research Paper No. 2022/49, UNSW Law Research Paper No. 22-30, September 2022, in *ssrn.com.*

[13] Cfr. European Commission, *Commission Work Programme 2023, Annex I: New Policy Objectives,* 18 October 2022.

Dall'Agenda dei lavori della Commissione, resa pubblica di recente, si evince la pubblicazione di una bozza di *framework* sull'*Open Finance,* calendarizzata per il 28 giugno 2023.

[14] Allo stato attuale, dei tre fattori ESG solo il primo (*environmental*) ha ricevuto opportuna attenzione, anche a causa di una tassonomia non riconosciuta o non condivisa con riguardo agli altri due (*social* e

diviene un vero e proprio *must* - talora un passaggio obbligato - ai fini sia della realizzazione tanto della Strategia per la transizione verso l'economia sostenibile, quanto del conseguimento delle finalità sottese al Piano d'Azione per la *Capital Markets Union*[15].
Tuttavia, l'effetto combinato dei profili di innovazione digitale e di sostenibilità va costantemente contestualizzato, involgendo di conseguenza la necessaria considerazione dei processi normativi afferenti allo specifico settore finanziario di volta in volta coinvolto.
In un dedalo di interventi ed azioni di diversa natura, che rendono particolarmente articolata l'attività di ricostruzione delle coordinate di un quadro normativo ancora *in fieri*, il presente contributo si propone quindi di individuare se e quali prospettive di credito "sostenibile" possano configurarsi nell'ambito di uno scenario di *Open Finance*, ovvero se un ecosistema di finanza aperta possa favorire (*rectius:* incrementare) le possibilità di accesso al credito da parte di consumatori e PMI, mantenendo quelle promesse di inclusione finanziaria diffusamente pubblicizzate[16] come manifesto della nuova sfida *disruptive*.
Il percorso terrà conto anche del processo evolutivo in direzione di un'economia guidata dai dati, nonché, con specifico riferimento al settore creditizio, di quello relativo alla revisione delle direttive in materia di credito ai consumatori (2008/48)[17] e di credito immobiliare ai consumatori (2014/17)[18].
Diversi sono quindi i tasselli di un *puzzle* complesso, che necessita preliminarmente di una considerazione autonoma di ciascun aspetto della tematica indicata (*Open Finance* da un lato e credito "sostenibile" dall'altro lato), di cui sembra opportuno dar conto per lo meno in una ricostruzione sommaria. Segue poi una visione d'insieme dei due profili, che si presta a diversi spunti di riflessione, i quali - lungi da ogni pretesa di esaustività[19] - saranno oggetto di alcune osservazioni, avendo riguardo ai concomitanti passi compiuti o ancora *in itinere*, a livello normativo e non, su entrambi i percorsi indicati.

governance).

[15] Cfr. Commissione europea, Comunicazione su "*Unione dei mercati dei capitali — Risultati conseguiti un anno dopo il piano d'azione*", COM(2021) 720 final, 25 novembre 2021, in *eur-lex.europa.eu*.

[16] Cfr. D. Awrey - J. Macey, *The Promise and Perils of Open Finance*, ecgi, Law Working Paper N° 632/2022, May 2022, in *ecgi.global*.

[17] Cfr. Commissione europea, *Proposta di direttiva del Parlamento europeo e del Consiglio relativa ai crediti al consumo*, COM(2021) 347 final, 30 giugno 2021.

[18] Cfr. European Commission, *Consultation Document. Review of the mortgage credit directive*, 22 November 2021, in *ec.europa.eu*.

[19] Le osservazioni proposte in questa sede, afferendo ad un percorso ancora *in fieri* ed aperto a diverse soluzioni, non sono esaustive, né tanto meno definitive.
Il presente contributo costituisce solo la prima di una serie di puntate sul tema *dell'Open Finance*, in relazione al quale il finale – parimenti al versante sulla sostenibilità – è ancora tutto da scrivere.

2. L'*Open Finance* e la prossima sfida dell'innovazione digitale: uno sguardo d'insieme

L'*Open Finance* rappresenta la prossima fermata del treno dell'innovazione che coinvolgerà indistintamente tutti i settori finanziari e tutti i *players* (in)direttamente coinvolti nel settore finanziario e non, ma soprattutto sancirà la centralità del cliente e dei suoi dati.

La nuova sfida è stata presentata dalla Commissione europea con tutti i sintomi caratteriali, tali da considerarla l'ennesima rivoluzione che riplasmerà il settore finanziario all'insegna di un ecosistema aperto e sulla scorta di un nuovo paradigma[20], quello dell'apertura dei dati, con la finalità di garantirne un maggiore accesso e condivisione in quella che potrebbe considerarsi "un'economia circolare dei dati".

Trattasi di un fenomeno innovativo, privo al momento di una definizione univoca[21], in attesa di quella normativa[22], che tuttavia fa leva su tre momenti fondamentali e connessi, tali da valorizzare la centralità dei dati del cliente, quali, in primo luogo, la considerazione dei dati come *commodities* suscettibili di accesso, condivisione e riuso, previo consenso del cliente medesimo, il quale dovrà conservare il controllo dei propri dati, acquisendo consapevolezza sul relativo utilizzo[23].

L'aggettivo di "apertura", che connota e svetta nella locuzione utilizzata, risulta *ictu oculi* foriero di implicazioni per un ecosistema finanziario già profondamente trasformato dalla tecnologia applicata e che, nel caso di specie, diviene un altro esempio del processo di frammentazione della catena di valore[24], diversamente ricomposta in virtù

---

[20] Una panoramica descrittiva sulle leve del prossimo sistema e sulle dinamiche rivenienti dall'avvento del paradigma *open*, si deve al rapporto curato da The European House Ambrosetti, dal titolo "*Come il paradigma «open» sta trasformando gli ecosistemi finanziari*", 1° aprile 2022.

[21] Quanto ai margini definitori della nuova rivoluzione, la difficoltà nell'offrire una precisa definizione emerge anche dalla cautela adottata dall'EIOPA nel cercare di descrivere il processo dell'*Open Insurance* - nato in parallelo, ma in realtà parte integrante dell'*Open Finance* – nell'ambito del Discussion Paper, pubblicato già a gennaio 2021, su *Open Insurance: accessing and sharing insurance-related data,* seguito il 15 giugno 2022 dalla pubblicazione di *Feedback Statement on Open Insurance: accessing and sharing insurance-related data*, entrambi reperibile sul sito istituzionale dell'Autorità europea: *«There is no uniform definition of open insurance or open finance, nor is there sufficient settled academic or expert literature on this, as these developments are relatively new. In available sources (e.g. Position Papers, industry papers) and in practice it is sometimes understood narrowly, referring to compulsory personal data sharing based on the explicit consent of consumer (so-called 'PSD2' type of approach). On the other hand it is also used to describe broader information sharing via APIs between different insurance market players, including in the back office and in a way that might not be directly 'visible' for the consumers (sometimes also referred as 'API insurance', 'Open API' or 'connected insurance' (e.g. interaction between insurers and intermediaries or other third parties/outsourcing partners, including Internet of Things (IoT) providers). This could include both personal data and non-personal data».*

[22] Quella di una definizione omnicomprensiva di tutte le fattispecie o *use cases* suscettibili di inclusione nel contesto del nuovo fenomeno costituisce già la prima sfida per il legislatore, che dovrà misurarsi con i limiti fissati da altre normative a tutela del consumatore (tra cui *inter alia* il GDPR).
Il tema è oggetto di osservazioni da parte di D. Medine - A. Plaitakis, *Combining Open Finance and Data Protection for Low-Income Consumers,* February 2023, in *cgap.org.*; World Bank Group, *The role of Consumer Consent in Open Banking. Financial Inclusion Support Framework*, Technical Note, December 2021, in *openknowledge.worldbank.org.*

[23] ING, *Open Finance: a blueprint for more customer control over financial data*, ING Viewpoint, September 2022, in *ing.com.*

[24] Sulle principali implicazioni della frammentazione della catena di valore nell'ambito della finanza

del differente utilizzo dei dati e del ruolo dei soggetti – *old* e *new players* - coinvolti nella nuova catena dei dati.

Il percorso intrapreso in questa direzione trae spunto e recepisce l'esperienza maturata con l'*Open Banking*[25], introdotta dalla PSD2, di cui ne prosegue il cammino[26], ne accentua l'effetto *disruptive* – quale tratto peculiare dell'impatto della tecnologia nella finanza -e raggiunge l'apice nel momento in cui oblitera i margini circoscritti ai servizi di pagamento per estendere l'orizzonte a tutti gli altri settori - ed ai dati raccolti nella prestazione dei vari servizi – a favore di un unico e più ampio ecosistema finanziario, basato sulle interazioni dapprima *cross sector*, nel prossimo futuro anche *cross industry*.

Gli impatti, soprattutto in termini di benefici ed opportunità per imprese e consumatori, possono essere molteplici con riguardo a tutti gli aspetti finanziari (i.e. creditizi, assicurativi, di investimento, di pagamento, etc.) che coinvolgono la vita (finanziaria) di detti destinatari, previo scioglimento però di alcuni nodi problematici che ogni innovazione porta inevitabilmente con sé[27], quando si confronta con un sistema tradizionale già strutturato.

Prodotti e servizi personalizzati, unitamente a maggiori possibilità di accesso ai servizi finanziari anche in termini di prospettive di inclusione finanziaria soprattutto di PMI e consumatori[28], si confermano i *target* fondamentali del prossimo quadro regolamentare, sebbene il *quomodo* sia ancora tutto da concertare in maniera univoca e convergente, identificando la vera sfida sia per i regolatori, sia per gli operatori finanziari che, in definitiva, saranno chiamati a condividere i dati dei clienti.

Nel cercare di offrire qualche spunto di riflessione su una tematica "aperta" a diverse sollecitazioni provenienti dai diversi profili di indagine ivi inclusi, appare opportuno

---

digitale si rinvia alla *Joint European Supervisory Authority response to the European Commission's February 2021 Call for Advice on digital finance and related issues: regulation and supervision of more fragmented or non-integrated value chains, platforms and bundling of various financial services, and risks of groups combining different activities*, ESA 2022 01 - 31 January 2022, in *esma.europa.eu.*

[25] Cfr. R. Pellittieri - R. Parrini - C. Cafarotti - B.A. De Vendictis, *Mercati, infrastrutture, sistemi di pagamento. L'Open Banking nel sistema dei pagamenti: evoluzione infrastrutturale, innovazione e sicurezza, prassi di vigilanza e sorveglianza*, Quaderno Banca d'Italia, n. 31, marzo 2023.

L'*Open Banking* ha però fatto emergere anche talune problematiche, che ne hanno frenato in qualche modo un'ampia diffusione. Osservazioni sulle diverse criticità si devono a F. Ciraolo, *Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti",* in *Rivista di Diritto Bancario,* 4, 2020, 611 ss.; M. Rabitti - S. Sciarrone Alibrandi, *I servizi di pagamento tra PSD2 e GDPR: Open Banking e conseguenze per la clientela*, in F. Capriglione (a cura di), *Liber Amicorum Guido Alpa*, Padova, 2019, 711 ss.; OECD, *Data Portability in Open Banking. Privacy and The Other Cross-Cutting Issues,* OECD Digital Economy Papers, No. 348*,* February 2023*,* in *oecd-ilibrary.org.*

[26] Cfr. OECD, *Shifting from Open Banking to Open Finance: Results from the 2022 OECD survey on data sharing frameworks*, OECD Business and Finance Policy Papers, 2023.

[27] Cfr. Keynote speech by Commissioner McGuinness at event in European Parliament "*From Open Banking to Open Finance: what does the future hold?*", Brussels, 21 March 2023, in *ec.europa.eu.*

[28] In particolare, «la finanza aperta può portare a un miglioramento dei prodotti finanziari, della consulenza mirata e dell'accesso per i consumatori, nonché a maggiore efficienza delle operazioni tra imprese. L'accesso a un numero maggiore di dati del cliente permetterebbe inoltre ai fornitori di servizi di offrire servizi più personalizzati e più in linea con le esigenze specifiche dei clienti. Un quadro normativo equilibrato per la condivisione dei dati relativi ai prodotti finanziari sosterrà il settore finanziario nella piena adozione della finanza basata sui dati e proteggerà in modo efficace gli interessati, che devono avere pieno controllo sui propri dati» (cfr. Commissione europea, *Strategia in materia di finanza digitale per l'UE,* cit. [COM(2020) 591 final, 24 settembre 2020).

prendere le mosse da una ricostruzione del contesto operativo in considerazione e dei passi in direzione della definizione del *framework* normativo in tema di *Open Finance*, per passare in una seconda parte a valutare le opportunità di credito – anche in termini di sostenibilità - che il nuovo contesto potrebbe offrire a consumatori e PMI.

2.1 La ricostruzione delle coordinate di nascita e di sviluppo dell'*Open Finance* tra percorsi verticali, intersezioni orizzontali e obiettivi ambiziosi: una strada di lunga percorrenza

Il processo di definizione di un *framework* in tema di *Open Finance* risulta piuttosto composito e si snoda in diversi passaggi – alcuni lineari, altri intersecati – di cui appare opportuno dar sommariamente conto con la finalità di individuare le diverse coordinate ed i molteplici ambiti (in)direttamente coinvolti in un disegno legislativo di ampia portata, ma soprattutto ambizioso.

Il percorso in direzione dell'*Open Finance* è stato graduale[29], prendendo l'avvio circa dieci anni orsono con la pubblicazione della prima[30] di una serie di comunicazioni della Commissione europea incentrate sul valore dei dati[31], in funzione dell'avvio del futuro mercato unico dei dati.

Il processo quindi non è recente, ma parte da lontano, con radici che crescono e si ramificano in un susseguirsi di passi che hanno dato vita ad un *trend* crescente, incentrato sulla tecnologia utilizzata (i.e. API) per valorizzare la centralità dei dati del cliente, incrementarne l'accesso e la condivisione, in modo da giungere – nelle intenzioni della Commissione europea – a realizzare l'obiettivo di un'economia guidata dai dati.

In questo contesto l'*Open Finance* rappresenta solo una parte di un complesso ecosistema, nel quale, in una visione di lungo corso, dovrebbe avvicinarsi, contaminarsi ed interagire con altre parti rivenienti dall'apertura dei dati in altrettanti diversi ambiti dell'economia.

Motivo per il quale il disegno del legislatore europeo comincia ad assumere contorni più precisi con la Strategia europea per i dati, ove l'intento di valorizzare questi ultimi viene finalizzato alla creazione di nove spazi comuni europei dei dati, tra cui trova pieno riconoscimento quello relativo ai dati finanziari, che si pone *a latere* rispetto a quelli

[29] Altrettanto graduale potrebbe essere la sua implementazione, una volta approvato il relativo *framework*, come proposto dall'EBA (cfr. *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*, EBA/Op/2022/06, 23 June 2022): «*The EBA believes that the implementation of a future legal framework on Open Finance should be phased. It could potentially start with opening access to non-payment accounts and banking products and subsequently extend to other financial products. Also, it should first and foremost focus on viable consumer propositions, business models and use-cases, to avoid setting requirements that require substantial costs to implement for a solution that is hardly used in the end*» (§ 419).

[30] Cfr. Comunicazione della Commissione europea, *Verso una florida economia basata sui dati*, COM(2014) 442 final del 2 luglio 2014, in *eur-lex.europa.eu.*

[31] Convergono verso lo stesso obiettivo anche le seguenti comunicazioni: "*Costruire un'economia dei dati europea*", COM(2017) 9 final del 10 gennaio 2017*;* "*Verso uno spazio comune europeo dei dati*", COM(2018) 232; "*Strategia europea per i dati*", COM(2020) 66 final, 19 febbraio 2020; tutte in *eur-lex.europa.eu.*

relativi: ai dati industriali (manifatturieri), ai dati sul *Green Deal*, ai dati sulla mobilità, ai dati sanitari, ai dati sull'energia, ai dati sull'agricoltura, ai dati per la pubblica amministrazione, ai dati sulle competenze. Rispetto a detti spazi comuni la Commissione si è riservata poi di individuarne di ulteriori, accomunati ai nove indicati dall'impatto sistemico che i relativi dati potrebbero avere sull'intero ecosistema.

In uno scenario in divenire la Strategia per i dati diviene lo snodo cruciale, quale punto di diramazione per altrettanti percorsi, taluni con un approccio settoriale, altri di rilevanza trasversale. Al momento, in una visione d'insieme diversi sono i passi compiuti, di cui peraltro taluni in successione progressiva[32], altri su versanti paralleli ma strettamente intersecati in un dedalo sempre più fitto.

Difatti, solo sul versante finanziario, il tema dell'*Open Finance*, già punto di forza della Strategia per la finanza digitale, diviene punto di raccordo con quelli, altrettanto attenzionati e convergenti verso finalità inclusive e sostenibili, rappresentati – come già anticipato, dal nuovo piano d'azione per la *Capital Markets Union*[33] e dalla Strategia europea per gli investimenti *retail*[34].

Entrambi si completano, dal momento che in quest'ultima la finanza aperta adotta la prospettiva dell'investitore per coinvolgerlo maggiormente nel processo di investimento, rafforzando nel contempo il quadro normativo di tutela.

L'effetto conseguente, nelle intenzioni del legislatore, dovrebbe tradursi nella fiducia accordata ai mercati, generando così un circolo virtuoso di cui può beneficiare anche l'Unione dei Mercati dei Capitali, il cui processo di completamento dovrebbe essere quasi al termine.

Ricerca di ulteriori canali di finanziamento per le PMI e potenziamento delle PMI a livello europeo tramite diversi canali di raccolta di capitale rappresentano il risultato dell'effetto combinato e dell'azione sinergica dei lavori condotti su più tavoli. Ulteriore sostegno deriva dall'*Open Finance* che, nel consentire l'accesso ai dati, può contribuire a canalizzare i flussi di raccolta verso le PMI e verso investimenti sostenibili[35].

---

[32] Traggono origine dall'indicata Strategia il Governance Act, il Data Act e l'AI Act.

[33] European Commission, *A Capital Markets Union for people and business – new action plan*, COM(2020) 590 final del 24 settembre 2020, in *eur-lex.europa.eu*.
Tuttavia il tema dell'*Open Finance* è oggetto di specifica considerazione nella comunicazione su "*Unione dei mercati dei capitali — Risultati conseguiti un anno dopo il piano d'azione"*, cit.

[34] Anche con riferimento a detta Strategia, è stato calendarizzato. nell'Agenda della Commissione europea per il 24 maggio p.v, la pubblicazione di un pacchetto di misure (i.e. *Retail Investment Package*) dirette ad incentivare e favorire un maggiore coinvolgimento degli investitori *retail* nei mercati dei capitali.

[35] *A latere* rispetto all'*Open Finance* si pone, nel contesto tanto della *Capital Markets Union*, quanto della Strategia europea per la finanza digitale, la proposta di regolamento europeo relativa *all'istituzione e il funzionamento del punto di accesso unico europeo* (ESAP), [COM(2021) 725 final del 25 novembre 2021, in *consilium.europa.eu*) che, in linea altresì con la Strategia europea dei dati e la creazione di uno spazio comune europeo dei dati finanziari, mira a rendere pubbliche (i.e. disponibili ed utilizzabili) le informazioni sulla sostenibilità delle attività dei soggetti europei, in modo da favorire – anche per questa via - gli investimenti privati in progetti e attività sostenibili.
Difatti, si legge nella premessa che «l'ESAP contribuirà al conseguimento degli obiettivi dell'Unione dei mercati dei capitali fornendo accesso in tutta l'UE alle informazioni pubblicate da soggetti pertinenti per i mercati dei capitali, i servizi finanziari e la finanza sostenibile, ossia principalmente informazioni sulle loro attività economiche e sui loro prodotti. L'ESAP fornirà l'accesso a tali informazioni in maniera efficiente e non discriminatoria. Le informazioni in merito alle attività e ai prodotti dei soggetti

I risultati possono quindi essere molteplici ed esplicare i propri effetti su tutti i piani considerati.
I passi successivi annoverano dapprima una consultazione della Commissione europea in tema di *Open Finance*[36], poi la pubblicazione di un *report*[37] a cura del gruppo di esperti nominato *ad hoc* su dette tematiche (in particolare sullo spazio comune europeo dei dati finanziari ed un sottogruppo sull'*Open Finance*), cui è stata sottoposta la valutazione circa la fattibilità di taluni casi d'uso, selezionati e riportati in un allegato[38] alla consultazione.
Tanto in vista della preparazione di eventuali proposte legislative ed iniziative politiche in tema di condivisione dei dati nel settore finanziario sia per promuovere la creazione di uno spazio comune europeo di dati finanziari e per valutare la necessità di qualsiasi interazione con altri spazi di dati e condivisione di dati al di fuori del settore finanziario, sia in funzione della descrizione delle componenti chiave di un ecosistema di *Open Finance* nell'Unione europea.

3. Il credito "sostenibile": il ruolo ambivalente di un aggettivo

Guardando ora all'altro termine del discorso, preliminare ad ogni tentativo di individuazione delle coordinate utili al tema su tratteggiato risulta una precisazione in ordine alla locuzione di "credito sostenibile" e, in particolare, al significato da attribuire all'aggettivo che – nei termini in cui si preciserà – potrebbe assumere una duplice valenza nel contesto dell'*Open Finance*. E' difatti suscettibile di riscontro su entrambi i versanti *digital* e *green*, determinando altrettanti risultati, ove però l'uno non esclude, ma può convivere ed essere supportato dall'altro.
Pertanto il riferimento alla sostenibilità, che in entrambi i casi connota – seppure in termini differenti – il credito, può essere declinato come:
sostenibilità del credito, nel senso di capacità del richiedente di adempiere a tutti gli obblighi contrattuali e di rimborsare il credito ricevuto, ove la capacità va rapportata

sono essenziali per il processo decisionale dei fornitori di capitale. L'ESAP contribuirà a integrare ulteriormente i servizi finanziari e i mercati dei capitali nel mercato unico, ad allocare i capitali in modo più efficiente in tutta l'UE e a promuovere lo sviluppo delle economie e dei mercati dei capitali nazionali di dimensioni inferiori offrendo loro una maggiore visibilità. L'ESAP consentirà inoltre ai soggetti non quotati, comprese le piccole e medie imprese (PMI), di rendere disponibili informazioni su base volontaria. Ciò faciliterà il loro accesso al capitale».

[36] Cfr. European Commission, *Consultation Document. Targeted Consultation on Open Finance Framework and Data Sharing in the Financial Sector*, 10 May 2022, in *finance.ec.europa.eu*, con annesso allegato (cfr. *Annex to the Consultation Document – User Cases Targeted Consultation on Open Finance Framework and Data Sharing in the Financial Sector*)
Contestualmente, a sancire il passaggio dall'*Open Banking* all'*Open Finance*, è stato pubblicato in pari data altro documento di consultazione finalizzato piuttosto a richiedere al mercato prove di evidenza utili per la revisione della PSD2 e per l'*Open Finance* (cfr. *Public Consultation on the Review of the Revised Payment Services Directive (PSD2) and on Open Finance*).

[37] Cfr. European Commission, *Report on Open Finance*, Report of Expert Group on European Financial Data Space, October 2022, in *finance.ec.europa.eu.*

[38] Su cui v. *infra.*

sia al tempo di impiego, sia al profilo creditizio e alla situazione economico-finanziaria dello stesso richiedente;
credito sostenibile, ove la sostenibilità assume altra sfumatura alla luce delle implicazioni derivanti dall'accesso al credito, coerente altresì con le finalità *green* e di rispetto dell'ambiente.
Il primo significato suona di certo più familiare, riconducendo verso il mantra del "prestito responsabile"[39], quale perno fondamentale della normativa consumeristica in materia di credito, con la precipua finalità di contrastare fenomeni di sovraindebitamento.
L'obiettivo di favorire una maggiore consapevolezza del consumatore è stato peraltro accentuato di recente in occasione della revisione della direttiva 2008/48/CE in tema di credito ai consumatori[40], che ha riconosciuto cittadinanza normativa all'utilizzo di sistemi di intelligenza artificiale – complice anche la proposta di regolamento in materia[41] – nella valutazione del merito creditizio[42], unitamente a talune precisazioni in ordine al perimetro informativo da prendere in considerazione nel processo di *credit scoring* del richiedente il credito[43].
Diversamente, la seconda accezione *supra* riportata involge un processo normativo

[39] In tema si rinvia alle osservazioni di G. Falcone, *"Prestito responsabile" e valutazione del merito creditizio*, in *Giurisprudenza Commerciale,* I, 2017, 147 ss.; A.A. Dolmetta, *"Merito del credito" e procedure di sovraindebitamento*, in *Fallimento*, 2021, 1207 ss.

[40] In tal senso anche i considerando 45 («Gli Stati membri dovrebbero adottare le misure appropriate per promuovere pratiche responsabili in tutte le fasi del rapporto di credito, tenendo conto delle specificità del proprio mercato creditizio. Tali misure possono includere, per esempio, l'informazione e l'educazione dei consumatori e anche avvertimenti sui rischi di un mancato pagamento o di un eccessivo indebitamento. In un mercato creditizio in espansione, in particolare, è importante che i creditori non concedano prestiti in modo irresponsabile o non emettano crediti senza preliminare valutazione del merito creditizio») e 46 («È essenziale che la capacità e la propensione del consumatore a rimborsare il credito sia valutata e accertata prima della stipula di un contratto di credito o di un contratto di servizi di credito tramite crowdfunding. Tale valutazione del merito di credito dovrebbe avvenire nell'interesse del consumatore, per evitare pratiche irresponsabili in materia di concessioni di prestiti e sovraindebitamento, e dovrebbe tener conto di tutti i fattori necessari e pertinenti che potrebbero influenzare la capacità del consumatore di rimborsare il credito. Gli Stati membri dovrebbero poter dare ulteriori orientamenti in merito ad altri criteri e ai metodi da applicare per valutare il merito creditizio di un consumatore, ad esempio stabilendo limiti sul rapporto mutuo concesso/valore dell'immobile o sul rapporto mutuo concesso/reddito percepito»).

[41] Cfr. Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, COM(2020) 206 final del 21 aprile 2021, in *eur-lex.europa.eu.*

[42] Nella citata proposta la verifica del merito creditizio o dell'affidabilità creditizia delle persone fisiche, effettuata con sistemi di intelligenza artificiale, viene classificata tra quelli ad alto rischio, «in quanto determinano l'accesso di tali persone alle risorse finanziarie o a servizi essenziali quali l'alloggio, l'elettricità e i servizi di telecomunicazione. Data l'alta posta in gioco, ogniqualvolta la valutazione del merito creditizio comporti un trattamento automatizzato, il consumatore dovrebbe avere il diritto di ottenere l'intervento umano da parte del creditore o dei fornitori di servizi di credito tramite crowdfunding. Il consumatore dovrebbe inoltre avere il diritto di ottenere una spiegazione significativa della valutazione effettuata e del funzionamento del trattamento automatizzato applicato, compresi, fra l'altro, le principali variabili, la logica e i rischi inerenti, come pure il diritto di esprimere la propria opinione e di contestare la valutazione del merito creditizio e la decisione» (cfr. considerando 48).

[43] Il riferimento è ai dati alternativi o non tradizionali, tratti dai *social media* (cd. *soft data*), oggetto di molteplici osservazioni, nel contesto della verifica del merito creditizio, da parte di F, Mattassoglio, *Innovazione tecnologica e valutazione del merito creditizio dei consumatori. Verso un Social Credit System?,* Milano,

innovativo ancora *in fieri* e su cui la Commissione sta muovendo i primi passi che devono tener conto di un fitto reticolato di misure orizzontali e verticali in materia di sostenibilità, strettamente – e non sempre adeguatamente – intersecate.

Gli Orientamenti dell'EBA in materia di concessione e monitoraggio dei prestiti[44], dal canto loro, pur essendo sistematicamente richiamati e prendendo in considerazione entrambi gli aspetti[45], riportano in un glossario introduttivo solo la definizione di "prestito sostenibile dal punto di vista ambientale"[46], a fronte dei cennati processi di revisione delle direttive in tema di credito ai consumatori e di credito immobiliare ai consumatori che insistono invece sul profilo del "prestito responsabile", da aggiornare all'era digitale.

Il che involge estensione, natura e qualità dei dati presi in considerazione ai fini della valutazione del merito creditizio, accesso a dati *aliunde* forniti dal consumatore, utilizzo sia dei sistemi di intelligenza artificiale per l'analisi dei dati[47], sia delle APIs per la condivisione dei dati del cliente (previo suo consenso), nonché fattispecie innovative emerse dall'applicazione tecnologica al settore del credito (a titolo esemplificativo, la

2018.

Sui dati alternativi il legislatore europeo assume una posizione del seguente tenore: «La valutazione del merito di credito dovrebbe basarsi sulle informazioni riguardanti la situazione economico-finanziaria del consumatore, reddito e spese comprese. Le Linee guida dell'Autorità bancaria europea sull'origine e il monitoraggio dei prestiti (EBA/GL/2020/06) indicano quali categorie di dati possano essere utilizzate per il trattamento dei dati personali ai fini della valutazione del merito creditizio, compresi i documenti giustificativi del reddito, le fonti di rimborso, le informazioni sulle attività e passività finanziarie o le informazioni su altri impegni finanziari. Nell'effettuare tale valutazione non dovrebbero essere usati i dati personali trovati sulle piattaforme dei media sociali, o i dati sanitari, compresi quelli relativi ai tumori. Per facilitare la valutazione, i consumatori dovrebbero fornire informazioni sulla loro situazione economico-finanziaria. In linea di principio, il credito dovrebbe essere erogato al consumatore solo quando i risultati della valutazione del merito creditizio indicano che gli obblighi derivanti dal contratto di credito o dal contratto per la fornitura di servizi di credito tramite crowdfunding saranno verosimilmente adempiuti secondo le modalità prescritte dal contratto in questione. Tuttavia, qualora tale valutazione dovesse dare esito negativo, il creditore o il fornitore di servizi di credito tramite crowdfunding può eccezionalmente concedere il credito in circostanze specifiche e giustificate, come nel caso di una relazione commerciale di lunga data con il consumatore, o in caso di prestiti per finanziare spese sanitarie eccezionali, prestiti destinati agli studenti e prestiti per consumatori con disabilità. In tali casi, nel decidere se concedere o meno il credito al consumatore, il creditore o il fornitore di servizi di credito tramite crowdfunding dovrebbe tenere conto dell'importo e della finalità del credito e della probabilità che gli obblighi derivanti dall'accordo siano rispettati» (cfr. considerando 47).

[44] Cfr. EBA/GL/2020/06 del 29 maggio 2020, in *eba.europa.eu*.

[45] Si legge *sub* § 131 che «nel valutare la posizione finanziaria dei clienti, gli enti dovrebbero valutare la sostenibilità e la fattibilità della futura capacità di rimborso in condizioni potenzialmente avverse pertinenti per il tipo e la finalità del prestito e che possono verificarsi nel corso della durata del contratto di prestito».

[46] Tale si intende «un prestito volto a finanziare attività economiche sostenibili dal punto di vista ambientale. Fa parte del più ampio concetto di «finanza sostenibile», espressione con la quale si intende qualsiasi strumento finanziario o investimento, compresi titoli di capitale, titoli di debito, garanzie o strumenti di gestione dei rischi emessi in cambio della prestazione di attività di finanziamento che soddisfano i criteri della sostenibilità ambientale».

[47] Sulla diffusione dei sistemi di intelligenza artificiale e di *machine learning* nel *credit scoring* si rinvia ai risultati di un sondaggio, riportati in Aa. Vv., *Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano*, Questioni di Economia e Finanza, Occasional Papers, Banca d'Italia, n. 721, ottobre 2022, nonché alle osservazioni *inter alia* di M. Rabitti, *Credit scoring* via *machine learning* e prestito responsabile, in *Riv. Dir. Banc.,* 1, 2023, 175.

crescente diffusione del *buy now pay later*)[48] e dalla revisione dei modelli di *business* alla luce di processi di *rebundling* della catena di valore per la prestazione dei servizi e/o la distribuzione di nuovi prodotti di credito[49].
Sebbene i cennati aspetti siano ancora da approfondire, in attesa di risposte specifiche (e imminenti, come già accennato) da parte della Commissione europea, di diverso tenore invece si è rivelato sinora l'approccio del legislatore all'integrazione dei profili di sostenibilità nel corso delle revisioni normative in atto.
La proposta di modifica della direttiva 2008/48/CE – e parimenti il testo modificato dal Consiglio d'Europa – sembra rimanere immune alle innovazioni *green*[50], a differenza di quello recante modifica della direttiva 2014/17/UE che, oltre a vantare un diverso *background*, offre una prospettiva dei mutui (*rectius:* crediti immobiliari), che ben si coniuga con tematiche di impatto ambientale (quali l'efficientamento energetico, etc.).
È pertanto a quest'ultima ed ai possibili sviluppi normativi che si dedicherà qualche osservazione, essendo al centro di più interventi tesi ad introdurre una definizione comune ed una disciplina sui mutui e sui prestiti *green*, tale però da colmare – nei termini in cui si illustrerà nel prosieguo - anche la predetta lacuna della direttiva sul credito ai consumatori.

4. Sostenibilità e credito: verso una disciplina dei mutui e prestiti *green*?

Sul versante incentrato sulla configurazione di prospettive di credito sostenibile[51], nello scenario normativo attuale e di prossima definizione (i.e. *Open Finance*), il panorama diviene oltremodo più articolato.
Il binomio – in questo caso tra credito e sostenibilità – si colora di altre sfumature, alla luce dell'attenzione pressoché esclusiva dedicata all'elemento *green*, che assume una connotazione trasversale a tutte le politiche europee, tanto da divenire il filo conduttore del processo di revisione di tutte le fonti normative settoriali in materia finanziaria, nella prospettiva di adeguarle all'era della sostenibilità (e in particolare ai profili di

[48] A tal proposito si segnala la comunicazione pubblicata da Banca d'Italia il 28 ottobre 2022 in materia di *Buy Now Pay Later* (BNPL), in *bancaditalia.it*.

[49] Cfr. da ultimo A. Perrazzelli, *Le banche estere in Italia: regolamentazione e innovazione,* Intervento presso AIBE, 3 aprile 2023, reperibile sul sito istituzionale di Banca d'Italia.
Si precisa che detto specifico profilo, il quale afferisce propriamente al versante della "sostenibilità del credito", viene per il momento accantonato, in quanto oggetto di approfondimento in altra sede. In questa il *focus* è posto piuttosto sulla seconda accezione *supra* riportata di "credito sostenibile".

[50] Il Comitato economico sociale europeo, nelle conclusioni presentate con riguardo alla proposta di modifica della direttiva 2008/48, ha difatti evidenziato come «le soluzioni previste dalla direttiva debbano concentrarsi maggiormente sull'impatto della digitalizzazione, sul maggior uso dei dispositivi digitali e sull'erogazione di prestiti «verdi» ai consumatori per aiutare questi ultimi a effettuare acquisti più sostenibili» (cfr. Parere del Comitato economico e sociale europeo sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa ai crediti al consumo [COM(2021) 347 final — 2021/0171 (COD)] (2022/C 105/14).

[51] In questo caso l'aggettivo "sostenibile" dovrebbe racchiudere e divenire espressione di tutti gli obiettivi abilitati dai criteri ESG, per quanto, come già evidenziato, al momento l'attenzione sia pressoché focalizzata solo sul tema *green*.

impatto ambientale)[52].

Nella specie, il percorso in direzione di detto obiettivo annovera diverse strade complementari, che in taluni casi rischiano però di sovrapporsi, avendo riguardo ora al *target* di clientela interessato (solo consumatori o PMI), ora alla natura pubblica o privata dei dati afferenti al richiedente il credito, ora all'interoperabilità e all'accesso ai dati medesimi, nonché *a fortiori* laddove i dati debbano integrarsi o rispecchiare pedissequamente la tassonomia europea delle attività sostenibili.

Di tanto, come detto, non vi è traccia né nella proposta di modifica della direttiva 2008/48/CE, né tanto meno nella posizione assunta al riguardo dal Consiglio d'Europa, che sono focalizzate maggiormente sull'accentuazione dei profili del prestito responsabile e della valutazione del merito creditizio, con precisazioni circa la natura e il novero dei dati da considerare o, viceversa, da escludere.

Diversamente, il tema della sostenibilità comincia ad entrare nel *radar* del legislatore europeo in sede di revisione della direttiva 2014/17/UE sui crediti immobiliari ai consumatori, che annovera *steps* preliminari di differente tenore, nel quale si sono alternate e/o contrapposte sollecitazioni provenienti da associazioni in rappresentanza dell'industria bancaria e dei consumatori, spingendo però per soluzioni di diverso contenuto.

Il tema della sostenibilità – seppure con sfumature ora generiche, ora specifiche - entra così a pieno titolo nelle valutazioni che precedono[53], ma anche in quelle che seguono[54] la consultazione con il mercato sulla revisione della citata direttiva[55].

Punto di partenza comune diviene, a livello generale, l'obiettivo della neutralità climatica da raggiungere entro il 2050 e da conseguire – per la parte che in questa sede rileva – attraverso processi di efficientamento energetico e nell'uso di materiali sostenibili nei lavori di ristrutturazione degli edifici / immobili, quali finalità precipue – e soprattutto quali presupposti - della concessione di mutui *green*.

Comincia così a farsi spazio la fattispecie dei "crediti ipotecari ad alta efficienza energetica", basate sugli esiti di diversi studi condotti sulla correlazione tra l'efficienza energetica dei beni immobili e l'andamento del credito[56]. In detti casi, oggetto dei

---

[52] Il processo di adeguamento delle legislazioni vigenti involge, come già evidenziato, anche il complementare obiettivo della transizione digitale, alla stregua delle linee direttrici della Strategia europea per la finanza digitale. Entrambi i processi di adeguamento dovrebbero favorire l'introduzione di nuove norme sull'interoperabilità e sull'accesso ai dati.

[53] Cfr. European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, *Evaluation of the Mortgage Credit Directive (Directive 2014/17/EU). Final Report*, Publications Office, November 2020, in *op.europa.eu*.

[54] Al riguardo si segnala il duplice intervento dell'EBA, chiamata a fornire ora un'*opinion* a seguito di richiesta della Commissione europea per un *technical advice* su taluni profili della direttiva (Cfr. *Opinion of the European Banking Authority on the European Commission request for technical advice on issues related to the Mortgage Credit Directive*, 23 June 2022, EBA/Op/2022/07, nonché annesso *EBA Report in response to the European Commission request for technical advice on issues related to the mortgage credit directive*, EBA/REP/2022/15), ora a fornire una risposta ad una specifica *Call for Advice* in ordine ai prestiti ed ai mutui *green* (cfr. *Call for Advice to the European Banking Authority on green loans and mortgages,* Ref. Ares(2022)8054528 – 22 November 2022, su cui v. meglio *infra*), per la quale ha tempo invece fino al 29 dicembre 2023.

[55] Cfr. European Commission, *Consultation Document. Review of the mortgage credit directive*, cit.

[56] Diversi studi condotti sul tema *de quo* sono menzionati e presi in considerazione dalla Commissione

primi prodotti creditizi distribuiti sul mercato, quale risposta ai cambiamenti climatici e per promuovere pratiche sostenibili[57], è emerso un rischio minore di inadempimento da parte dei mutuatari[58].

È anche vero che quello dei mutui verdi rappresenta un mercato ancora di nicchia, rimesso alla discrezionalità degli intermediari finanziari che offrono prodotti talora connotati da termini e condizioni preferenziali nell'ambito dei crediti disponibili, ma tuttora penalizzato – come peraltro riconosciuto anche dall'EBA – dalle criticità riscontrate con riguardo agli *standard* di etichettatura "*green*" e alla disponibilità di dati sufficienti in materia.

Obiettivo, quest'ultimo, che – come *supra* evidenziato - unitamente a quello relativo alla transizione digitale, è posto al centro del processo di completamento della *Capital Markets Union*, ove l'azione europea è finalizzata tanto a favorire le PMI nel reperimento di capitali sul mercato e nell'accesso a fonti di finanziamento anche alternative a quelle bancarie, quanto nel canalizzare il risparmio delle famiglie verso investimenti sostenibili[59] e quindi verso imprese impegnate in attività rilevanti ai fini dell'impatto ambientale.

Eppure costituisce opinione condivisa quella che assegna ai mutui ed a prestiti verdi un ruolo chiave per "supportare gli obiettivi politici europei per gestire i rischi finanziari derivanti dal degrado ambientale e dal cambiamento climatico e riorientare flussi di capitale verso investimenti sostenibili per realizzare la transizione verso l'economia sostenibile"[60].

Differenti si prospettano invece le soluzioni proposte sulle modalità per incentivare la diffusione sul mercato di mutui e prestiti *green*, l'adozione dei medesimi da parte dei consumatori e soprattutto a monte, quale questione preliminare e del tutto scriminante ai fini dell'accesso, cosa debba intendersi per prestiti verdi e come debbano essere disciplinati.

Su quest'ultimo punto, in particolare, le proposte spaziano da interventi normativi *ad hoc*, sino all'integrazione dei profili di sostenibilità all'interno del testo della direttiva mutui, con annesse implicazioni e ricadute sul processo di valutazione del merito creditizio.

---

europea, *Evaluation of the Mortgage Credit Directive (Directive 2014/17/EU),* cit.

[57] A livello europeo si segnalano i lavori svolti in proposito dall'EEFIG (*Energy Efficiency Financial Institutions Group*) per la valutazione del rischio, mentre in ambito industriale rilevano le iniziative in tema di crediti ipotecari ad efficienza energetica dell'EMF-ECBC.

[58] In tal senso Commissione europea, *Relazione della Commissione europea al Parlamento e al Consiglio relativa al riesame della direttiva 2014/17/UE del Parlamento europeo e del Consiglio in merito ai contratti di credito ai consumatori relativi a beni immobili residenziali*, COM(2021) 229 final, 11 maggio 2021, in *data.consilium.europa.eu.*

[59] Siffatta duplice finalità, già evidenziata nella comunicazione relativa all'"*Unione dei mercati dei capitali — Risultati conseguiti un anno dopo il piano d'azione*", cit., è stata di recente ribadita nell'European Commission - Statement, *Capital Markets Union: EU renews commitment to integration and development of capital markets* (28 April 2023, in *ec.europa.eu*), ove si legge: «*developed capital markets are essential to complement public funding to finance the twin green and digital transitions. The EU has high levels of savings which could be channeled towards our green and more sustainable future. Our banking system, however, cannot do it alone*».

[60] Sic EBA, *Opinion of the European Banking Authority on the European Commission request for technical advice on issues related to the Mortgage Credit Directive,* cit.

In uno scenario ancora particolarmente confuso in materia[61], la Commissione europea nel documento posto in consultazione, mira ad ottenere *feedback* utili attraverso domande specifiche, che traggono tutte origine dalla necessità o meno di creare un'ampia definizione europea di mutui *green*, giungendo poi a comprendere se:
detta definizione debba tener conto della tassonomia europea con riguardo all'attività sottostante (i.e. acquisto o ristrutturazione di un edificio già esistente o, ancora, costruzione di uno nuovo);
possano trarne beneficio sia consumatori che finanziatori;
quali misure debbano essere adottate per incoraggiare e favorire la crescita del mercato dei mutui verdi;
di quali specifiche *skills*, tra conoscenze e competenze, debbano dotarsi gli intermediari del credito e il personale di cui si avvalgono i finanziatori, ovvero di tutti quei soggetti che, entrando a diretto contatto con la clientela, dovrebbero fornire informazioni sui prodotti creditizi *de quibus,* eventualmente inseriti nel catalogo della mandante o comunque forniti dai finanziatori.
Occorre poi considerare se e come la definizione di mutuo verde possa influire sulla definizione di contratto immobiliare ai consumatori, dal momento che la scelta potrebbe tradursi nell'introduzione *ex novo* di una definizione di credito immobiliare sostenibile o *green*, nell'integrazione di quella vigente con il profilo della sostenibilità oppure con l'inclusione di detta nuova fattispecie nel novero delle attività incluse nel perimetro di applicazione della direttiva aggiornata.

5. *Open Finance* e credito sostenibile: lavori in corso all'insegna di un merito creditizio sostenibile o di un *green credit scoring*? Qualche osservazione conclusiva

Il punto di congiunzione delle due tematiche indicate emerge dalla considerazione congiunta di più percorsi che devono però ancora trovare una convergenza.
Da un lato si pone la consultazione lanciata dalla Commissione europea in tema di *Open Finance*, unitamente ai casi d'uso individuati e sottoposti alla valutazione del gruppo di esperti nominato con riguardo alla creazione di uno spazio comune europeo dei dati finanziari[62]. Dall'altro lato si prospettano le innovazioni provenienti sia dalla revisione della direttiva sul credito immobiliare ai consumatori, sia dal versante specifico dei mutui e dei prestiti *green*, a cura prima dell'EBA, poi della Commissione europea. Il tutto inserito nell'ampio raggio di azione della Strategia europea per la finanza digitale e della Strategia per il finanziamento per la transizione all'economia sostenibile.

[61] Confusione, unita ad inadeguatezza a coprire tutti i versanti rilevanti, emergono proprio dai passaggi articolati della *Call for Advice to the European Banking Authority on green loans and mortgages,* cit., inviata dalla Commissione europea nell'ambito nella Strategia europea per il finanziamento della transizione ad un'economia sostenibile. Quale seguito di detta richiesta, l'EBA il 13 febbraio 2023 ha lanciato una *survey* (cfr. *EBA seeks input from credit institutions on green loans and mortgages,* in *eba.europa.eu*) finalizzata a ricevere *feedback* dalle istituzioni creditizie sui mutui e prestiti *green*, nonché sulle pratiche di mercato diffuse in materia.

[62] Su cui v. *supra.*

Così con riguardo al primo versante indicato (i.e. consultazione in tema di Open Finance e condivisione dei dati), viene dedicato ampio spazio all'accesso delle PMI alle opzioni di finanziamento, considerato – alla stregua di quanto riconosciuto dalla stessa Commissione europea – che le PMI sono talora esposte a costi di transazione e a condizioni talora più gravose rispetto a quelle praticate alle grandi imprese, in mancanza di sufficienti informazioni per valutare adeguatamente il merito creditizio delle PMI, il rischio di credito e conseguentemente proporre prodotti finanziari su misura.
Un simile *gap* – a parere della Commissione europea - potrebbe essere colmato "attingendo" da altri dati, afferenti anche all'attività commerciale svolta *online* o ai dati tratti da altri settori[63], nonché riconoscendo anche alle PMI la portabilità dei dati in un formato strutturato con il fine di trasferirli ad altri intermediari finanziari, nonché consentire a questi ultimi di accedere ai dati delle PMI tramite API[64].
Ad adiuvandum, i casi d'uso prospettati nell'allegato alla consultazione sono suscettibili di considerazione individuale, ma – ai fini di un credito sostenibile, nell'accezione seguita in questa sede – potrebbero essere considerati in una dimensione complementare.
Così il primo caso d'uso risulta incentrato sulla prestazione di un servizio consulenza creditizia a valore aggiunto, prendendo in considerazione un'ampia gamma di offerte sul mercato ove individuare quella più adeguata al richiedente il credito, il cui profilo sia stato ricostruito sulla scorta di dati pubblici e privati.
Gi stessi dati hanno però una rilevanza biunivoca laddove "le impronte energetiche e climatiche" del cliente (oggetto del secondo *use case*) sono suscettibili di utilizzo nella prospettiva di supportare il cliente medesimo nella transizione ambientale, ma anche per aprire l'accesso ad un ampio spettro di prodotti creditizi basati sui dati ESG[65].
Sul versante parallelo, invece, se gli esiti della valutazione preliminare per la revisione della direttiva 2014/17/UE hanno lasciato emergere la possibilità di adeguare il processo di valutazione del merito creditizio agli obiettivi della politica in materia di cambiamenti climatici e di ambiente (oltre che agli sviluppi in tema di intelligenza arti-

[63] Viene infatti riconosciuto che «*Primary data collection from SMEs during a loan application process is costly and may not deliver all the relevant data. To make sure that the funding provided is appropriate to the economic and financial circumstances of SMEs, credit institutions and other lenders might benefit from the additional access to data, including ecommerce data. Online commercial activity and other cross-sectoral data generally improves the quality of SME creditworthiness assessment and may lead to enhanced financing, with a positive impact on the overall financial health of SMEs*» (cfr. European Commission, *Targeted Consultation on Open Finance framework and data sharing in the financial sector*, cit.).

[64] «*Open finance principles could also be applied to the sharing of data relevant to SME funding applications among funding providers, which is one of the actions under the capital markets union action plan. Credit institutions and alternative providers could allow authorised funding providers to access the relevant SME data via APIs in a standardised and machine-readable format, subject to the SME's consent. Another possibility would be to ensure portability of data in a structured and machine-readable format that SMEs could transfer to other financial intermediaries themselves. In both cases, the data shared would be retrieved from the SME's funding application. By facilitating the sharing of standardised data on SMEs with funding providers, such a scheme would have the potential to help SMEs secure funding while helping funding providers source new clients / investments*».

[65] In particolare, «*the use case is based on ESG Data (EPCs data, utilities Data, airlines and railway data on mobility impact, supply chain data, financial data) to support customers in their environmental transition. It covers banking activity (energy renovation loans proposal for housing classified E, F, G / loan proposal for replacement of oil-fired boilers/ green loans, specialised lending (e.g. commodities finance), leasing, insurance cover, green bonds, comparison and recommendations)*».

ficiale)[66], la vera innovazione potrebbe derivare dal *Technical Advice* che l'EBA entro fine anno fornirà alla Commissione europea sui mutui e prestiti *green*, come parte del lavoro afferente alla Strategia per il finanziamento della transizione all'economia sostenibile, ma con significative ricadute positive sull'accesso al credito da parte di consumatori e PMI e in linea con gli obiettivi sia della *Capital Markets Union*, sia della Strategia europea per gli investimenti *retail*[67].

Tanto discende dal contenuto della *Call for Advice* rivolta all'EBA e dalla relativa *survey*, entrambe dirette ad approfondire principalmente quattro aree tematiche, quali: una panoramica sulle pratiche di mercato diffuse in tema di prestiti *green*; l'introduzione di una definizione di prestito *green* basata sulla tassonomia europea; l'individuazione di misure finalizzate ad incoraggiare l'adozione di prestiti *green* da parte sia dei consumatori che delle PMI; la definizione del processo di erogazione del prestito *green*.

A parte le rilevanti manovre di avvicinamento del percorso di tutela delle PMI a quello dei consumatori, quale finalità dichiarata dell'EBA tra le considerazioni in gioco, il flusso di interventi predetti sembra far propendere per uno nuovo sistematico intervento consumeristico, di cui si stanno gradualmente ponendo le basi, con riguardo ai profili della sostenibilità, che per ora involgono specificamente prestiti e mutui verdi, in un prossimo futuro potrebbero estendersi – in una prospettiva di *Open Finance* – agli altri prodotti finanziari.

Tuttavia, in uno scenario simile, la condivisione dei dati potrebbe conseguire quale effetto (in)diretto quello di generare una sorta di profilo di sostenibilità (i.e. profilo finanziario/creditizio di sostenibilità) del cliente che, a seconda della maggiore o minore impronta ambientale, potrebbe talora trasformarsi in un *boomerang* ed assurgere a nuova scriminante nell'accesso al credito ed ai prodotti del settore.

In particolare, l'accesso e il conseguente riuso dei dati condivisi nell'ambito di un ecosistema finanziario aperto, se per un verso potrebbe in teoria favorire o ampliare, a seconda dei casi, l'accesso al credito (sotto forma di prestiti *green*), per altro verso in mancanza di altri dati, anche di natura non finanziaria a tal fine rilevanti e/o in presenza di profili finanziari basati su dati contrastanti o contraddittori, potrebbero diversamente rendere più costoso il credito richiesto, sino a creare nuove forme di esclusione.

Sebbene la possibilità di accedere a mutui e prestiti *green* attivi indirettamente un processo virtuoso, che spinge su tutti i fronti alla transizione verso un'economia sostenibile, è anche vero che per favorire detta transizione, i crediti sostenibili sono offerti con costi più bassi ed a condizioni privilegiate, al fine di incentivare le scelte creditizie dei richiedenti il credito.

Queste ultime però rischiano di tradursi in una scelta pressoché obbligata, qualora il richiedente rimanesse sprovvisto di altre alternative finanziarie da poter considerare quale termine di confronto, tanto da vedersi precluso ogni altro accesso al credito ordinario[68], in quanto erogato a condizioni economicamente insostenibili e di fatto

[66] In tal senso le conclusioni della Commissione europea, *Relazione della Commissione europea al Parlamento e al Consiglio relativa al riesame della direttiva 2014/17/UE del Parlamento europeo e del Consiglio in merito ai contratti di credito ai consumatori relativi a beni immobili residenziali*, cit.

[67] Si rammenta che l'*Open Finance* rappresenta un funto di forza in entrambi.

[68] A titolo esemplificativo, una situazione del genere potrebbe prospettarsi nel caso in cui il richiedente

inaccessibili a talune fasce di consumatori e PMI.
Tanto vale *a fortiori* nel caso in cui l'accesso ai mutui *green* fosse incentrato non tanto sul profilo creditizio del richiedente il credito, sulla sua capacità prospettica di rimborso del credito e di adempimento agli obblighi contrattuali, bensì sulla connotazione "*green*" del comportamento del cliente (tratto, ad es. dalle informazioni sui relativi consumi energetici), del prestito e della rispondenza dell'attività svolta alla preordinata tassonomia UE.
In definitiva, se in taluni casi quella dei mutui *green* potrebbe rilevare quale via per l'inclusione finanziaria di consumatori e PMI, l'altra faccia della medaglia potrebbe far emergere nuovi criteri di valutazione del merito creditizio, basato in misura crescente sull'impronta ambientale del richiedente il credito e su quella dell'attività eventualmente esercitata.
Infine, elemento non secondario diviene poi quello di prevedere forme di orientamento per consumatori e PMI che, diversamente, rischiano di perdersi nel labirinto delle misure messe in campo, talora accomunate solo da un'etichetta (peraltro non standardizzata, né tanto meno definita), utile a farle ascrivere al mondo *green*. In questo contesto decisivo potrebbe essere il servizio – questo sì a valore aggiunto – prestato da un consulente specializzato e in grado di districarsi nei meandri della sostenibilità[69].

il credito non possa modificare o intervenire sull'immobile, seguendo tutte le indicazioni necessarie per usufruire di un prestito *green* per condizioni strutturali dello stesso immobile che non si prestano al fine indicato o comportano un aggravio di costi nell'ambito del complessivo impegno finanziario.

[69] In tal senso si segnalano le iniziative messe in campo da IASE Italy in direzione di percorsi di specializzazione e di conseguente certificazione ESG delle competenze acquisite dai consulenti, alla stregua di *standard* riconosciuti a livello internazionale.

Dalla Decisione per il rafforzamento della protezione delle informazioni su internet alla Legge sulla tutela delle informazioni personali della RPC "con caratteristiche cinesi"*

Enrico Toti

Abstract

La Cina è uno dei principali attori dell'economia globale che si basa fortemente sulla gestione dei *big data* e sul progresso tecnologico, ed in cui un ristretto numero di attori ne controlla e domina ampi segmenti. Le ragioni ed implicazioni sono molte, anche in considerazione della connessione al tema della sicurezza nazionale, del controllo politico sull'economia volto a garantire la stabilità sociale, e dell'integrità territoriale. Notevoli gli sforzi da parte del legislatore cinese al fine di dotarsi di un apparato normativo in materia di privacy che tenga conto dei modelli preesistenti, in modo particolare di Europa e Stati Uniti, ma che fa proprio un modello in funzione della specifica e complessa realtà del territorio.

China is a major player in the global economy, which heavily relies on big data and technological progress and where a small number of players control and dominate large segments of the economy. The reasons and implications are many, not least in terms of national security, political control over the economy to ensure social stability and territorial integrity. Significant efforts have been made by the Chinese legislator to provide a regulatory apparatus on privacy taking into account pre-existing models, especially those of Europe and the United States, though building its own model according to the specific and complex local reality.

Sommario

Premessa. - 1. Sovranità informatica e autoritarismo digitale in Cina. - 2. Evoluzione normativa. - 3. Il Codice civile cinese, artt. 1032-1039. - 4. Struttura e tratti salienti

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

della Legge sulla tutela delle informazioni personali. - 5. Posizione e ruolo della Legge sulla protezione delle informazioni personali all'interno dell'ordinamento. La coerenza del sistema. - 6. Diritto alla riservatezza e tutela delle informazioni personali. - 7. Lo specifico ambito delle informazioni personali sensibili. - 8. Privacy con caratteristiche cinesi.

Keywords

autoritarismo digitale - codice civile cinese - diritto alla riservatezza - Cina - dati sensibili

Premessa

La Cina è uno dei principali attori dell'economia globale che si basa fortemente sulla raccolta e gestione dei big data e sul progresso tecnologico, in cui un ristretto numero di operatori controlla e domina ampi segmenti del mercato. La protezione delle informazioni personali, la maggior parte delle quali viene veicolata attraverso la rete, è fondamentale per mantenere integra la fiducia delle persone, anche come consumatori, delle imprese e di tutti i protagonisti di questa economia, al fine di garantire una concorrenza leale sul mercato, allineare la Cina alle tendenze mondiali, mantenere fede all'impegno assunto di diventare un leader tecnologico, con particolare attenzione ai servizi digitali innovativi e al commercio elettronico. Le ragioni ed implicazioni sono molte, anche in considerazione della connessione al tema della sicurezza nazionale ed in alcune fasi del controllo politico sull'economia volto a garantire la stabilità sociale, l'integrità territoriale e la guida del governo sullo sviluppo economico[1].

Illuminante, a mio parere, per inquadrare e comprendere la materia è la Spiegazione della Bozza della Legge sulla protezione delle informazioni personali della Repubblica Popolare Cinese (中华人民共和国个人信息保护法 (草案) 的说明) pronunciata da Liu Junchen (刘俊臣) Vicedirettore della Commissione per gli Affari Legislativi del Comitato permanente dell'Assemblea Popolare Nazionale, il 13 ottobre 2020 nel corso della Ventiduesima Sessione del Comitato permanente della Dodicesima Assemblea Popolare Nazionale, in cui sono riportate riflessioni degne di nota e, nel medesimo tempo, per porre le basi della decodificazione e comprensione del testo normativo della Legge[2]. Riporto la traduzione, a mia cura, di alcune parti della Spiegazione:

> «Con la continua e profonda integrazione dell'informatizzazione e della società economica, la rete è diventata un nuovo spazio di produzione e di vita, un nuovo motore per lo sviluppo economico e un nuovo strumento per la comunicazione e la cooperazione. A marzo 2020, gli utenti internet del mio paese hanno raggiunto i 900 milioni, ci sono più di 4 milioni di siti internet e più di 3 milioni di applicazioni. La raccolta e l'uso delle informazioni personali è sempre più ampia. Sebbene

[1] R. Bertinelli, *Economia e politica nella Cina contemporanea*, Roma, 1990.

[2] Il testo è disponibile in The National Peolple's Congress of the People's Republic of China.

la protezione delle informazioni personali del mio paese sia stata continuamente rafforzata negli ultimi anni, nella vita reale alcune aziende, istituzioni e persino individui, a partire da interessi commerciali, raccolgono casualmente, ottengono illegalmente, abusano e scambiano illegalmente informazioni personali. Questioni quali la sicurezza abitativa delle persone e il pericolo per la vita, la salute e la sicurezza della proprietà delle persone sono ancora molto importanti. Nell'era dell'informazione, la protezione delle informazioni personali è diventata uno degli interessi più diretti e pratici del grande pubblico. Vari aspetti della società hanno ampiamente richiesto l'introduzione di una legge speciale sulla protezione delle informazioni personali. […] Il Comitato centrale del Partito attribuisce grande importanza alla costruzione dello stato di diritto nel ciberspazio […] Il segretario generale Xi Jinping ha ripetutamente sottolineato che dobbiamo aderire al principio della sicurezza della rete per le persone, garantire la sicurezza delle informazioni personali e salvaguardare i diritti e gli interessi legittimi dei cittadini nel ciberspazio, proporre requisiti chiari per rafforzare la protezione delle informazioni personali. Al fine di rispondere tempestivamente alle voci e alle aspettative del pubblico in generale […] è di grande importanza formulare una legge speciale sulla protezione delle informazioni personali.

In primo luogo, la formale emanazione della Legge è un requisito per rafforzare ulteriormente la protezione giuridica delle informazioni personali. Dal 18° Congresso Nazionale del Partito Comunista Cinese, l'Assemblea Popolare Nazionale e il suo Comitato Permanente hanno stabilito le regole principali per la protezione delle informazioni personali di cui il rafforzamento della protezione delle informazioni di rete è parte, quali la Legge sulla sicurezza della rete e la Legge sul commercio elettronico, emendando al contempo la Legge sulla tutela dei consumatori. Nella revisione del diritto penale, è stato migliorato il sistema normativo per punire i reati comportanti la violazione delle informazioni personali; nella compilazione del Codice civile, le informazioni personali sono protette dalla legge come un importante diritto civile. Il sistema normativo di protezione delle informazioni personali del mio Paese è stato gradualmente stabilito, ma è ancora difficile adeguarlo alla realtà del rapido sviluppo dell'informatizzazione e alle crescenti esigenze delle persone per una vita migliore. Pertanto, le leggi speciali dovrebbero essere formulate e promulgate sulla base delle leggi esistenti per migliorare la sistematicità, la pertinenza e l'operatività delle norme, dar vita ad un sistema più completo e fornire una tutela più forte in termini di protezione delle informazioni personali.

In secondo luogo, la formulazione di una Legge sulla protezione delle informazioni personali è un'esigenza pratica per mantenere una buona ecologia nel ciberspazio. Il ciberspazio è la casa comune di centinaia di milioni di persone e deve operare sul binario dello stato di diritto. La raccolta e l'uso illegale di informazioni personali e altre attività non solo danneggiano gli interessi vitali delle persone, ma mettono anche in pericolo la sicurezza delle transazioni, interrompono la concorrenza di mercato e turbano l'ordine del ciberspazio. Pertanto, dovrebbero essere formulate leggi speciali per regolamentare le attività di elaborazione delle informazioni personali con sistemi rigorosi, standard rigorosi e responsabilità rigorose,

> fissare obblighi e responsabilità dei responsabili del trattamento delle informazioni personali.
> In terzo luogo, la formulazione di una Legge sulla protezione delle informazioni personali è una misura importante per promuovere il sano sviluppo dell'economia digitale. Al momento, l'economia digitale quale nuovo fattore di produzione è in forte espansione e la concorrenza sui dati è diventata un campo importante della concorrenza internazionale e i dati sulle informazioni personali sono il nucleo e il fondamento dei big data. Il rapporto del Diciannovesimo Congresso Nazionale del Partito comunista cinese ha presentato i requisiti del compito per costruire un paese forte nella rete, una Cina digitale e una società intelligente. In base a questo requisito, la protezione e l'utilizzo delle informazioni personali devono essere coordinate a livello di sistema, regole, diritti e responsabilità chiari, la protezione deve essere efficace.
> […]
> La redazione della Legge sulla protezione delle informazioni personali è stata inclusa nella Programmazione legislativa e nel Piano di lavoro legislativo annuale del Comitato permanente della Tredicesima Assemblea Popolare Nazionale.
> […]
> Il lavoro di redazione presta attenzione ai seguenti punti: in primo luogo, combinare le condizioni nazionali e attingere all'esperienza internazionale».

Nonostante questi intenti, sforzi e progressi, sono ancora diverse le questioni non risolte in Cina in materia di privacy. Il crescente uso della tecnologia da parte del governo, si pensi all'utilizzo di sistemi di riconoscimento facciale[3] e di analisi dei big data che possono essere utilizzati per tracciare e monitorare le persone, seppur indicato come necessario per la sicurezza nazionale, accresce la preoccupazione da parte dei cittadini per il potenziale abuso di queste misure e la conseguente violazione della propria privacy[4].

La regolamentazione sulla protezione delle informazioni personali in Cina è assai recente a differenza dell'Unione europea e degli Stati Uniti, che vantano modelli ben consolidati: il modello dell'Unione europea, infatti, riconosce la riservatezza e la tutela delle informazioni personali quali diritti fondamentali, la normativa ha un vasto spettro di applicazione, la definizione di dati personali è assai ampia e molte sono le garanzie di protezione offerte. Negli Stati Uniti, diversamente, non esiste una normativa unitaria che disciplini la materia nella sua interezza, ma le disposizioni sono frammentate in fonti primarie e secondarie e la protezione risulta nel complesso meno

[3] V. L. Wang *Face Recognition in Law Enforcement: A Comparative Analysis of China and the United States*, in *Open Journal of Social Sciences*, 2021, 9; Y. Liu – W. Yan – B. Hu, *Resistance to Facial Recognition Payment in China: The Influence of Privacy-Related Factors*, in *Telecommunications Policy*, 45, 2021, 5.

[4] Riguardo alla vaghezza della normativa cinese che vieta contenuti internet, v. F. Proutè, *Censoring Pornography, the role of sexual media in the fight for freedom of expression in the People's Republic of China*, in *Mapping China Journal*, 2018, 135 ss.; G. Kostka - L. Steinacker - M. Meckel, *Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States*, in *Public Understanding of Science*, 30(6), 2021, 671 ss.; G. Santoni, *La Cina e lo spazio digitale. Questioni di governance nello spazio digitale globale*, in *Orizzonte Cina*, 11, 2020, 70 ss.; S. Del Gatto, *Il riconoscimento facciale in Cina. Interviene la Corte Suprema*, in *IRPA*, 2021.

efficace se paragonata a quella europea. La Cina, come è accaduto per altri settori del diritto, tiene in debita considerazione modelli precedentemente elaborati e, considerata la delicatezza della materia, e le specifiche caratteristiche del contesto, ha proceduto ad elaborare la normativa con gradualità. Ad una prima fase, caratterizzata da una regolamentazione frammentaria e non sempre coordinata, è seguita l' elaborazione di un testo legislativo unitario e comprensivo della disciplina dell'intero settore in cui, come si vedrà più avanti, emergono le peculiarità proprie del contesto sociale e politico.
Il presente contributo, alla luce di quanto sopra anticipato, facendo riferimento ad una ampia bibliografia[5], intende esaminare solo alcuni specifici profili che, a parere dello scrivente, raccolgono l'attenzione degli studiosi e degli esperti della materia: ai paragrafi introduttivi, necessari a fornire un quadro chiaro del contesto e dei testi normativi di riferimento, segue una seconda parte volta ad affrontare alcune importanti e poco note questioni per far emergere la configurazione del modello concepito dal legislatore cinese.
I testi utilizzati a conforto del presente lavoro sono, come di consueto, principalmente in lingua cinese, al fine di avvicinare, per quanto possibile, il lettore alla mentalità del legislatore cinese ed analizzarne dal più fedele angolo visuale le diverse implicazioni.

1. Sovranità informatica e autoritarismo digitale in Cina

Negli ultimi anni in Cina è stata avvertita l'esigenza di creare un adeguato impianto normativo che fosse in grado di garantire la sicurezza del trattamento delle informazioni personali in un più ampio ecosistema normativo[6]. I testi di riferimento sono la Legge sulla sicurezza della rete della Repubblica Popolare Cinese (*Cyber security La*w, CSL, 中华人民共和国网络安全法) promulgata il 7 novembre 2016, in vigore dal 1° giugno 2017 la cui finalità è fissata dall'art.1:

> «La presente legge è elaborata al fine di garantire la sicurezza informatica, di proteggere la sovranità del ciberspazio, la sicurezza nazionale e l'interesse pubblico, di salvaguardare i legittimi diritti ed interessi dei cittadini, delle persone giuridiche e delle altre organizzazioni e di promuovere un sano sviluppo dell'informatizzazione dell'economia e della società».

La Legge sulla sicurezza dei dati della Repubblica Popolare Cinese (*Data security Law*, DSL, 中华人民共和国数据安全法) promulgata il 10 giugno 2021, in vigore dal 1° settembre 2021 la cui finalità è fissata dall'art. 1:

[5] Per una prima bibliografia della Legge sulla tutela delle informazioni personali della Repubblica Popolare Cinese, P. De Hert - E. Papakonstantinou, *The Data Protection Regime in China*, in *Brussels Privacy Hub Working Paper,* 1, 2015, 1 ss.; E. Pernot-Leplay, *China's approach on data privacy flaw: a third way between the US and the EU?* in *Penn State Journal of Law & International Affa*ir, 2020, 49 ss.

[6] I. Calzada, *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)*, in *Smart Cities*, 5, 2022, 1129 ss.

> «Questa Legge è promulgata per regolare le attività di elaborazione dei dati, garantire la sicurezza dei dati, promuovere l'elaborazione e l'utilizzo dei dati, proteggere I diritti e gli interessi legittimi degli individui e delle organizzazioni, e salvaguardare la sovranità, la sicurezza e gli interessi di sviluppo dello Stato».

La Legge sulla tutela delle informazioni personali (Personal Information Protection Law, PIPL, 中华人民共和国个人信息保护法) promulgata il 20 agosto 2021, in vigore dal 1° novembre 2021 la cui finalità è fissata dall'art. 1:

> «Questa legge è emanata in conformità con la Costituzione per proteggere i diritti e gli interessi delle informazioni personali, disciplinare il trattamento dei dati personali e promuovere l'uso ragionevole delle informazioni personali».

Tale ecosistema deve essere compreso alla luce del principio dell'autoritarismo digitale[7] esercitato dalla Cina attraverso la progressiva costituzione di un consistente numero di strumenti e organi di sorveglianza sottoposti al controllo ed alla supervisione dell'Amministrazione per la sicurezza del ciberspazio (*Cyberspace Administration of China*, *CAC*)[8]. Il controllo governativo della rete ha previsto la creazione del *Great Firewall*[9], ossia una struttura di leggi, software e forme di controllo realizzata allo scopo di sorvegliare, intercettare e bloccare le trasmissioni di dati che risultino in contrasto con le direttive governative, gestendo in tal modo la circolazione dei dati in generale e la loro fuoriuscita dai confini nazionali[10]. Sotto la guida politica di Xi Jinping l'attività di controllo del governo cinese sulle persone è stata ulteriormente estesa, sono stati implementati meccanismi informatici di valutazione dell'affidabilità dei cittadini attraverso il sistema di credito sociale (*social credit system*, 社会信用体系, *shèhuì xìnyòng tǐxì*) . La Cina è contestualmente diventava uno dei leader mondiali nel settore tecnologico, grazie a politiche di settore quali la *National IT Development Strategy*, *Made in China 2025* e la *China Standards 2035*, inoltre le tecnologie utilizzate da parte del governo sono al centro della Via della Seta digitale (*Digital Silk Road*) e costituiscono una delle punte di diamante del settore export del Paese. In particolare, esse sono oggetto di numerosi accordi commerciali con paesi del Nord Africa e del Medio Oriente[11] che

[7] Con il termine "autoritarismo digitale" si intende «l'uso delle tecnologie dell'informazione digitale da parte di regimi autoritari al fine di sorvegliare, reprimere e manipolare la popolazione locale e straniera» secondo la definizione di A. Polyakova - C. Meserole, *Exporting digital authoritarianism*, in *Brookings Institute Foreing Policy Reports*, 2019. Sul tema Qiang X., *Chinese Digital Authoritarianism and Its Global Impact*, in *Digital Activism and Authoritarian Adaptation in the Middle East*; A.N. Liaropoulos, *Digital Authoritarianism "Made in China": Installing a Digital Dystopia*, 23, 1, 2022, 124 ss.

[8] W. Miao - W. Lei, *Policy review: The Cyberspace Administration of China*, in *Global Media and Communication*, 12, 2016, 337 ss.

[9] S. Chandel - Z. Jingji - Y. Yunnan - S. Jingyao - Z. Zhipeng, *The Golden Shield Project of China: A Decade Later - An In Depth Study of the Great Firewall*, in *Conference proceeding of 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Guilin, China, 2019, 111 ss.

[10] X. Qiang, *Chinese Digital Authoritarianism and Its Global Impact*, in *Digital Activism and Authoritarian Adaptation in the Middle East*, 2021, 35 ss.; J. Rudolph, *Sharper Eyes: Surveilling the Surveillers (Part 1)*, in *China Digital Times*, 2019.

[11] M. Chen - J. Grossklags, *Social Control in the Digital Transformation of Society: A Case Study of the Chinese*

si candidano a divenire, in un prossimo futuro, i nuovi esponenti dell'autoritarismo digitale sul modello cinese[12].
Importanti le considerazioni di Rogier Creemers che ben sintetizzano il quadro attuale:

> *«[…] Chinese legislation and regulation are inextricably linked with the "bigger picture" (daju) of the project that the Chinese Communist Party aims to achieve. Overall, its major objectives are restoring China to a position of wealth and strength (fuqiang), but the specific policy implications of this have varied and evolved over time. In 2014, Xi Jinping announced a drive to turn China into a "cyber power" (wangluo daguo) through the combination of informatization, the introduction of digital technologies in social, economic, and political life, and cybersecurity. In other words, informatization is concerned with the realization of positive plans and policies that leverage digital capabilities for national development goals, which include economic growth and effective governance, applied by both the state and private actors [..]*»[13].

2. Evoluzione normativa

La cultura cinese, sin dall'antichità, ha anteposto l'interesse del gruppo agli interessi dell'individuo sottolineando la posizione subordinata del singolo al gruppo, scelta confermata dal Confucianesimo nel seguente passo "修身,齐家,治 国平天下"[14] in cui prevale il contributo alla famiglia, allo Stato, alla collettività: la riservatezza risiede principalmente nell'unità familiare, distinta dallo Stato[15]. Successivamente, a seguito dei mutamenti sociali a livello globale, anche in Cina, l'individuo ha acquisito un ruolo centrale nella società, non solo come cittadino[16].
Si è intenzionalmente scelto, quale punto di partenza della ricognizione della materia, il periodo della riforma economica cinese in funzione dell'apertura della Cina al resto del mondo, tramite la Politica della porta aperta varata da Deng Xiaoping sotto l'attento controllo del Partito Comunista Cinese[17]. Al fine di sostenere ed accrescere il sistema economico, la Cina ha accolto parziali forme di de-collettivizzazione dell'agricoltura, ha fatto ricorso ad un massiccio ingresso di investimenti stranieri, ha proceduto alla privatizzazione di numerose aziende statali, ha monitorato e gestito l'emersione

Social Credit System, in *Soc. Sci.,* 2022, 11*,* 229 ss.

[12] J. Kurlantzick, *China's Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom?* in *The Diplomat*, 2020.

[13] Sulla Via della seta digitale e per una prima bibliografia, di interesse *Assessing China's Digital Silk Road Initiative*, in *Council on Foreign Relations.*

[14] R. Creemers, *China's emergin data protection framework*, in *Journal of Cybersecurity*, 2022, 1 ss.

[15] Il passo, contenuto nel Grande insegnamento (大学 *dàxué*), è uno dei principi centrali dell'antica filosofia confuciana ed è stato citato dal Presidente Xi Jinping nel 2014, *The governance of China*, Beijing, 2014, 187.

[16] Y. Yan, *The Chinese path to individualization*, in *The British Journal of Sociology*, 2010, 489 ss.

[17] Sull'emersione del quadro normativo della protezione dei dati in Cina riguardo a singoli periodi e per indicazioni bibliografiche R. Creemers, *China's emerging data protection framework*, cit.

del mercato dei capitali[18]. Le riforme si sono, quindi, concentrate sull'incentivazione degli individui a partecipare in modo attivo alla costruzione economica, valorizzando la crescita del benessere individuale accanto a quello della collettività[19]. Ciò è stato accompagnato da una progressiva, seppur lenta, protezione dei diritti dei singoli, incluso quello alla riservatezza. A tale cambiamento ha contribuito, non solo per far fronte alle istanze dei governi esteri, l'adesione della Cina alla WTO[20], alle organizzazioni internazionali ed una crescente interazione con l'Occidente[21].

Dal 2012 sono stati molteplici gli interventi normativi settoriali relativi alla protezione dei dati personali[22] e gli sforzi del legislatore cinese hanno portato a risultati significativi, in particolar modo nel settore creditizio e della sicurezza informatica, tra i quali: la Decisione per il rafforzamento della protezione delle informazioni su internet (*Resolution to Strengthen the Protection of Information on the Internet*, 全国人民代表大会常务委员会关于加强网络信息保护的决定) pubblicata il 28 dicembre 2012[23]; il Regolamento sull'amministrazione del settore dell'informazione creditizia (*Regulation on Credit Information Industry Administration*, 征信业管理条例) sul modello americano del Fair Credit Reporting Act , pubblicato il 21 gennaio 2013 ; la Decisione del Comitato permanente dell'Assemblea Popolare Nazionale sulla revisione della Legge della Repubblica Popolare Cinese sulla tutela dei diritti e degli interessi dei consumatori (*Decision of the Standing Committee of the National People's Congress on Revision of the Law of the People's Republic of China on the Protection of Rights and Interests of Consumers,* 全国人民代表大会常务委员会关于修改《中华人民共和国消费者权益保护法》的决定) del 25 ottobre 2013 in cui è riconosciuta la protezione delle informazioni personali dei consumatori [24].

Nel 2015 il IX emendamento alla Legge Penale della Repubblica Popolare Cinese (*Ninth Amendment to the People's Republic of China's Criminal Law*, 中华人民共和国刑法修正案-九) ha stabilito che chiunque venda o fornisca informazioni personali a terze parti, in violazione della legge, è soggetto a responsabilità penale. La previsione della

[18] Sul tema con valutazioni critiche ad opera di autori cinesi, v. W. Mengkui, *China's Economic Transformation Over 20 Years*, Beijing, 2000; C. Fulin, *China's Economic Reform at the Turn of the Century*, Beijing, 2000; C. Fulin, *China. The New Stage of Reform*, Beijing, 2004; F. Spigarelli, *Politica industriale e cambiamenti strutturali: la via cinese alla crescita*, in *L'industria. Rivista di economia e politica industriale*, 2018, 511 ss.

[19] S. L. Nah - J. Wong, *China's Emerging New Economy: The Internet and E-Commerce*, Singapore, 2000, 1 ss.; I. Claus – L. Oxley, *China's Economy: A Collection of Surveys*, New Jersey, 2015, 1 ss.; J.A.G. Roberts, *Storia della Cina. La politica, la realtà sociale, la cultura, l'economia dall'antichità ai nostri giorni*, Roma, 2002, 590 ss.

[20] T. Cheek, *Vivere le riforme. La Cina dal 1989*, Torino, 2008, 119: «L'esperienza della riforma non è affatto uniforme, né nella Cina nel suo complesso, né all'interno di una singola comunità . In larga misura, le reazioni ai suoi effetti si possono suddividere, semplicemente, in risposte dei vincitori e risposte dei perdenti».

[21] S. Chiarlone - A. Amighini, *L'economia della Cina*, Roma, 2007, 71 ss.

[22] E.W Capen, *The Western Influence in China*, in *The Journal of Race Development*, 1913, 412 ss. Per una attenta ricostruzione in chiave storica del quadro regoalmentare di internet in Cina, v. M. Weishan – H. Zhu – Z. Chen, *Who's in charge of regulating the internet in China: the history and evolution of China's internet regulatory agencies*, in *China Media Research*, 2018.

[23] Le normative analizzate nel paragrafo sono reperibili in lingua originale nel sito del Consiglio degli Affari di Stato della Repubblica Popolare Cinese.

[24] Il testo in lingua cinese è disponibile sul sito internet della SAMR.

pena è maggiore quando l'attività illecita è compiuta nell'esercizio dei propri doveri[25]. Nel Maggio 2017 sono stati individuati alcuni standard nazionali di classificazione dei sistemi di sicurezza informatica sulla base di requisiti tecnici e gestionali: Specificazioni relative alla sicurezza delle informazioni personali (GB/T 35273-2020) (*Information Security Technology - Personal Information Security Specification (GB/T 35273-2020)*, 信息安全技术 个人信息安全规范) successivamente emendate il 6 marzo 2020 ed in vigore dal 1° ottobre 2020[26]; Linee Guida per la protezione della sicurezza delle informazioni personali su internet (*Guidelines for the Protection of Personal Information Security on Internet,* 互联网个人信息安全保护指南) pubblicate dal Ministero della Pubblica Sicurezza il 10 aprile 2019 che, pur non avendo carattere coercitivo costituiscono riferimento della materia[27]; Regolamento sulla protezione della sicurezza delle infrastrutture critiche informatizzate (*Critical Information Infrastructure Security Protection Regulations*, 关键信息基础设施安全保护条例) pubblicato il 27 aprile 2021 ed in vigore dal 1° settembre 2021. Accanto al formante legislativo è emerso, in via marginale, il formante giurisprudenziale, per cui si menzionano due decisioni, seppur non recentissime, in grado di aiutare a meglio comprendere il quadro regolamentare: nel 2014, la Corte Suprema del Popolo si è pronunciata con le Disposizioni della Corte Suprema del Popolo su diverse questioni relative all'applicazione della legge nei processi civili che coinvolgono l'uso delle reti informatiche per la violazione dei diritti e degli interessi personali (最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定) riconoscendo la tutela del nome, dell'immagine, della reputazione e dell'onore, oltre che dei dati personali dei cittadini cinesi; nel 2017, con le Interpretazione della Corte Suprema del Popolo e della Procura Suprema del Popolo su diverse questioni riguardanti l'applicazione della legge nella gestione di casi penali di violazione delle informazioni personali dei cittadini (最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解)[28].

La Cina ha, pertanto, ritenuto opportuno dotarsi di un apparato normativo efficace e moderno, collegandolo ad alcuni riferimenti normativi preesistenti, primi fra tutti, l'art. 40 della Costituzione del 1982[29], l'art. 252 del Codice penale[30], l'art. 101 dei Prin-

[25] Il testo in lingua cinese della Decisione è disponibile nel sito internet del Consiglio degli Affari di Stato della Repubblica Popolare Cinese.

[26] Per una approfondita disamina del testo delle Specificazioni relative alla sicurezza delle informazioni personali, J. Wizhi, *Breve analisi del valore della versione 2020 delle Specificazioni per la sicurezza delle informazioni personali nell'orientare le politiche aziendali di protezione delle informazioni personali*.

[27] Le "Linee guida" stabiliscono in modo esaustivo i requisiti di attuazione che devono essere rispettati dalle imprese per la protezione delle informazioni personali in termini di misure di gestione, impostazioni del personale, raccolta e utilizzo delle informazioni, archiviazione, condivisione e risposta agli incidenti e si sovrappongono parzialmente ai contenuti delle "Principali norme di sicurezza" ed altri documenti.

[28] I testi in lingua cinese sono disponibili nel sito della Corte Suprema del Popolo della Repubblica Popolare Cinese.

[29] Art. 40: «La libertà e la riservatezza relativa alla corrispondenza dei cittadini della Repubblica Popolare Cinese sono protette dalla legge. Nessuna organizzazione o individuo può, per nessun motivo, violare la libertà e la riservatezza della corrispondenza dei cittadini, salvo nei casi in cui, per soddisfare le esigenze della sicurezza dello Stato o delle indagini penali, gli organi di pubblica sicurezza o i procuratori sono autorizzati a censurare la corrispondenza secondo le procedure previste dalla legge».

[30] Art. 252: «Chiunque nasconde, distrugge o apre illecitamente una corrispondenza altrui, violando

cipi generali del diritto civile, questi ultimi abrogati con l'ingresso del Codice civile, ed istituendo una pluralità di autorità deputate al funzionamento dell'intero sistema. Su questo complesso quadro regolamentare poggiano le basi le tre leggi, precedentemente menzionate, che ne costituiscono i pilastri, integrate da fonti ulteriori che lo completano e ne consentono la concreta attuazione[31].

così il diritto del cittadino alla libertà di corrispondenza, se le circostanze sono gravi, è condannato alla reclusione a tempo determinato non superiore a un anno o alla detenzione penale».

[31] Accanto alla molteplicità di autorità coinvolte, sempre alla luce di meglio comprendere l'ecosistema normativo, si è ritenuto opportuno riportare, per completezza, una serie di fonti poche note che regolamentano la materia al fine di predisporre un quadro il più esauriente possibile: Linee guida per la protezione delle informazioni personali su Internet 2019 (*Guidelines on Internet Personal Information Security Protection*, 2019, 互联网个人信息安全保护指南) pubblicate dal Ministero della Pubblica Sicurezza il 19 aprile 2019 con effetti a decorrere dal 19 aprile 2019; Disposizioni sulla protezione online dei dati personali dei bambini (*Provisions on Online Protection of Children's Personal Information*, 2019, 儿童个人信息网络保护规定) pubblicate dall'Amministrazione per la sicurezza del ciberspazio il 22 agosto 2019 con effetti a decorrere dal 1° ottobre 2019; Tecnologia di protezione delle informazioni - Guida per l'anonimizzazione dei dati personali (*Information Security Technology - Guide for De-identifying Personal Information* -GB/T37964-2019 - 信息安全技术†- 个人信息去标识化指南) pubblicate dal Comitato tecnico nazionale per la standardizzazione della sicurezza delle informazioni (TC 260) il 30 di agosto 2019 con effetti a decorrere dal 1° marzo 2020; Avviso sulla protezione dei dati personali e utilizzazione di Big data per sostenere gli sforzi congiunti per la prevenzione e il controllo del COVID-19, 2020 (*Notice on Ensuring Personal Information Protection and Utilization of Big Data to Support Joint Efforts for COVID-19 Prevention and Control, 2020,* 做好个人信息保护利用大数据支撑联防联控工作的通知) pubblicato dall' Amministrazione per la sicurezza del ciberspazio il 4 febbraio 2020 con effetti a decorrere dal 4 febbraio 2020; Specifiche tecniche sulla protezione delle informazioni finanziarie personali, 2020 (*Personal Financial Information Technical Protection Specification, JR/T0171-2020*, 个人金融信息技术保护规范) pubblicate dalla Banca popolare cinese il 13 febbraio 2020 con effetti a decorrere dal 13 febbraio 2020; Tecnologia per la sicurezza delle informazioni - Specifiche per la sicurezza delle informazioni personali (*Information Security Technology - Personal Information Security Specification - GB/T 35273-2020*- 信息安全技术†- 个人信息安全规范), pubblicate dal Comitato tecnico nazionale per la standardizzazione della sicurezza delle informazioni (TC 260) il 6 marzo 2020 con effetti a decorrere dal 1° ottobre 2020, in sostituzione della versione pubblicata il 29 dicembre 2017; Misure attuative per la protezione dei diritti e degli interessi dei consumatori finanziari (*Implementing Measures for Protection of the Rights and Interests of Financial Consumers, 2020*, 中国人民银行金融消费者权益保护实施办法) pubblicate dalla Banca popolare cinese il 15 settembre 2020 con effetti a decorrere dal 1° novembre 2020; Tecnologia di protezione delle informazioni - Guida alla valutazione dell' impatto sulla sicurezza dei dati personali (*Information Security Technology - Security Impact Assessment Guide of Personal Information, GB/T 39335-2020*, 信息安全技术†- 个人信息安全影响评估指南), pubblicate dal Comitato tecnico nazionale per la standardizzazione della sicurezza delle informazioni (TC 260) il 19 novembre 2020 con effetti a decorrere dal 1° giugno 2021; Disposizioni su diverse questioni riguardanti l'applicazione della legge nel processo di cause civili relative all'uso della tecnologia di riconoscimento facciale per il trattamento dei dati personali, 2021 (*Provisions on several issues concerning the application of law in the trial of civil cases related to the use of facial recognition technology to process personal information*, 2021, 审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定) pubblicate dalla Corte suprema del popolo il 27 luglio 2021 con effetti a decorrere dal 1° agosto 2021; Misure per la gestione dei servizi di indagine creditizia, 2021 (*Measures for Credit Investigation Services Management, 2021*, 征信业务管理办法) pubblicate dalla Banca popolare cinese il 17 settembre 2021 con effetti a decorrere dal 1° gennaio 2022; Disposizioni sulla gestione della raccomandazione algoritmica nel servizio di informazione su Internet, 2021 (*Provisions on Administration of Algorithmic Recommendation in the Internet Information Service, 2022*, 互联网信息服务算法推荐管理规定) pubblicate congiuntamente dall' Amministrazione per la sicurezza del ciberspazio, dal Ministero per l'industria e l'informazione tecnologica, Ministero della Pubblica Sicurezza e l'Amministrazione statale per la regolamentazione del mercato il 1° marzo 2022 con effetti a decorrere dal 1° marzo 2022; Tecnologia di protezione delle informazioni - Specifica sulla valutazione del rischio per la sicurezza delle informazioni (*Information Security Technology - Risk Assessment method for Information Security*, 信息安全技术信息安全风险评估方法) pubblicata dal Comitato tecnico nazionale per la standardizzazione della sicurezza delle informazioni (TC 260) il 15 aprile 2022 con

A capo delle autorità garanti del corretto funzionamento del quadro normativo rinveniamo l'A Amministrazione per la sicurezza del ciberspazio (*Cyberspace Administration of China,* CAC, 国家互联网信息办公室)[32] a cui si affiancano il Ministero della Pubblica Sicurezza (*Ministry of Public Security*, MPS, 公安部)[33], il Ministero per l'Industria e l'Informazione Tecnologica (*Ministry of Industry and Information Technology,* MIIT, 国家

effetti a decorrere dal 1° novembre 2021; Pareri su diversi problemi relativi all'applicazione della legge nel giudizio di cause penali (*Opinions on Several Issues in the Application of Criminal Procedures in Handling Cases of Information Network Crimes*, 2022, 最高人民法院 最高人民检察院 公安部关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见), pubblicati congiuntamente dalla Corte suprema del popolo, dalla Procura suprema del popolo e dal Ministero della Pubblica Sicurezza il 26 agosto 2022, con effetti a decorrere dal 1° settembre 2022; Tecnologia di protezione delle informazioni - Linee guida per l'ingegnerizzazione della protezione dei dati personali [*Information Security Technology - Guidelines for personal information security engineering* (GB/T 41817-2022) 信息安全技术†- 个人信息安全工程指南) (征求意见稿], pubblicate il 14 ottobre 2022 con effetti a decorrere dal 1° maggio 2023; Legge sul commercio elettronico, 2018 (*Electronic Commerce Law, 2018,* 电子商务法), promulgata il 31 agosto 2018, in vigore dal 1° gennaio 2019; Interpretazioni su diverse questioni riguardanti l'applicazione della legge nella gestione dei giudizi penali, quale la questione dell'uso illegale delle reti informatiche e del sostegno alle attività criminali informatiche, 2019 (*Interpretations on Several Issues concerning the Application of Law in Handling Criminal Cases such as Making Illegal Use of Information Networks and Assisting Information Network Criminal Activities*, 2019, 办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释), pubblicate di concerto dalla Corte suprema del popolo e dalla Procura suprema del popolo con effetti a decorrere dal 1° novembre 2019; Misure per la valutazione della sicurezza del trasferimento transfrontaliero dei dati (*Measures on Cross-Border Data Transfer Security Assessment,* 数据出境安全评估办法) pubblicate dall' Amministrazione per la sicurezza del ciberspazio il 7 luglio 2022, con effetti a decorrere dal 1° settembre 2022; Contratto standard per il trasferimento transfrontaliero di informazioni personali (*Standard contract for cross-border transfer of personal information* 个人信息出境标准合同) e Misure definitive sul contratto standard per il trasferimento transfrontaliero di informazioni personali *(Final version of the Measures for the Standard Contract for Cross-Border Transfer of Personal* 个人信息出境标准合同办法) pubblicate dall' Amministrazione per la sicurezza del ciberspazio il 22 febbraio 2023 con effetti a decorrere dal 1° giugno 2023; Guida pratica agli standard di sicurezza di rete - Specifiche tecniche per la certificazione di sicurezza del trattamento transfrontaliero delle informazioni personali (*Network Security Standards Practice Guide - Technical Specifications for the Security Certification of Personal Information Cross-Border Processing,* 网络安全标准实践指南—个人信息跨境处理活动安全认证规范) pubblicata il 16 marzo 2023 da parte del Comitato Tecnico Nazionale per la Standardizzazione della Sicurezza Informatica (TC260), in aggiornamento rispetto alla precedente versione del 24 giugno 2022 la cui finalità è di fornire ai responsabili del trattamento delle informazioni personali maggiore chiarezza riguardo alle aspettative delle autorità cinesi in merito alle modalità di trasferimento transfrontaliero dei dati in conformità con la legge sul trattamento dei dati personali.

[32] L' Amministrazione per la sicurezza del ciberspazio (国家互联网信息办公室, *Cyberspace Administration of China,* CAC), fondata nel 2011, opera a partire dal 2014 sotto la diretta supervisione del Gruppo dirigente centrale per gli affari del ciberspazio (中共中央网络安全和信息化领导小组办公室, *Central Leading Group for Cyberspace Affairs*). L'Amministrazione è responsabile della sicurezza del ciberspazio e della regolamentazione dei contenuti di internet; le sue funzioni principali sono: la direzione, il coordinamento e la supervisione della gestione dei contenuti online e la gestione della procedura amministrativa di autorizzazione per le imprese operanti nel campo della informazione online.

[33] Il Ministero della Pubblica Sicurezza (公安部,*Ministry of Public Security*, MPS), istituito nel 1954, è la principale autorità cinese per la sicurezza pubblica nazionale. Si occupa della prevenzione e dell'investigazione sulle attività illegali, criminali e terroristiche, della salvaguardia della sicurezza pubblica e dell'ordine sociale, oltre ad essere coinvolto nella gestione dell'immigrazione, della registrazione di famiglie e carte d'identità dei residenti, nella gestione di assemblee, cortei e manifestazioni e ad essere responsabile della sicurezza della rete di informazione pubblica. Inoltre, svolge una generica funzione di coordinamento degli altri organi statali, delle organizzazioni pubbliche, imprese e istituzioni che operano nell'ambito della sicurezza pubblica. Il sito web del Ministero della Pubblica sicurezza è disponibile qui.

市场监督管理总局), l'Amministrazione Statale per la Regolamentazione del Mercato (*State Administration for Market Regulation,* SAMR, 国家市场监督管理总局)[34], l'Amministrazione della Cina per la Standardizzazione (*Standardisation Administration of China,* SAC, 国家标准化管理委员会), il Comitato tecnico nazionale per la standardizzazione della sicurezza delle informazioni (*National Information Security Standardisation Technical Committee*, TC 260, 全国信息安全标准化技术委员会) i quali pubblicano linee guida e standard nazionali non vincolanti volti o a colmare le lacune o funzionali alla predisposizione di una normativa sperimentale da convertire successivamente in disciplina cogente.

3. Il Codice civile cinese, artt. 1032 - 1039

In linea con la generale attenzione riservata al tema in esame, il Cod. civ. cin., in vigore dal 1° gennaio 2021, contiene norme specifiche in materia di tutela delle informazioni personali nel Libro Quarto "Dei diritti di personalità", Titolo Sesto "Dei diritti alla riservatezza e alla protezione delle informazioni personali" (artt. 1032 - 1039).
Il primo articolo ad occuparsi della materia è il 1032 che qualifica in termini di diritto soggettivo quello alla riservatezza e fissa il generale divieto di violazione, descrivendone il contenuto:

> «Ogni persona fisica ha diritto alla riservatezza. Nessuna organizzazione o individuo può ledere l'altrui diritto alla riservatezza attraverso l'indagine, l'intromissione, la divulgazione o la pubblicizzazione e simili.
> La riservatezza consiste nella serenità della vita privata di una persona fisica e della sua sfera intima, delle sue attività private e nelle sue informazioni private che non vuole siano rese note ad altri».

La tutela di questo diritto in Cina ha attraversato una profonda evoluzione passando dall'inesistenza, all'esistenza, ed infine ad un progressivo rafforzamento. Il primo riferimento a tale ambito di tutela si rinviene nella Legge di procedura civile (民事诉讼法试行) del 1982 e successivamente nell'art. 140 delle Opinioni sui Principi generali del diritto civile (民法通则意见) del 1988 in cui si pongono le basi per la previsione di una protezione più articolata. In prosieguo di tempo, nell'Interpretazione giudiziaria sul risarcimento dei danni morali (精神损害赔偿司法解释) del 2001, la tutela giudiziaria è concepita in termini di interesse così come nell' Interpretazione giudiziaria sul risarcimento dei danni alla persona (人身损害 赔偿司法解释) del 2003. Solo nel 2005, per la prima volta, a seguito dell'emendamento della Legge sulla protezione dei diritti e degli interessi delle donne (妇女权益保障法) si riconosce la riservatezza quale diritto. Ulteriore avanzamento si ha, poi, nell'art. 2 della Legge sulla responsabilità civile (侵权责任法) del 26 novembre 2009:

[34] L'Amministrazione Statale per la Regolamentazione del Mercato (国家市场监督管理总 *State Administration for Market Regulation*, SAMR) è stata istituita nell'aprile 2018, consolidando le responsabilità di supervisione del mercato precedentemente suddivise tra diverse agenzie.

> «Coloro che violano i diritti e gli interessi civili sono soggetti alla responsabilità per illecito civile ai sensi della presente legge.
> I diritti e gli interessi civili utilizzati nella presente legge comprendono il diritto alla vita, il diritto alla salute, il diritto al nome, il diritto alla reputazione, il diritto all'onore, il diritto alla propria immagine, il diritto alla riservatezza, l'autonomia coniugale, la tutela, la proprietà, l'usufrutto, gli interessi di sicurezza, il diritto d'autore, il diritto di brevetto, il diritto esclusivo all'uso di un marchio, il diritto di invenzione, i titoli di credito, il diritto di successione e altri diritti e interessi personali e patrimoniali».

La Legge non solo distingue il diritto alla riservatezza dal diritto alla reputazione ma compensa le carenze dei Principi generali del diritto civile del 1987, oggi sostituiti dalla disciplina del Cod. civ. cin. che, nella Parte generale, all'art. 110 dispone:

> «La persona fisica ha diritto alla vita, all'integrità del corpo, alla salute, al nome, all'immagine, alla reputazione, all'onore, alla riservatezza e all'autonomia coniugale.
> La persona giuridica o l'organizzazione priva di personalità giuridica ha diritto alla denominazione, alla reputazione e all'onore».

confermando e chiarendo che si tratta di un diritto civile riferito alle persone fisiche rientrante tra i diritti della personalità. Parte della dottrina cinese va oltre ed introduce la riservatezza correlata, relativa cioè al diritto alla riservatezza di soggetti terzi; l'esercizio del proprio diritto alla riservatezza, include l'interesse alla tutela del medesimo diritto di altri[35].
L'art. 1033 tratta del diritto alla riservatezza e della protezione delle informazioni personali. Enumera alcuni atti tipici che costituiscono violazione della riservatezza salvo che la legge non preveda diversamente o le parti non lo concordino. La disposizione, pertanto, conferma e consolida quanto contenuto nella Decisione del Comitato permanente dell'Assemblea Popolare Nazionale (全国人民代表大会常务委员会关于加强网络信息保护的决定) del 2012, ma conferisce una accezione più ampia riguardo ai comportamenti che configurano la violazione:

> «Salvo diversa disposizione di legge o espresso consenso del titolare del diritto,

[35] Il Comitato Tecnico Nazionale per la Standardizzazione della Sicurezza delle Informazioni (全国信息安全标准化技术委员会 *National Information Security Standardization Technical Committee*, TC260), istituito il 15 aprile 2002 a Pechino con l'approvazione dell'Amministrazione per la Standardizzazione della Repubblica Popolare Cinese (中国国家标准化管理委员会, *Standardization Administration of the People's Republic of China*, SAC), è un'organizzazione di natura tecnica impegnata nella formulazione a livello nazionale di standard di sicurezza informatica le cui principali attività sono l'emanazione di standards nel campo della sicurezza tecnologica, dei servizi di sicurezza, del *security managment* e del *security assesment*. Il 7 marzo 2020 ha annunciato l'approvazione e la pubblicazione di otto standard di sicurezza informatica ("Cybersecurity Standards"). In particolare, uno degli standard, le *Specifiche tecniche per la sicurezza delle informazioni personali GB / T 35273-2020* ("Standard di sicurezza delle informazioni"), fornisce i principi di base per la salvaguardia delle informazioni personali, nonché indicazioni sulla loro raccolta e la conservazione.

nessuna organizzazione o individuo deve compiere gli atti di seguito indicati:
(1) intromettersi nella vita privata di un'altra persona tramite telefonate, invio di messaggi di testo, utilizzo di strumenti di messaggistica istantanea, invio di posta elettronica e volantini e simili;
(2) entrare, scattare fotografie o spiare negli spazi privati altrui come la residenza o la camera d'albergo di un'altra persona;
(3) scattare fotografie, spiare, intercettare o divulgare le attività private di un'altra persona;
(4) scattare fotografie o spiare le parti intime del corpo di un'altra persona;
(5) elaborare le informazioni private di un'altra persona;
(6) violare la riservatezza di un'altra persona con altri mezzi».

Con riferimento al punto 5, la dottrina chiarisce che l'espressione "informazioni private" si riferisce a qualsiasi informazione che i privati non vogliono che sia resa nota ad altri, purché tale occultamento non violi la legge e la moralità sociale. Nello specifico, le informazioni private possono includere: le informazioni biologiche personali quali altezza, peso, gruppo sanguigno, colore della pelle, aspetto, sesso, geni, stato di salute, informazioni sulle malattia *et cetera*; informazioni riguardo al proprio corpo in riferimento alle parti del corpo che il singolo non vuole mostrare ad altri ed in particolare organi sessuali, parti disabili *et cetera*; riservatezza della proprietà privata, riservatezza riguardo alla famiglia come ad esempio, relazioni familiari, parentela di sangue, relazione matrimoniale *et cetera*, riservatezza della comunicazione quali processi di comunicazione e contenuti generati con vari mezzi quali lettere, email e telefonate che non devono essere monitorati o intercettati da altri; riservatezza delle conversazioni, contenuti che gli individui non desiderano che siano resi noti al pubblico durante il processo di comunicazione; riservatezza delle esperienze personali, storia lavorativa, amicizie, la riservatezza alla vita personale quale nome di una persona fisica, occupazione, luogo di lavoro, ambito di amicizia, preferenze di consumo, indirizzo, residenza, telefono, etnia , credo religioso, diario e altri documenti privati . La violazione, per configurarsi tale, deve essere integrata da un comportamento attivo, con ciò intendendosi atti di intrusione, monitoraggio, spionaggio, perquisizione, divulgazione, pubblicità e altri metodi di violazione. La violazione della riservatezza si manifesta, quindi, principalmente nella divulgazione di informazioni private altrui come l'interferenza nella vita privata di altre persone ed intromissione nello spazio e dominio privato altrui.
La dottrina si è occupata in modo accurato del tema precisando che non sia necessario che l'atto di violazione sia compiuto in un luogo pubblico, accogliendo un'accezione di violazione assai ampia ed inclusiva che appare privilegiare l'elemento oggettivo del comportamento. Di interesse, sempre secondo la dottrina, è che le conseguenze della violazione del diritto alla riservatezza si manifestino principalmente come danno psicologico, pur potendo provocare, in via indiretta, danni al diritto di proprietà di cui la persona sia titolare[36].
Il successivo art. 1034:

[36] W. Liming (王利明), *Ricerca sui diritti della personalità* (人格权法研究), Beijing, 2004, 600.

> «Le informazioni personali di una persona fisica sono tutelate dalla legge.
> Le informazioni personali sono quelle registrate elettronicamente o in altri modi che possano essere utilizzate, da sole o in combinazione con altre, per identificare una persona fisica, inclusi nome, data di nascita, numero di carta di identità, informazioni biometriche, indirizzo di residenza, numero di telefono, indirizzo email, informazioni sanitarie, ubicazione e simili della persona.
> Alle informazioni personali sensibili si applicano le disposizioni sul diritto alla riservatezza o, in mancanza, si applicano quelle sulla protezione delle informazioni personali».

riprende quanto già fissato dall'art. 111 del Cod. civ. cin:

> «Le informazioni personali di una persona fisica sono protette dalla legge. Qualsiasi organizzazione o soggetto che abbia necessità di ottenere informazioni altrui deve ottenerle in conformità alla legge e garantire la sicurezza di tali informazioni e non deve raccogliere, utilizzare, elaborare o trasmettere illegalmente le informazioni personali di altre persone, né può acquistare, vendere, fornire, o pubblicare illegalmente informazioni personali»,

nella Decisione del Comitato permanente dell'Assemblea Popolare Nazionale sul rafforzamento della protezione delle informazioni di rete (全国人民代表大会常务委员会关于加强网络信息保护的决定) del 28 dicembre 2012 e nelle Interpretazioni su diverse questioni relative all'applicazione della legge nella gestione dei casi penali di violazione delle informazioni personali dei cittadini (办理侵犯公民个人信息刑事案件 适用法律若干问题的解释) del 1° giugno 2017. In tal senso la dottrina rileva che l'utilizzo dei *big data* e della tecnologia legata allo sviluppo dell'intelligenza artificiale ha reso molto semplice l'analisi e l'utilizzo di grandi quantità di dati e il potenziale uso improprio delle informazioni personali è aumentato drasticamente, accrescendo il rischio di danneggiamento della dignità delle persone fisiche e di libero sviluppo della personalità[37] per cui il Cod. civ. cin. mira a porre un argine, imponendo con l'art. 999 l'uso ragionevole delle informazioni personali:

> «Il nome, la denominazione, l'immagine, i dati personali e simili di un soggetto di diritto possono essere ragionevolmente utilizzati da coloro che si occupano della diffusione di notizie, del monitoraggio di opinioni pubbliche o simili, per interessi pubblici. Se vi sia un loro irragionevole utilizzo, lesivo dei diritti della personalità del soggetto, si è tenuti a risponderne civilmente in conformità con la legge»

e prevedendo, agli artt. 1029 e1030, la facoltà di rettificare o eliminare informazioni funzionali alla determinazione del *social credit system*:

> «Un soggetto di diritto può consultare la propria valutazione di credito in conformità con la legge; ha diritto di sollevare un'obiezione e chiedere la rettificazione,

[37] Y. Lixin (杨立新), *Trattato sulla responsabilità civile* (侵权法论), Beijing, 2013, 464.

la cancellazione o altre misure necessarie da adottare se riscontri che il rapporto di credito non è corretto. I valutatori della sua affidabilità devono essa minare tempestivamente la relazione e prendere le misure necessarie in modo tempestivo se si accerta che è non veritiera».
«Le disposizioni di questo libro sulla protezione delle informazioni personali e le disposizioni pertinenti di altre leggi e regolamenti amministrativi si applicano al rapporto tra i soggetti di diritto e gli elaboratori di informazioni di credito come il sistema di informazioni creditizie».

Le due disposizioni, sia pur operanti in un ambito specifico, conferiscono una efficace tutela alle informazioni personali, in funzione di protezione della dignità umana e della libertà personale .
L'art. 1035 fissa i principi che devono essere rispettati nel trattamento delle informazioni personali e, contestualmente, le condizioni necessarie affinché il trattamento possa avvenire:

«Il trattamento delle informazioni personali deve essere conforme ai principi di liceità, legittimità, necessità, proporzionalità e deve avvenire nel rispetto delle condizioni di seguito indicate:
(1) il consenso deve essere ottenuto dalla persona fisica o dal suo tutore, salvo quanto diversamente previsto da leggi o dai regolamenti amministrativi;
(2) le regole per il trattamento delle informazioni devono essere rese pubbliche;
(3) lo scopo, il metodo e l'ambito del trattamento delle informazioni sono espressamente indicati;
(4) non vi sia violazione di leggi o regolamenti amministrativi o dell'accordo tra entrambe le parti.
Il trattamento delle informazioni personali include la raccolta, l'archiviazione, l'utilizzo, il perfezionamento, la trasmissione, la fornitura, la divulgazione e simili dei dati personali.
Durante il trattamento delle informazioni personali, un soggetto non risponde civilmente in presenza di una delle condizioni di seguito indicate:
(1) esegue ragionevolmente l'atto nella misura in cui la persona fisica o il suo tutore acconsente;
(2) tratta ragionevolmente le informazioni divulgate dalla persona fisica stessa o le altre informazioni che sono già state divulgate legalmente, a meno che detta persona lo rifiuti esplicitamente o il trattamento delle informazioni leda un interesse significativo della persona;
(3) esegue ragionevolmente gli altri atti necessari per proteggere l'interesse pubblico o i diritti e gli interessi legali della persona».

La disposzione trova un suo precedente nell'art. 41 della Legge sulla sicurezza della rete e nell'art. 29 della Legge sulla tutela dei diritti e degli interessi dei consumatori. Requisito fondamentale riguardo alla raccolta e al trattamento delle informazioni personali è che questi abbiano una base giuridica e soddisfino le condizioni fissate

dalla legge. L'oggetto della raccolta e del trattamento delle informazioni deve essere lecito; la determinazione di quali soggetti siano autorizzati a raccogliere ed elaborare le informazioni personali altrui deve essere effettuata in conformità alle disposizioni di legge.

In generale, esistono due tipi di organi che raccolgono ed elaborano le informazioni personali: le autorità statali che possono raccogliere, elaborare e utilizzare le informazioni personali nell'ambito dei loro poteri, indipendentemente dal consenso dell'interessato e i soggetti che raccolgono informazioni solo con il consenso dell'interessato e le cui modalità di raccolta devono essere conformi a quanto stabilito dalla legge. Correlati a questa disposizione l'art. 12, c. 1, della Legge sulla prevenzione e il controllo delle malattie infettive (传染 病防治法) emendata da ultimo il 28 agosto 2004[38]:

> «Tutte le unità e gli individui all'interno del territorio della Repubblica Popolare Cinese devono accettare le misure di prevenzione e controllo, come le indagini, i test, la raccolta di campioni e l'isolamento e il trattamento delle malattie infettive da parte delle istituzioni di prevenzione e controllo delle malattie e delle istituzioni mediche, e fornire informazioni pertinenti in modo veritiero. Le istituzioni di prevenzione e controllo delle malattie e le istituzioni mediche non devono divulgare informazioni o dati relativi alla privacy delle persone».

e l 'art. 25 del Regolamento sulla risposta alle emergenze di salute pubblica (突发公共卫生事件应急条例) del 9 maggio 2003 i quali prevedono che il Dipartimento amministrativo sanitario competente del Consiglio degli Affari di Stato sia responsabile della diffusione di informazioni al pubblico sull'emergenza. Inoltre, la conservazione delle informazioni personali deve essere conforme al principio del tempo minimo di conservazione, vale a dire che, se non diversamente previsto da leggi o regolamenti o autorizzato dall'interessato, le informazioni personali devono essere conservate per il tempo minimo necessario a raggiungere lo scopo per il quale l'interessato è autorizzato a utilizzarle.

Una particolare attenzione deve essere riservata al tema del consenso, la necessità del cui rilascio assurge, nella normativa generale, non solo cinese, a principio informatore della materia. Si pensi alla disciplina elaborata nell'ambito dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), nelle sue Linee guida del 1980 sulla protezione della privacy e dei flussi transfrontalieri di dati personali[39]; alla direttiva 95/46/CE sulla protezione del trattamento dei dati personali e sulla libera circolazione di tali dati del 1995[40], art. 7 lett. a; alla Legge federale sulla protezione dei dati della Germania, nonché alla normativa emanata da Francia e Regno Unito che hanno previsto il consenso informato nelle rispettive leggi sulla protezione dei dati personali.

---

[38] W. Liming (王利明), *Ricerca sui diritti della personalità,* cit.

[39] Z. Xinbao (张新宝), *Lo sviluppo del sistema giuridico di protezione della privacy in Cina* (我国隐私权保护法律制度的发展), nel *Giornale del collegio statale dei procuratori*, Beijing, 2010, 2 ss. dove la riservatezza, partendo dalla Legge sulla responsabilità civile, è ricostruita quale diritto attraverso un ragionamento deduttivo.

[40] C. Xiao (程啸), *Protezione delle informazioni dalla prospettiva di compilazione del Codice civile* (民法典编纂视野下的个人信息保护), in *China Legal Science*, 2019, 26 ss.

Nella Repubblica Popolare Cinese, nel 2012, l'art. 2 della Decisione del Comitato permanente dell'Assemblea Popolare Nazionale sul rafforzamento della protezione delle informazioni di rete (全国人民代表大会常务委员会关于加强网络信息保护的决定) ha esplicitamente stabilito che i fornitori di servizi di rete e le imprese nel corso delle loro attività commerciali e le istituzioni possono raccogliere ed utilizzare le informazioni elettroniche personali dei cittadini, richiedendo il consenso della persona le cui informazioni sono raccolte. In linea con quanto stabilito dall' art. 22, c. 3, della Legge sulla sicurezza della rete (网络安全法) ha chiaramente previsto, inoltre, che «quando i prodotti e i servizi di rete hanno la funzione di raccogliere informazioni sugli utenti, i loro fornitori devono renderlo chiaro agli utenti e ottenere il loro consenso». L'art. 41 della Legge sulla sicurezza della rete afferma, altresì, che l'operatore di rete deve ottenere il consenso della persona le cui informazioni personali devono essere raccolte per il trattamento. Per quanto riguarda il consenso informato, la dottrina rileva che esso deriva dal principio di volontarietà. In termini di natura dell'atto il consenso è, infatti, una forma di espressione della libera volontà del titolare del diritto riferito alle proprie informazioni. Positivo o negativo, il consenso della persona interessata dalla raccolta e dal trattamento dei suoi dati personali è inteso a rendere effettiva la libertà d'azione e l'autodeterminazione dell'individuo, e a conseguire gli effetti giuridici che intende ottenere[41].
L'art. 1036 delimita l'ambito di esclusione di responsabilità con riferimento al trattamento delle informazioni personali:

> «Durante il trattamento delle informazioni personali, un soggetto non risponde civilmente in presenza di una delle condizioni di seguito indicate:
> (1) esegue ragionevolmente l'atto nella misura in cui la persona fisica o il suo tutore acconsente;
> (2) tratta ragionevolmente le informazioni divulgate dalla persona fisica stessa o le altre informazioni che sono già state divulgate legalmente, a meno che detta persona lo rifiuti esplicitamente o il trattamento delle informazioni leda un interesse significativo della persona;
> (3) esegue ragionevolmente gli altri atti necessari per proteggere l'interesse pubblico o i diritti e gli interessi legali della persona».

In tale ambito la previsione del principio di presunzione della colpa è funzionale a conferire una adeguata tutela al titolare del diritto, stante la difficoltà per l'interessato a dimostrare che il responsabile del trattamento delle informazioni abbia commesso errori nel processo di raccolta, elaborazione, archiviazione e utilizzo delle informazioni[42].

[41] C. Xiao (程 啸), *Sulla Legge sulla tutela delle informazioni personali del mio paese. Regole per il trattamento dei dati personali* (论我国个人信息保护法中的个人信息处理规则), in *Tsinghua University Law Journal*, 2021, 55 ss.

[42] Y. Zhiqiang (尹志强), *Rimedi di diritto civile per violazione delle informazioni personali nell'ambiente di rete* (网络环境下侵害个人信息的民法救济), in *Leggi applicabili*, 8, 2013, 14 ss. Per una diversa impostazione della dottrina che ritiene opportuno seguire il principio della responsabilità per colpa, v. Yang Lixin (杨立新), *Illeciti e responsabilità di violazione delle informazioni personali elettroniche dei cittadini* (侵害公民个人电

Riguardo all'art. 1037:

> «Una persona fisica può consultare o fare copie delle sue informazioni personali presso l'elaboratore del trattamento delle informazioni in conformità con la legge. Se la persona riscontra che le informazioni sono errate ha diritto di sollevare un'obiezione e chiederne rettifica o altre misure necessarie da adottare in modo tempestivo.
> Se una persona fisica rilevi che un elaboratore di informazioni ha violato le disposizioni di leggi o regolamenti amministrativi o l'accordo tra le parti durante l'elaborazione delle sue informazioni personali ha diritto di chiedere all'elaboratore di informazioni di cancellarle in modo tempestivo».

La disposizione trova un precedente nell'art. 34 della Legge federale tedesca sulla protezione dei dati, nell' art. 15 del GDPR, nell'art. 3.11 della Legge sulla protezione dei dati personali di Taiwan.
Ci avviamo alla conclusione di questa rassegna. L'art. 1038:

> «Il responsabile del trattamento delle informazioni non deve divulgare o manomettere le informazioni personali che raccoglie e memorizza e senza il consenso del titolare non può offrire illegalmente ad altri le informazioni personali, salvo che queste, dopo essere state elaborate, non siano più riconducibili a uno specifico soggetto e non possano essere riportati al loro stato originario.
> Il responsabile del trattamento delle informazioni deve adottare misure tecniche e altre misure necessarie, per garantire la sicurezza delle informazioni personali che raccoglie e archivia e impedire che le informazioni siano divulgate, manomesse o smarrite. Se le informazioni personali di una persona sono divulgate, manomesse o smarrite o è probabile che lo siano, si devono adottare misure correttive in modo tempestivo e informare le persone fisiche in conformità con i regolamenti e riferire alle autorità competenti interessate».

specifica il divieto di fornire illegalmente informazioni personali senza il consenso del titolare. Il termine "divulgare" comprende sia la diffusione a soggetti non specificati sia la fornitura di informazioni a persone specifiche. Nell'era dei big data, le informazioni o i dati sono un'importante risorsa produttiva e competitiva, i dati costituiscono il veicolo attraverso il quale le informazioni esistono nel mondo di internet. L'elaborazione tecnica e il trasferimento delle informazioni, così come l'accesso da parte di terzi, sono le situazioni principali in cui le informazioni personali vengono fornite ad altri. In tutti e tre i casi la divulgazione di informazioni personali richiede il consenso della persona.
Secondo l'art. 42, c. 1, della Legge sulla sicurezza della rete, l'anonimizzazione dovrebbe raggiungere un livello tale da non consentire l'identificazione di un individuo spe-

子信息的侵权行为及其责任), in *Journal of Legal Science (Journal of Northwest University of Political Science and Law)*, 2013, 147 ss.

cifico. Il c. 2 prevede, inoltre, un obbligo specifico, per i responsabili del trattamento delle informazioni di salvaguardarne la sicurezza. Questa disposizione, che riprende l'art. 4 della Decisione del Comitato permanente dell'Assemblea Popolare Nazionale sul rafforzamento della protezione delle informazioni di rete (全国人民代表大会常务委员会关于加强网络信息保护的决定) del 28 dicembre 2012, prevede che i responsabili del trattamento delle informazioni adottino misure tecniche e altre misure necessarie per garantire la sicurezza delle informazioni personali dagli stessi raccolte ed archiviate al fine di prevenirne la fuga, la distruzione o la perdita. La violazione dell'obbligo di garantire la sicurezza delle informazioni si differenzia dalla suddetta violazione del principio del consenso informato in quanto la prima si concentra sulla raccolta e sul trattamento delle informazioni effettuate intenzionalmente dai responsabili del trattamento senza il consenso dell'interessato. Richiamando anche le previsioni degli standard tecnici relativi alla sicurezza delle informazioni personali, gli artt. 10 e 11 delle Specificazioni relative alla sicurezza delle informazioni personali (*Information Security Technology Personal Information Security Specification*, 信息安全技术个人信息安全规范) forniscono disposizioni dettagliate su come i responsabili del trattamento delle informazioni personali debbano gestire i casi di "incidente" e sui requisiti per la gestione della sicurezza delle informazioni personali all'interno dell'organizzazione responsabile del trattamento delle informazioni personali.
L'ultimo articolo che il Cod. civ. cin. dedica in modo specifico alla materia è il 1039 con una disposizione generale:

> «Gli organi statali e le istituzioni previste dalla legge che svolgono funzioni amministrative nonché il loro personale, devono rispettare la riservatezza delle persone fisiche e i dati personali ottenuti nello svolgimento delle loro funzioni, non potendoli divulgare o fornire illegalmente ad altri».

Nella versione finale è stato aggiunto «Gli organi statali e le istituzioni previste dalla legge che svolgono funzioni amministrative», sul presupposto che gli organi statali raccolgono spesso informazioni personali su larga scala per lo svolgimento dei loro compiti. Alla luce di ciò, l'art. 10, c. 2, della Decisione del Comitato permanente dell'Assemblea Popolare Nazionale sul rafforzamento della protezione delle informazioni su internet (全国人民代表 大会常务委员会关于加强网络信息保护的决定) del 2012 emendato nel 2021 dispone che «[…] gli organi statali e il loro personale devono mantenere riservate le informazioni elettroniche personali dei cittadini conosciute nell'esercizio delle loro funzioni e non devono divulgarle, manometterle o distruggerle, né venderle o fornirle illegalmente ad altri». Medesima linea è fissata dall'art. 44 della Legge sulla sicurezza della rete:

> «Nessun individuo o organizzazione può sottrare o ottenere informazioni personali in modi illegali, o vendere o fornire illegalmente informazioni personali ad altri».

così come dall'art. 45:

> «I dipartimenti responsabili della supervisione e dell'amministrazione della sicurezza della rete in conformità con la legge e il loro personale devono proteggere rigorosamente le informazioni personali, la privacy e i segreti commerciali di cui vengono a conoscenza nell'esercizio delle loro funzioni».

La dottrina ha, a tal proposito, sostenuto che l'uso dei big data abbia rafforzato il differenziale di potere esistente tra le autorità statali e i soggetti interessati alla tutela delle informazioni[43].

4. Struttura e tratti salienti della Legge sulla tutela delle informazioni personali

La Legge sulla protezione delle informazioni personali si compone di 74 articoli raccolti in otto capitoli. Si è ritenuto opportuno riportare in questa sede, ed a fini di chiarezza dello scritto, le disposizioni salienti della Legge al fine di comprenderne il significato.
Il capitolo Primo "Disposizioni generali", fissa all'art. 1 l'ambito di applicazione della normativa da cui si evincono le diverse finalità della Legge medesima: proteggere i diritti e gli interessi relativi alle informazioni personali, disciplinarne il trattamento e promuoverne l'utilizzo ragionevole (合理*hélǐ*):

> «Questa legge è emanata in conformità con la Costituzione per proteggere i diritti e gli interessi relativi alle informazioni personali□, disciplinare il trattamento delle informazioni personali e promuoverne l'uso ragionevole».

È evidente la somiglianza con l'art. 1 del GDPR ma, in modo particolare, è interessante soffermarsi sul riferimento alla ragionevolezza, quale criterio che consente un certo margine di libertà nell'uso delle informazioni personali ed in funzione dei singoli obiettivi, di volta in volta, da raggiungere. Importante, inoltre, il riferimento alla conformità costituzionale, che conferisce alla Legge una posizione privilegiata riguardo alla finalità perseguita.
L'art. 3:

> «La presente legge si applica al trattamento delle informazioni personali delle persone fisiche all'interno del territorio della Repubblica Popolare Cinese.
> La presente legge si applica anche al trattamento delle informazioni personali di persone fisiche all'interno del territorio della Repubblica popolare cinese al di fuori del territorio della Repubblica popolare cinese in una delle seguenti circostanze:
> i) quando lo scopo è quello di fornire prodotti o servizi a persone fisiche nazionali;
> ii) quando le attività delle persone fisiche nazionali sono analizzate e valutate; e
> iii) altre circostanze previste dalle leggi e dai regolamenti amministrativi»,

[43] In lingua cinese 个人信息 *gèrén xìnxī*.

fissa il principio di extraterritorialità che garantisce una sorta di estensione extraterritoriale della Legge. La Legge sulla sicurezza della rete non ha validità extraterritoriale, mentre tale principio è contenuto nella Legge sulla sicurezza dei dati, all'art.2. La disposizione prevede l'applicazione della Legge sia al trattamento delle informazioni personali delle persone fisiche all'interno dei confini della Repubblica Popolare Cinese sia al trattamento delle medesime informazioni ma effettuato al di fuori dei confini della Repubblica Popolare Cinese, nelle ipotesi in cui la finalità ultima sia quella di fornire prodotti o servizi ad individui cinesi che si trovino entro i confini nazionali; sia alle ipotesi di analisi o valutazione delle attività di persone fisiche all'interno dei confini del Paese sia ad altre circostanze previste da leggi o regolamenti amministrativi. Nel contenuto, dunque, l'art. 3 è analogo al suo corrispondente nel GDPR.
L'art. 4 fornisce la nozione di informazione personale e di trattamento:

> «Per informazioni personali si intendono tutti i tipi di informazioni relative a persone fisiche identificate o identificabili, registrate con mezzi elettronici o di altro tipo, ad esclusione delle informazioni gestite in forma anonima.
> Il trattamento delle informazioni personali comprende la raccolta, l'archiviazione, l'uso, l'elaborazione, la trasmissione, la fornitura, la divulgazione e la cancellazione, ecc. delle informazioni personali».

Sono informazioni personali tutte quelle registrate con mezzi elettronici o altri mezzi, relative a persone fisiche identificate o identificabili, escluse le informazioni che risultino dal trattamento di anonimizzazione. Pertanto, ai sensi della Legge le informazioni anonimizzate non sono informazioni personali coperte dall'ambito di tutela della Legge. La disposizione ha un contenuto analogo all'art. 4 del GDPR secondo il quale è dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera a tal fine identificabile la persona fisica che può essere individuata, direttamente o indirettamente, con particolare riferimento ad elementi quali il nome, un numero di identificazione, dati relativi alla sua generale ubicazione, identificativi presenti online o ad uno o più elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale con una sostanziale corrispondenza di tenore salva una maggiore attenzione della disposizione cinese circa la definizione di trattamento.
Gli artt. 6, 7, 8 ed 11 guidano il trattamento e l'utilizzo delle informazioni personali contemperando diversi interessi, circoscrivendo il trattamento ad uno "scopo preciso e ragionevole" quasi a proteggere in modo aperto e dichiarato il singolo, restituendo dignità e cercando di porre fine alla smisurata raccolta di dati:

> «Il trattamento delle informazioni personali deve avere uno scopo preciso e ragionevole, essere direttamente correlato allo scopo del trattamento e deve essere condotto in modo da ridurre al minimo l'impatto sui diritti e gli interessi personali.
> La raccolta di informazioni personali deve essere limitata al minimo indispensabile per raggiungere lo scopo del trattamento e non è consentita una raccolta eccessiva

di informazioni personali».

L'art. 7 fissa i principi guida e di interpretazione dell'intero testo di Legge:

> «Il trattamento dei dati personali deve seguire i principi di apertura e trasparenza, rendere pubbliche le regole per il trattamento dei dati personali e indicare espressamente le finalità, le modalità e la portata di tale trattamento».

La previsione è analoga a quella contenuta nel Considerando 39 del GDPR secondo cui qualsiasi trattamento dei dati personali deve essere lecito e corretto, le modalità con cui sono raccolti i dati, il loro utilizzo, la loro consultazione e trattamento devono essere chiari e precisi per le persone fisiche. I principi fondamentali qui elencati, chiave di lettura e di interpretazione dell'intero testo della Legge erano già presenti nelle linee guida sulla privacy dell'OCSE e della Convenzione 108 del Consiglio d'Europa, per poi trovare conferma sia nella direttiva 95/46/CE dell'Unione europea sia nell' *Asia-Pacific Economic Cooperation Privacy Framework*.
Tra i principi generalmente presenti nei diversi ordinamenti vi sono quelli secondo cui i dati devono essere trattati in modo equo e lecito, e solo per le finalità specificate all'individuo; devono essere raccolte e trattate solo le informazioni personali necessarie per tali finalità e poi cancellate; tali dati devono essere pertinenti, accurati e aggiornati, i soggetti devono essere messi al corrente del trattamento che ne viene effettuato e dei loro relativi diritti, tali da consentire loro di esercitare un controllo. Devono essere previste garanzie aggiuntive per categorie particolari di dati, tutti i dati devono essere protetti da rischi quali la perdita o l'accesso non autorizzato, la distruzione, l'uso, la modifica o la divulgazione ed i responsabili del trattamento rispondono della mancata attuazione a questi principi.
Alcuni di questi principi esistono sia nell' Unione europea che negli Stati Uniti, quali ad esempio i requisiti di minimizzazione dei dati, trasparenza e qualità dei dati e risultano essere più stringenti in Europa; altri, quali ad esempio la protezione aggiuntiva per i dati sensibili, le restrizioni sui trasferimenti transfrontalieri, la supervisione da parte di un'autorità di vigilanza indipendente ed i limiti alla profilazione, diversamente, sono assenti nella normativa degli Stati Uniti.
L'art. 8 della Legge prevede che il trattamento delle informazioni personali debba garantire la qualità delle informazioni personali ed evitare effetti negativi sui diritti e sugli interessi individuali derivanti da informazioni personali imprecise o incomplete:

> «La qualità delle informazioni personali deve essere garantita nel trattamento delle informazioni personali per evitare l'impatto negativo sui diritti e gli interessi personali causato da informazioni personali inesatte o incomplete».

Analoga previsione è contenuta nel Considerando 86 del GDPR, secondo il quale il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine

di consentirgli di prendere le necessarie precauzioni.
L'art. 11, vera e propria proclamazione, analoga all'art. 51 del GDPR, afferma il ruolo centrale dello Stato, il quale istituisce un sistema efficiente e completo per la protezione delle informazioni personali al fine di prevenire e punire atti lesivi dei diritti e degli interessi sulle informazioni personali, rafforzare la pubblicità e l'educazione sulla protezione delle informazioni personali ed infine promuovere la creazione di un contesto idoneo alla protezione delle informazioni personali medesime:

> «Lo Stato stabilisce un solido sistema di protezione delle informazioni personali, previene e punisce la violazione dei diritti e degli interessi delle informazioni personali, rafforza la pubblicità e l'educazione alla protezione delle informazioni personali e promuove la formazione di un buon ambiente in cui il governo, le imprese, le organizzazioni sociali interessate e il pubblico partecipano congiuntamente alla protezione delle informazioni personali».

Alle modalità di trattamento delle informazioni personali e ai diversi tipi di consenso sono dedicati diversi articoli: 13, 15, 23, 29 e 39.
Art. 13:

> «Solo in una delle seguenti circostanze il responsabile del trattamento delle informazioni personali può trattarle:
> i) ove sia ottenuto il consenso dell'interessato;
> ii) quando il consenso è necessario per la conclusione o l'esecuzione di un contratto di cui l'interessato è parte, o per l'attuazione della gestione delle risorse umane in conformità con le norme e i regolamenti del lavoro formulati in conformità alla legge e al contratto collettivo concluso a norma di legge;
> iii) ove sia necessario per l'adempimento di doveri o obblighi di legge;
> iv) ove sia necessario per la risposta a un'emergenza sanitaria pubblica o per la tutela della vita, della salute e della sicurezza dei beni di una persona fisica;
> v) laddove atti come la segnalazione di notizie e la supervisione da parte dell'opinione pubblica siano effettuati nell'interesse pubblico e il trattamento dei dati personali rientri in uno scopo ragionevole;
> vi) quando è necessario trattare le informazioni personali divulgate dall'interessato o altre informazioni personali che sono state legalmente divulgate entro un ambito ragionevole in conformità con le disposizioni della presente legge;
> vii) altre circostanze previste da leggi e regolamenti amministrativi.
> Il trattamento delle informazioni personali è soggetto al consenso dell'interessato in conformità con le altre disposizioni pertinenti della presente legge; tuttavia, il consenso dell'interessato non è richiesto nelle circostanze di cui ai punti da ii) a vii) del comma precedente».

Quanto disposto dall'art. 13 della Legge è analogo a quanto previsto dall'art. 6 del GDPR, che indica come i dati personali possano essere utilizzati in modo lecito e trasparente, laddove il primo statuisce che il trattamento dei dati è lecito solo se e nella

misura in cui ricorrano determinate condizioni, tra cui la prestazione del consenso espresso dall'interessato, la necessità del trattamento rispetto all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, *et cetera.*
Il consenso è disciplinato dall'art. 15:

> «Qualora il trattamento dei dati personali si basi sul consenso dell'interessato, l'interessato ha il diritto di revocare il consenso. Il responsabile del trattamento dei dati personali fornisce un metodo conveniente per l'individuo per revocare il proprio consenso.
> La revoca del consenso da parte dell'interessato non pregiudica la validità di qualsiasi attività di trattamento dei dati personali condotta sulla base del consenso dell'interessato prima di tale revoca».

La Legge stabilisce il principio di convenienza. Anche se non è specificato chiaramente in cosa consista, è generalmente inteso che la difficoltà di "rilevare il consenso" non dovrebbe essere maggiore di quella di prestarlo.
Riguardo alle informazioni sensibili queste trovano una propria regolamentazione negli artt. 28 - 32:

> «Le informazioni personali sensibili si riferiscono alle informazioni personali che potrebbero ledere la dignità personale di qualsiasi persona fisica, o danneggiare la sua sicurezza personale o patrimoniale una volta divulgate o utilizzate illecitamente, comprese informazioni quali l'identificazione biometrica, il credo religioso, l'identità specifica, lo stato di salute, i conti finanziari, la posizione e le tracce, nonché le informazioni personali dei minori di 14 anni.
> Solo per specifiche finalità e sufficienti necessità, e qualora siano state adottate rigorose misure di protezione, il responsabile del trattamento può trattare le informazioni sensibili»;

> «Il trattamento delle informazioni personali sensibili di un individuo è soggetto al separato consenso dell'interessato; ove le leggi e i regolamenti amministrativi prevedano che il trattamento delle informazioni personali sensibili sia subordinato al consenso scritto, prevalgono tali disposizioni»;

> «Riguardo alle informazioni personali sensibili di una persona fisica, il responsabile del trattamento dei dati personali deve informare la persona interessata, oltre alle fattispecie indicate dal comma 1 dell'articolo 17, della necessità del trattamento delle sue informazioni sensibili e dell'impatto sui suoi diritti soggettivi e interessi, ad eccezione delle circostanze per le quali può essere esentato dall'informare l'individuo in conformità con questa legge»;

> «Per operare il trattamento delle informazioni personali di un minore di età inferiore ai 14 anni, il responsabile del trattamento deve ottenere il consenso dei

genitori o di altri tutori del minore.
Per operare il trattamento delle informazioni personali dei minori di età inferiore ai 14 anni, il responsabile del trattamento predisporrà regole specifiche per il trattamento dei dati personali».

L'art. 31 della Legge e l'art. 8 del GDPR disciplinano entrambi il trattamento delle informazioni personali dei minori. Vi sono, tuttavia, alcune differenze tra le due disposizioni: l'art. 31 della Legge cinese richiede che i responsabili del trattamento ottengano il consenso esplicito dei tutori legali dei minori prima di procedere al trattamento dei dati; l'art. 8 del GDPR richiede, invece, che i responsabili del trattamento ottengano il consenso esplicito dei minori stessi se hanno un'età idonea a comprendere le implicazioni del loro consenso prestato. Inoltre, il Considerando 38 del GDPR riconosce espressamente che i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia nonché dei loro diritti in relazione al trattamento delle informazioni personali.

«Qualora leggi e regolamenti amministrativi prevedano che il trattamento delle informazioni personali sensibili sia soggetto alla relativa autorizzazione amministrativa o ad altre restrizioni, prevarranno tali disposizioni».

Altro tema centrale affrontato dalla Legge riguarda il trasferimento e la localizzazione dei dati su cui già si è riferito nell'art. 3. Sul tema si sofferma un intero capitolo, il Terzo della Legge "Regole per la fornitura transfrontaliera di informazioni personali", artt. 38 - 43.
Gli artt. 38 e 39 impongono ai responsabili del trattamento dei dati che intendono fornire informazioni personali al di fuori del territorio della Repubblica Popolare Cinese di adottare una tra le seguenti misure: i) una valutazione del rischio di trasferimento dei dati da parte della Amministrazione per la sicurezza del ciberspazio (*Cybersecurity Administration of China*, CAC); ii) una certificazione legale rilasciata da un'agenzia specializzata nella protezione delle informazioni personali; iii) la sottoscrizione di clausole contrattuali standard (*Standard Contractual Clauses*, SCC) formulate dalla medesima Amministrazione; iv) l'adozione di altre misure richieste da leggi, regolamenti amministrativi o dall' Amministrazione per la sicurezza del ciberspazio. Si richiede, inoltre, il consenso separato dell'interessato. Sul tema, a dimostrazione del continuo aggiornamento, sono stati rilasciati sia un nuovo regolamento sulla valutazione del rischio di trasferimento "Misure di valutazione della sicurezza per i trasferimenti di dati in uscita" (*Security assessment measures for outbound data transfers,* 数据出境安全评估办法[44], di seguito "Misure") in vigore dal 1° settembre 2022 [45], sia le Disposizioni sui contratti

[44] Il Regolamento, pubblicato il 7 luglio 2022, è in vigore dal 1° settembre 2022. Disciplina il trasferimento dei dati in uscita, protegge diritti e interessi inerenti alle informazioni personali e mira a garantire al contempo la sicurezza nazionale e un flusso transfrontaliero libero. Le Misure sono formulate tenendo conto della previgente disciplina contenuta nelle tre principali leggi in materia di dati e nei regolamenti di dettaglio.

[45] Per la traduzione in lingua inglese del Regolamento, vedi qui.

standard per il trasferimento transfrontaliero di informazioni personali (*Provisions on Standard Contracts for Cross-border Transfers of Personal Information*, 个人信息出境标准合同规定) in vigore dal 1° giugno 2023.

Dalla lettura del combinato disposto dell'art. 40 della Legge e dell'art. 4 delle Misure, si evince che il responsabile del trattamento delle informazioni che fornisce informazioni all'estero deve, in una delle seguenti circostanze, richiedere una valutazione della sicurezza del trasferimento delle informazioni in uscita al Dipartimento nazionale per la sicurezza informatica e l'informatizzazione attraverso il dipartimento locale: i) il responsabile del trattamento dei dati fornisce dati importanti[46] all'estero; ii) gli operatori di infrastrutture informatiche critiche (CIIO)[47] o i responsabili del trattamento dei dati che elaborano i dati personali di oltre 1 milione di persone hanno la necessità di fornire informazioni personali all'estero; iii) i responsabili del trattamento dei dati hanno fornito all'estero informazioni personali di oltre 100.000 persone o informazioni personali sensibili[48] di oltre 10.000 persone, dal 1° gennaio dell'anno precedente; iv) altre circostanze stabilite dalla CAC.

In base agli articoli 60, 63 e 64 della Legge, la Cina ha implementato meccanismi diversificati riguardo alla protezione delle informazioni personali. L' Amministrazione per la sicurezza del ciberspazio è responsabile del coordinamento della protezione delle informazioni personali e delle relative attività di supervisione e amministrazione, così come i competenti dipartimenti del Consiglio degli Affari di Stato sono responsabili della protezione, supervisione e amministrazione della protezione delle informazioni personali in conformità con le leggi e i regolamenti vigenti:

> «L'Amministrazione per la sicurezza del ciberspazio è responsabile per il coordinamento della protezione dei dati personali e del relativo lavoro di supervisione e di amministrazione. I dipartimenti pertinenti del Consiglio di Affari di Stato sono responsabili per la protezione, la supervisione e l'amministrazione della pro-

[46] Gli "*important data*" erano già previsti sia dalla CSL, sia dalla DSL, sebbene in nessuna delle due Leggi fosse fornita una definizione precisa. La lacuna è stata colmata dall'art 19 delle nuove Misure, che li definisce come «dati che, se alterati, distrutti, trapelati, acquisiti o utilizzati illegalmente, ecc. possono danneggiare la sicurezza nazionale, le operazioni economiche, la stabilità sociale, la salute o la sicurezza pubblica, ecc.».

[47] L'art. 2 dei Regolamenti sulla sicurezza e la protezione delle infrastrutture critiche informatizzate (*Critical Information Infrastructure Security Protection Regulations* - 关键信息基础设施安全保护条例), in vigore dal 1° settembre 2021, le identifica in infrastrutture di rete e sistemi informativi, impegnati in importanti settori come le telecomunicazioni pubbliche e i servizi informativi, l'energia, i trasporti, l'acqua, la finanza, i servizi pubblici, l'*e-government*, la scienza, la tecnologia e l'industria della difesa nazionale, o qualsiasi altra importante struttura di rete o sistema informativo che possa danneggiare gravemente la sicurezza, l'economia nazionale e i mezzi di sussistenza delle persone, o l'interesse pubblico in caso di incapacità, danni o fughe di dati.

[48] I dati personali sensibili vengono definiti dall'art 28 della PIPL come «i dati personali che, una volta divulgati o utilizzati illegalmente, potrebbero causare un danno alla dignità personale di una persona fisica o un danno alla sua sicurezza personale o patrimoniale, compresi i dati di identificazione biometrica, il credo religioso, l'identità specifica, la salute medica, il conto finanziario e gli spostamenti e le tracce, nonché i dati personali dei minori di 14 anni». Lo stesso articolo specifica, a seguire, che tali dati possono essere trattati solo «per uno scopo specifico e per una necessità sufficiente, e se sono state adottate misure di protezione rigorose».

tezione delle informazioni personali nell'ambito delle loro rispettive funzioni in conformità con le disposizioni della presente legge, delle leggi e dei regolamenti amministrativi pertinenti.
Le funzioni dei dipartimenti pertinenti dei governi del popolo locali a un livello pari o superiore alla contea per la protezione, la supervisione e l'amministrazione della protezione dei dati personali devono essere determinati in conformità con le relative disposizioni dello Stato.
I dipartimenti menzionati nei precedenti due paragrafi sono collettivamente indicati come le autorità preposte alle funzioni di protezione dei dati personali».

«Le autorità che svolgono compiti di protezione dei dati personali possono adottare le seguenti misure nello svolgimento di tali compiti:
(1) informare le parti interessate e indagare sulle circostanze relative alle attività di trattamento dei dati personali;
(2) esaminare e copiare contratti, registrazioni, libri contabili e altro materiale pertinente relativo alle attività di trattamento dei dati personali delle parti interessate;
(3) svolgere ispezioni in loco e indagini sulle attività di trattamento dei dati personali sospettate illecite;
(4) ispezione dei dispositivi e degli oggetti relativi alle attività di trattamento dei dati personali; i dispositivi e gli oggetti risultanti utilizzati per attività illecite di trattamento dei dati personali possono essere sequestrati o confiscati previa istanza scritta e approvazione del responsabile principale dell'autorità interessata.
Le autorità che svolgono compiti di protezione dei dati personali adempiono a tali obblighi ai sensi di legge, gli interessati prestano assistenza e collaborazione, non rifiutano od ostacolano tale adempimento».

Quanto disposto dall'art. 63 della Legge è paragonabile a quanto previsto dall'art. 58 del GDPR, il quale indica i poteri di indagine, correttivi, autorizzativi e consultivi delle autorità. L'art. 63 conferisce alle autorità di protezione dei dati il potere di imporre multe e altre sanzioni amministrative nei confronti dei responsabili e degli incaricati del trattamento dei dati che violano le disposizioni della Legge, così come l'art. 58 del GDPR conferisce alle autorità di protezione dei dati il potere di imporre multe e altre sanzioni amministrative ai responsabili e agli incaricati del trattamento che violano le disposizioni del Regolamento.

«Qualora le autorità che svolgono compiti di protezione dei dati personali rilevino nell'esercizio di tali compiti che vi sono rischi elevati nelle attività di trattamento dei dati personali o si sono verificati incidenti di sicurezza dei dati personali, possono, secondo i limiti e le procedure prescritte, avere un colloquio con il legale rappresentante o il principalmente responsabile del gestore del trattamento dei dati personali interessato, o richiedere a tale gestore di affidare a un'agenzia specializzata lo svolgimento di un controllo di conformità sulle sue attività di trattamento dei dati personali. Il gestore del trattamento dei dati personali adotta come richiesto delle misure al fine di rettificare ed eliminare i pericoli nascosti.

> Qualora le autorità preposte alla protezione dei dati personali riscontrino nell'esercizio di tali compiti che un trattamento illecito di dati personali sia sospettato di costituire reati, ne informano tempestivamente le autorità di pubblica sicurezza al fine di provvedere a norma di legge».

Infine, meritevole di considerazione è il Capitolo settimo "Responsabilità legale", artt. 66 - 71. Rispetto alla normativa precedentemente elaborata, le sanzioni previste dalla Legge in esame sono assai più elevate in connessione alle maggiori responsabilità configurate in capo sia agli individui che alle organizzazioni.

> «Nel caso in cui i dati personali siano trattati in violazione delle disposizioni della presente legge, o i dati personali siano trattati senza adempiere all'obbligo di protezione dei dati personali previsto dalla presente legge, le autorità che svolgono compiti di protezione dei dati personali ordina all'interessato di apportare correzioni, notificare avvertimenti, confiscare i ricavati illeciti, a qualsiasi applicazione che tratti illecitamente dati personali è ordinata la sospensione o la cessazione della prestazione dei servizi; colore che rifiutano il giusto adempimento, si applica la sanzione pecuniaria non superiore a 1 milioni di yuan; per coloro che sono principalmente e direttamente responsabili si applica la sanzione pecuniaria non inferiore a 10.000 yuan e non superiore a 100.000 yuan.
> Per ogni atto illecito precedentemente indicati, con circostanze gravi, le autorità che svolgono compiti di protezione dei dati personali a livello provinciale o superiore ordinano all'interessato di apportare correzioni, confiscare i ricavi illeciti e si applica la sanzione pecuniaria non superiore a 50 milioni di yuan o non più del 5% del fatturato dell'anno precedente, e può anche ordinare la sospensione dell'attività pertinente o sospendere l'attività per la rettifica e informare le autorità competenti pertinenti di revocare il relativo permesso commerciale o licenza commerciale; alle persone principalmente e direttamente responsabili si applica la sanzione pecuniaria non inferiore a 100.000 yuan e non superiore a 1 milione di yuan, è possibile inoltre vietare a tali persone di agire come amministratori, supervisori, alti dirigenti e responsabili della protezione dei dati personali delle imprese interessate entro un determinato periodo di tempo».

Può essere effettuato un parallelismo tra la disposizione dell'art. 66 della Legge e l'art. 83 del DGPR. L'art. 66 della Legge prevede che le aziende debbano ottenere il consenso degli utenti prima di raccogliere le loro informazioni personali e richiede che esse informino gli utenti sul loro utilizzo e sul loro diritto di richiederne la cancellazione. Disposizione simile si rinviene all'art. 83 del GDPR, il quale stabilisce le condizioni generali per comminare sanzioni amministrative di tipo pecuniario, che le sanzioni amministrative pecuniarie debbano essere efficaci, proporzionate e dissuasive, che qualora un titolare del trattamento o un responsabile del trattamento violi, con dolo o colpa più disposizioni del Regolamento l'importo totale della sanzione amministrativa pecuniaria non possa superare l'ammontare previsto per la violazione più grave.

«Gli atti illeciti previsti dalla presente legge sono registrati negli archivi dei crediti secondo le disposizioni di legge e di regolamento amministrativo in materia e sono portati a conoscenza del pubblico».

«Qualora un organo statale non adempia all'obbligo di protezione delle informazioni personali previsto dalla presente legge, il suo organo superiore o le autorità che svolgono compiti di protezione delle informazioni personali ordinano alle persone principalmente o direttamente responsabile di apportare correzioni, e gli sono comminate sanzioni ai sensi di legge».

Una disposizione simile all'art. 68 della Legge è totalmente assente nel GDPR, probabilmente ciò è dovuto alla natura indipendente della autorità europea di controllo e dell'applicabilità, a tali casi, degli ordinari rimedi previsti dal diritto amministrativo. La disposizione più simile presente nel GDPR è quella dell'art. 83 secondo cui, fatti salvi i poteri correttivi delle autorità di controllo a norma dell'art. 58, par. 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti nello Stato membro.

«Qualora un membro del personale delle autorità che svolge compiti di protezione dei dati personali trascuri il proprio dovere, abusa del proprio potere, fa favoritismi e commette irregolarità, che non costituiscono reato, gli sono comminate sanzioni in conformità con la legge»;

«Qualora il trattamento dei dati personali leda i diritti e gli interessi in materia di dati personali e causi un danno, il gestore del trattamento dei dati personali, se non può dimostrare di non avere colpa, è considerato responsabile per i danni e per le altre violazioni responsabili»;
«La responsabilità per i danni precedentemente indicati è determinata sulla base delle perdite così subite dall'interessato o dei benefici così ottenuti dal gestore del trattamento; se le perdite così subite dall'interessato o i benefici così ottenuti dal gestore del trattamento delle informazioni sono difficili da determinare, l'importo dei danni deve essere determinato in base alle circostanze effettive»;

«Qualora un gestore del trattamento delle informazioni personali elabori informazioni personali in violazione della presente legge, che lede i diritti e gli interessi di un gran numero di persone, la Procura del popolo, le organizzazioni dei consumatori riconosciute dalla legge e le organizzazioni determinate dall'ACC possono portare una querela davanti a un tribunale del popolo ai sensi di legge»;

«Qualora la violazione delle presenti disposizioni costituisca violazione dell'amministrazione di pubblica sicurezza, si applica la sanzione amministrativa di pubblica sicurezza a norma di legge e, se si configura reato, la responsabilità penale è accertata a norma di legge».

5. Posizione e ruolo della Legge sulla protezione delle informazioni personali all'interno dell'ordinamento. La coerenza del sistema

Come anticipato nei precedenti paragrafi, è evidente il crescente impegno del legislatore cinese per la costruzione di un regime di protezione delle informazioni personali. A fronte della presenza di un testo legislativo unitario di riferimento, permane riferibile ad una pluralità di fonti di diverso grado, di Interpretazioni della Corte Suprema del Popolo nonché di standard tecnici che regolamentano la materia.
In tal senso merita di essere verificata la coerenza interna dell'ordinamento, nello specifico il rapporto tra la Legge ed il Cod. civ. cin.[49] i cui libri sono stati pubblicati in periodi diversi: il 1° ottobre 2017 è entrato in vigore il Libro Primo del Codice "Parte generale"; il 1° gennaio 2021 sono entrati in vigore i restanti sei libri del Codice; il 1° novembre 2021, come già riportato, è entrata in vigore la Legge sulla tutela delle informazioni personali[50].
L'art. 1 della Legge, già precedentemente menzionato:

> «Questa legge è emanata in conformità con la Costituzione per proteggere i diritti e gli interessi delle informazioni personali, disciplinare il trattamento dei dati personali e promuovere l'uso ragionevole delle informazioni personali».

indica la conformità alla Costituzione, quale fattore essenziale che conferisce alla Legge una posizione privilegiata in linea con quanto avviene nella normativa europea dove l'art. 8 della Carta dei diritti fondamentali del 2000 assegna alla protezione delle informazioni personali il carattere di diritto fondamentale indipendente[51]. La Legge, ritenuta fondamentale (基本法*jīběnfǎ*) appena al di sotto della Costituzione, deve rispettare le disposzioni del Cod. civ. cin. con cui deve necessariamente coordinarsi.
L'art. 69 della Legge pone un rinvio al Codice:

---

[49] Sul tema di interessse le considerazioni in L. Wang – B. Xiong, *Personality Rights in China's New Civil Code: A Response to Increasing Awareness of Rights in an Era of Evolving Technology*, in *Modern China*, 47(6), 2021, 703 ss.

[50] W. Liming, *On China's Civil Law Codification and the Development of China's Civil Law Scholarship*, in *Contemporary Social Sciences*, 3, 2020, 99 ss. , spec. 103 ss.:« […] *the codification improved the value system of civil law. From the perspective of comparative law, after the enactment of the civil code, the changes of the social, political, and cultural backgrounds and the economic conditions will cause scholars to re-examine and discuss the value and rationality of corresponding regulations. Alan Watson pointed out that the value rationality of the civil code is the ultimate concern for people (Watson, 2005, 269). In essence, civil law is the law for people, and strengthening the concern for humanism is an important trend in contemporary civil law. China's civil legislation reflects the concern for humanism and the innovation of ideas. Traditional civil law is concerned only with abstract individuals, not with the interests of special groups (Radbruch, 1997, 66). From an abstract concept to a specific person, "it is closer to the essence of private law to improve the status of the weak in the market and enhance their ability to realize their will." The concern of humanism has been sufficiently demonstrated in China's civil code*».

[51] Art. 8 Carta dei diritti fondamentali dell'Unione europea: «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

> «Qualora il trattamento delle informazioni personali leda i diritti e gli interessi in materia di informazioni personali e causi un danno, il responsabile del trattamento delle informazioni personali, se non può dimostrare di non avere colpa, è considerato responsabile per i danni e per le altre violazioni responsabili.
> La responsabilità per i danni precedentemente indicati è determinata sulla base delle perdite così subite dall'interessato o dei benefici così ottenuti dal gestore del trattamento; se le perdite così subite dall'interessato o i benefici così ottenuti dal gestore del trattamento delle informazioni sono difficili da determinare, l'importo dei danni deve essere determinato in base alle circostanze effettive»,

laddove, accanto alla presunzione di colpa quale principio di imputazione vi è un rimando alle disposizioni del Codice civile sulla responsabilità civile con esplicito riferimento alla responsabilità per fatto illecito.
A dimostrazione di questa ampia coesistenza a livello sistemico interno, ora tra Legge e Codice penale, è di ausilio l'art. 71 della Legge:

> «Qualora la violazione delle presenti disposizioni costituisca violazione dell'amministrazione di pubblica sicurezza, si applica la sanzione amministrativa di pubblica sicurezza a norma di legge e, se si configura reato, la responsabilità penale è accertata a norma di legge».

Entriamo più nel dettaglio con alcuni esempi. Per quanto riguarda la nozione di informazione personale questa è prevista sia dall'art. 1034, c. 2, del Cod. civ. cin.:

> «Le informazioni personali sono quelle registrate elettronicamente o in altri modi che possano essere utilizzate, da sole o in combinazione con altre, per identificare una persona fisica, inclusi nome, data di nascita, numero di carta di identità, informazioni biometriche, indirizzo di residenza, numero di telefono, indirizzo email, informazioni sanitarie, ubicazione e simili della persona»,

sia dall'art. 4, c. 2, della Legge:

> «Per informazione personale si intende ogni tipo di informazione relativa a persone fisiche identificate o identificabili registrata con mezzi elettronici o con altri mezzi, escluse le informazioni trattate in forma anonima».

Quest'ultima disposizione è certamente più concisa e diverso ne è l'ambito di applicazione escludendo esplicitamente le informazioni anonimizzate che in tal modo non rientrano più nell'ambito delle informazioni personali escludendo l'applicabilità della Legge. Ulteriore esempio riguarda i diritti conferiti sulle proprie informazioni personali normativa fissata sia dall'art.1037 del Cod. civ. cin.:

> «Una persona fisica può consultare o fare copie delle sue informazioni personali

presso il responsabile del trattamento delle informazioni in conformità con la legge. Se la persona riscontra che le informazioni sono errate ha diritto di sollevare un'obiezione e chiederne rettifica o altre misure necessarie da adottare in modo tempestivo.
Se una persona fisica rilevi che un responsabile del trattamento delle informazioni ha violato le diposizioni di leggi o regolamenti amministrativi o l'accordo tra le parti durante l'elaborazione delle sue informazioni personali, ha diritto di chiedere al responsabile del trattamento delle informazioni di cancellarle in modo tempestivo».

sia dagli artt. 45, 46, c. 1 e c. 2, 47 e 48:

«Un individuo ha il diritto di consultare o copiare le proprie informazioni dal responsabile del trattamento dei dati personali, salvo che per le circostanze previste dall'art. 18 comma 1, e 35.
Qualora un individuo richieda di consultare o copiare le proprie informazioni, il responsabile del trattamento delle informazioni personali fornisce tali informazioni tempestivamente.
Qualora un individuo richieda di trasferire le proprie informazioni a un responsabile del trattamento dei dati personali da lui designato, il quale soddisfi le condizioni indicate dall'Amministrazione per la sicurezza del ciberspazio, il gestore delle informazioni personali fornisce indicazioni per il trasferimento»;

«Qualora un individuo ritenga che le proprie informazioni personali siano imprecise o incomplete, ha diritto di richiedere al responsabile delle informazioni personali di apportare correzioni o integrazioni.
Qualora un individuo richieda correzioni o integrazioni alle proprie personali, il responsabile del trattamento verifica e corregge o integra tempestivamente tali informazioni»;

«In una delle seguenti circostanze, un responsabile del trattamento delle informazioni personali assume l'iniziativa di cancellare le informazioni personali; qualora ometta di cancellarle, l'interessato ha il diritto di richiedere la cancellazione di tali informazioni:
(i) se la finalità del trattamento è stata raggiunta, è impossibile raggiungere tale obiettivo o non è più necessario raggiungerlo;
(ii) se il responsabile del trattamento delle informazioni personali cessa di fornire prodotti o servizi o il periodo di conservazione è scaduto;
(iii) se l'individuo ritira il proprio consenso;
(iv) se il responsabile del trattamento delle informazioni personali elabora informazioni personali in violazione della legge, regolamenti amministrativi o accordi;
(V) altre circostanze stabilite dalla legge o dai regolamenti amministrativi.
Se il periodo di conservazione previsto dalle leggi e dai regolamenti amministrativi non scade, o la cancellazione dei dati personali è difficile da realizzare tecnicamen-

te, il responsabile del trattamento dei dati personali interrompe il trattamento, oltre all'archiviazione e alle necessarie misure di protezione della sicurezza»;

«Gli individui hanno diritto a richiedere a un responsabile dei dati personali di indicare le proprie regole di processazione delle informazioni personali».

È evidente come la normativa fissata dalla Legge sia più dettagliata rispetto a quella fissata dal Cod. civ. cin. con cui ha continui rimandi ed integrazioni, modalità tipica del diritto cinese in continuo assestamento. Il legislatore, pertanto, è partito dal presupposto che la Legge debba coesistere con il previgente diritto civile e penale ma nel medesimo tempo arricchisca la normativa o resti silente laddove questa abbia già provveduto.

6. Diritto alla riservatezza e tutela delle informazioni personali

Il rapporto tra riservatezza ed informazioni personali è stato a lungo discusso in dottrina e concettualizzato in una solida tripartizione: quello alla protezione delle informazioni personali e quello alla riservatezza sono diritti distinti ma complementari; la protezione delle informazioni personali è un sottoinsieme del diritto alla riservatezza; il diritto alla tutela delle informazioni personali ha carattere indipendente e serve una moltitudine di funzioni, tra cui, ma non solo, la protezione dei dati personali. Accanto alla riservatezza ed alle informazioni personali, assumono caratteri precipui le informazioni sensibili.
Il diritto alla riservatezza trova una prima sistemazione, seguendo il criterio cronologico, negli artt. 38 e 40 della Cost.:

«La dignità personale dei cittadini della Repubblica Popolare Cinese è inviolabile».

«La libertà e la segretezza (秘密*mìmì)* della corrispondenza dei cittadini della Repubblica Popolare Cinese sono tutelate dalla legge. Nessuna organizzazione o individuo può, per nessun motivo, violare la libertà e la segretezza della corrispondenza dei cittadini, tranne nei casi in cui, per soddisfare le esigenze di sicurezza dello Stato o di indagini su reati penali, gli organi di pubblica sicurezza o procuratori sono autorizzati a censurare la corrispondenza secondo le procedure previste dalla legge».

e negli artt. 110, c. 1, e 1032 del Cod. civ. cin.:

«La persona fisica ha diritto alla vita, all'integrità del corpo, alla salute, al nome, all'immagine, alla reputazione, all'onore, alla riservatezza e all'autonomia coniugale».
«Ogni persona fisica ha diritto alla riservatezza. Nessuna organizza-

zione o individuo può ledere l'altrui diritto alla riservatezza attraverso l'indagine, l'intromissione, la divulgazione o la pubblicizzazione e simili. La riservatezza consiste nella serenità della vita privata di una persona fisica e della sua sfera intima, delle sue attività private e nelle sue informazioni private che non vuole siano rese note ad altri».

Riguardo all'ambito di tutela, secondo quanto stabilisce l'art. 1032, il diritto alla riservatezza comprende lo spazio privato, le attività private e le informazioni private di una persona fisica che non vuole che altri ne vengano a conoscenza. Le informazioni personali, diversamente, sono informazioni di identificazione personale, tra cui il nome, la data di nascita, il numero del documento d'identità, le informazioni biometriche, l'indirizzo, il numero di telefono, l'indirizzo e-mail, le informazioni sulla salute, gli spostamenti, *et cetera*. Pertanto, come è evidenziato dalla dottrina tra diritto alla riservatezza e tutela delle informazioni personali vi sono alcune differenze: la riservatezza consiste nel diritto di tenere segreti aspetti, comportamenti, atti relativi alla sfera intima della persona, le informazioni personali enfatizzano l'identificazione e l'individuazione personale; il rapporto tra le due, non è di inclusione o esclusione, subordinazione o sovraordinazione, bensì un rapporto trasversale[52]. Certo è, tuttavia, che alcune informazioni personali, soprattutto quelle che riguardano la sfera personale, appartengono all'ambito della riservatezza (ad esempio lo stato civile, la salute fisica, le informazioni creditizie, il luogo in cui ci si trova, *et cetera*) essendo informazioni personali private (个人私密信息, *gèrén sīmì xìnxi*) mentre, di altre informazioni personali è evidente il carattere pubblico, nel senso di pubblicamente reperibili, quali ad esempio il nome, il sesso, il luogo di origine, *et cetera*. Le informazioni personali private rappresentano dunque il punto di intersezione tra riservatezza ed informazioni personali. In generale, è possibile sostenere che costituiscono informazioni personali private tutte le informazioni che un privato non vuole divulgare, non desiderando che altri ne vengano a conoscenza quali ad esempio le condizioni fisiche, lo stato di salute, le informazioni sui beni in proprietà, sulla famiglia, le informazioni genetiche, quelle relative ad esperienze personali e altre informazioni attinenti alla vita personale[53]. A causa di questo ambito di coincidenza, esse vengono tutelate su due diversi fronti.

Il Cod. civ. cin. sceglie di dare priorità alla tutela della riservatezza e la ragione di questa impostazione risiede nel fatto che il diritto alla riservatezza si concentra sulla protezione della dignità umana, mentre il diritto alla tutela delle informazioni personali si concentra sulla protezione dell'identità personale. La protezione della riservatezza, quindi, è più rigorosa e forte rispetto alla protezione delle informazioni personali. In secondo luogo, la materia della divulgazione delle informazioni personali private è soggetta al principio di riserva di legge in quanto nucleo centrale di protezione del diritto alla riservatezza, sebbene il diritto alla riservatezza appartenga ai diritti della personalità,

[52] Z. Xinbao (张新宝), *Raccolta di informazioni personali: i limiti dell'applicazione del principio del consenso informato*, in *Studi di diritto comparato*, 2019, 1 ss. e per ampi profili di comparazione Z. Xinbao, *Protezione giuridica del diritto alla riservatezza* (隐私权的法律保护), in *Mass Publishing House*, 1997.

[53] W. Liming (王利明) – C. Xiao (程啸), *Commentario al Codice civile cinese: diritti della personalità*, Beijing, 2020, 392 ss.

così come il diritto alla vita e alla salute, ma differenza dell'inderogabilità assoluta di questi ultimi, può essere derogato in modo condizionato in base alle esigenze di interesse pubblico o di interessi superiori[54]. Tuttavia, la possibile deroga può avvenire solo per legge, in base all'art. 1033[55] del Cod. civ. cin., quale atto approvato dall'Assemblea Popolare Nazionale[56].

L'art. 1033 del Codice stabilisce le regole e le procedure per il trattamento delle informazioni personali, stabilendo che nessuna organizzazione o individuo può trattare le informazioni private di un'altra persona salvo «diversa disposizione di legge o espresso consenso del titolare del diritto» diverso sia dal «consenso implicito», ma anche dal «semplice consenso». In tal senso, il titolare del diritto deve fornire un'esplicita manifestazione di volontà che deve essere una specifica espressione di consenso a specifiche informazioni private, non una vaga o una generica autorizzazione.

La portata del "consenso espresso" del titolare è vincolante per chi lo riceve e la divulgazione di informazioni private deve essere coerente con esso. Per ragioni di efficienza, il "consenso espresso" del titolare del diritto non è limitato alla forma scritta, ma può essere prestato oralmente, salva l'ipotesi prevista dall'art. 15 del Regolamento della Repubblica Popolare Cinese sulla divulgazione di informazioni governative (中华人民共和国政府信息公开条例) pubblicato il 5 aprile 2017 e successivamente emendato il 3 aprile 2019:

> «L'organo amministrativo non deve divulgare informazioni governative che riguardano segreti commerciali, riservatezza personale o altre informazioni la cui divulgazione causerebbe un danno ai legittimi diritti e interessi di terzi. Tuttavia, se i terzi acconsentono alla divulgazione o se l'organo amministrativo ritiene che la mancata divulgazione avrebbe un impatto significativo sull'interesse pubblico, le informazioni devono essere divulgate».

Il riferimento all'interesse pubblico deve essere inteso in senso stretto, a riprova di tale impostazione è l'art. 32 del Regolamento:

> «Qualora la divulgazione di informazioni governative in risposta a una domanda pregiudichi i diritti e gli interessi legittimi di un terzo, l'organo amministrativo chiede

---

[54] Z. Xinbao (张新宝), *Protezione giuridica del diritto alla riservatezza*, cit.

[55] Art. 1033 Cod. civ.cin.: «Salvo diversa disposizione di legge o espresso consenso del titolare del diritto, nessuna organizzazione o individuo deve compiere gli atti di seguito indicati:
(1) intromettersi nella vita privata di un'altra persona tramite telefonate, invio di messaggi di testo, utilizzo di strumenti di messaggistica istantanea, invio di posta elettronica e volantini e simili;
(2) entrare, scattare fotografie o spiare negli spazi privati altrui come la resi- denza o la camera d'albergo di un'altra persona;
(3) scattare fotografie, spiare, intercettare o divulgare le attività private di un'altra persona;
(4) scattare fotografie o spiare le parti intime del corpo di un'altra persona;
(5) elaborare le informazioni private di un'altra persona;
(6) violare la riservatezza di un'altra persona con altri mezzi».
V. anche art. 13 Legge sulla legislazione (立法法, *lìfǎ fǎ*) da ultimo emendata il 13 marzo 2023.

[56] Esempio è costituito dalla Legge sulla sicurezza dello stato (国家安全法*Guójiā ānquán fǎ*) promulgata dall'Assemblea Popolare Nazionale il 1° luglio 2015.

il parere del terzo per iscritto. Il terzo deve presentare il proprio parere entro 15 giorni lavorativi dalla data di ricevimento della richiesta di osservazioni. Se il terzo non presenta il proprio parere entro il termine stabilito, l'organo amministrativo decide se divulgarlo o meno in conformità alle disposizioni del presente Regolamento. Se il terzo non acconsente alla divulgazione e ha ragionevoli motivi per farlo, l'organo amministrativo non divulga le informazioni. Se l'organo amministrativo ritiene che la mancata divulgazione possa avere un impatto significativo sull'interesse pubblico, può decidere di divulgare l'informazione e informare per iscritto il terzo del contenuto e delle ragioni della decisione di divulgare l'informazione governativa».

Certo è che in questo modo è interamente delegata alla discrezionalità dell'autorità amministrativa ogni decisone e valutazione.
Il Codice civile cinese ha elaborato due distinte regole per la tutela della riservatezza e delle informazioni personali ed ha rafforzato la ripartizione tra le loro funzioni a vantaggio della corretta gestione delle controversie nella pratica, dell'equilibrio tra la protezione e l'uso delle informazioni personali e della promozione dello sviluppo economico nell'era digitale. Poiché il diritto alla riservatezza è strettamente connesso alla tutela della dignità umana, qualora si considerassero tutte le informazioni personali come rientranti nell'ambito tutelato dalla riservatezza, dovrebbero al contempo ignorarsi le esigenze della comunicazione interpersonale e le attuali pratiche commerciali, nonché il valore apportato dalla condivisione delle informazioni medesime.

7. Lo specifico ambito delle informazioni personali sensibili

Le informazioni personali sensibili sono definite in termini di informazioni personali che, una volta diffuse o utilizzate illegalmente, possono causare una violazione della dignità personale delle persone fisiche o metterne in pericolo la sicurezza personale e patrimoniale. Se ne menzionano quali esempi, l'art. 6 della Convenzione 108 del Consiglio d'Europa[57]:

«I dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relati-

[57] La Convenzione di Strasburgo del 1981, o anche Convenzione 108 del Consiglio d'Europa è uno dei più importanti strumenti legali per la protezione delle persone rispetto al trattamento automatizzato dei dati personali e l'unico giuridicamente vincolante a livello internazionale in tale materia, potendo ad essa aderire anche Stati non membri del Consiglio d'Europa. La Convenzione 108 scaturisce dall'esigenza di tutela per le persone a seguito del proliferare di tecnologie dell'informazione e comunicazione a partire dagli anni '60. Riguardo all'ambito, si applica a tutti i trattamenti di dati personali effettuati sia nel settore privato che nel settore pubblico, pertanto anche ai trattamenti compiuti da polizia e autorità giudiziaria. La Convenzione ha la finalità di proteggere gli individui da abusi e regolamentare i flussi transnazionali di dati, e trae diretta vocazione dall'articolo 8 della Convenzione europea dei diritti dell'uomo:«Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»)».

> vi alla salute o alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno preveda delle garanzie appropriate. Lo stesso vale per i dati a carattere personale relativi a condanne penali»;

l'art. 9 del GDPR:

> «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona»;

la Legge del Brasile sulla protezione dei dati personali (LGPD, *Lei General de Proteção de Dados*) in vigore dal 18 settembre 2020 che può essere considerata la risposta del Brasile al GDPR con cui ha diverse somiglianze e si occupa dei dati sensibili all'art. 5, c. 2:

> «Ai fini della presente legge si considerano […] dati personali sensibili: i dati personali relativi all'origine razziale o etnica, alle convinzioni religiose, alle opinioni politiche, all'appartenenza sindacale o ad un'organizzazione religiosa, filosofica o politica, i dati relativi alla salute o alla vita sessuale, i dati genetici o biometrici, quando collegati a una persona fisica»;

infine, la Legge del Giappone sulla protezione dei dati personali (*Act on the Protection of Personal Information*) promulgata nel 2003 e da ultimo emendata il 1° aprile 2022, all'art. 2, c. 3, dispone:

> «Ai sensi della presente legge, per "dati personali sensibili" si intendono i dati personali relativi alla razza, al credo, allo stato sociale, all'anamnesi, ai precedenti penali, al fatto di aver subito un danno da reato, o ad altri elementi identificativi o equivalenti prescritti da un'ordinanza del Consiglio dei ministri che richiedono particolare attenzione per non causare ingiuste discriminazioni, pregiudizi o altri svantaggi a tale persona[58]».

Gli Stati Uniti, diversamente, non hanno una definizione unica di dati personali sensibili a livello legislativo federale, ma hanno previsto, in distinti testi normativi, disposizioni speciali per alcune specifiche categorie di essi: si pensi ad esempio agli standard relativi alla riservatezza delle informazioni sanitarie formulati dal Dipartimento della salute e dei servizi umani degli Stati Uniti (*United States Department of Health and Human Services*)[59].

[58] この法律において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう, disponibile in Japanese Law translation.

[59] Da tale approccio si è di recente distaccato lo Stato della California avviandosi ad introdurre una normativa unitaria della materia.

Sebbene il Cod. civ. cin. non adotti direttamente il concetto di informazioni personali sensibili un riferimento è presente nell'art. 1034, c. 3[60]:

> «[…] Le informazioni personali sono quelle registrate elettronicamente o in altri modi che possano essere utilizzati, da soli o in combinazione con altri, per identificare una persona fisica, inclusi nome, data di nascita, numero di carta di identità, in- formazioni biometriche, indirizzo di residenza, numero di telefono, indirizzo *e-mail*, informazioni sanitarie, ubicazione e simili della persona. Alle informazioni personali sensibili si applicano le disposizioni sul diritto alla riservatezza o, in mancanza, si applicano quelle sulla protezione dei dati personali».

Inoltre, l'art. 1035, c. 1, del Cod. civ. cin. stabilisce che il trattamento delle informazioni personali è soggetto al consenso della persona fisica o del suo tutore, il che rappresenta una protezione speciale dei dati dei minori, pertanto, distinguendo tra diversi tipi di informazioni personali e delegando alla Legge sulla protezione delle informazioni personali ogni maggior dettaglio.
Di ausilio per la maggior comprensione di quanto si sta indagando l'art. 2 delle Disposizioni su diverse questioni riguardanti l'applicazione della legge nelle cause civili relative al trattamento delle informazioni personali mediante la tecnologia di riconoscimento facciale (审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定) pubblicate dalla Corte Suprema del Popolo il 1° agosto 2021 che considera qualsiasi violazione delle norme sul trattamento delle informazioni personali come una violazione dei diritti della personalità e dei legittimi interessi degli individui nell'ambito del diritto civile. Di conseguenza, nella prassi giudiziaria hanno iniziato a comparire espressioni quali «diritto di controllare le informazioni personali» nella prospettiva dei diritti della personalità e «contenuto principale del diritto alle informazioni personali quale ambito di dominio e oggetto di decisione autonoma del suo titolare».
L'art. 28 della Legge definisce le informazioni personali sensibili:

> «Le informazioni personali sensibili si riferiscono alle informazioni che potrebbero ledere la dignità personale di qualsiasi persona fisica, o danneggiare la sua sicurezza personale o patrimoniale una volta divulgate o utilizzate illecitamente, comprese le informazioni quali l'identificazione biometrica, il credo religioso, l'identità specifica, lo stato di salute, i conti finanziari, la posizione e le tracce, nonché i dati personali dei minori di 14 anni».

Secondo il metodo della sintesi e della enumerazione, da un lato la disposizione ne definisce chiaramente la nozione, dall'altro pone il parametro di valutazione sul quale identificarne nella pratica i diversi tipi: quello cioè della facilità con cui la loro violazione può danneggiare la dignità personale delle persone fisiche o metterne in pericolo la sicurezza personale e patrimoniale. Il parametro fornisce una base fondamentale per identificare con precisione le informazioni personali sensibili nella pratica; al medesimo tempo, la definizione generalizzata è sufficientemente flessibile e aperta ad accogliere

[60] V. art. 76, c. 5, della Legge sulla sicurezza informatica della Repubblica Popolare Cinese.

tipi di informazioni emergenti ed in rapida evoluzione nell'era digitale in connessione alle esigenze dello sviluppo sociale. L'art. 28 vi include i dati biometrici, le credenze religiose, le identità specifiche, l'assistenza medica e sanitaria, i conti finanziari, gli spostamenti e altre informazioni, nonché le informazioni personali dei minori di 14 anni.
La maggior parte degli ordinamenti adotta il metodo dell'enumerazione delle informazioni personali sensibili, senza specificarne le caratteristiche[61]. La Legge sulla protezione delle informazioni personali, diversamente, ne prevede gli elementi fondamentali per la successiva identificazione, fondando il proprio criterio di qualificazione nella eventuale incidenza sulla dignità personale e la sicurezza della vita e della proprietà, determinando un danno alle persone.
Le informazioni personali dei minori di 14 anni sono incluse tra quelle sensibili[62].
Secondo l'art. 31 della Legge sulla protezione dei dati personali:

> «Per operare il trattamento dei dati personali di un minore di età inferiore ai 14 anni, il responsabile del trattamento deve ottenere il consenso dei genitori o di altri tutori del minore.
> Per operare il trattamento dei dati personali dei minori di età inferiore ai 14 anni, il responsabile del trattamento predisporrà regole specifiche per il trattamento dei dati personali».

il trattamento dei dati personali dei minori richiede il consenso dei loro tutori. Quando tratta le informazioni personali di un minore, il responsabile del trattamento dei dati personali deve verificare se la persona che processa i dati è un minore e se la persona che dà il consenso è il tutore del minore. In teoria, questo è il cosiddetto "obbligo di doppia verifica".
Nel valutare le informazioni personali sensibili occorre, innanzitutto, valutarle sia in base ai parametri legali, sia al contesto. Riguardo ai parametri legali questi devono essere determinati in combinazione con le disposizioni di altra normativa, si pensi, ad esempio all'art. 14 del Regolamento sull'amministrazione del settore creditizio che include il gruppo sanguigno nell'ambito dei dati personali sensibili; oppure all' Interpretazione giudiziaria del riconoscimento facciale che protegge le informazioni del volto quali dati personali sensibili.
La dottrina cinese evidenzia come il contesto debba aiutare a qualificare le informazioni come sensibili o meno[63]. Motivo per cui si dovrebbe adottare tale impostazione è che i cambiamenti sociali e la loro portata incerta impongono questo approccio, confermato anche dall'utilizzo della formulazione aperta dell'art. 28 in cui l'elencazione delle informazioni personali sensibili non è limitata a «l'identificazione biometrica, il credo religioso, l'identità specifica, lo stato di salute, i conti finanziari, agli spostamenti». In futuro, con l'ulteriore sviluppo della società, ci saranno nuovi tipi di informazioni per-

[61] Art. 6 del GDPR, l'art. 5 della Legge generale sulla protezione dei dati del Brasile, l'art. 2 della Legge sulla protezione dei dati personali del Giappone, l'art. 23 della Legge coreana sulla protezione dei dati personali.

[62] Art. 9 del GDPR.

[63] H. Nissenbaum, *Privacy as Contextual Integrity* , in *Washington Law Review*, 2004, 119 ss.

sonali sensibili, quale risultato inevitabile dello sviluppo della scienza e della tecnologia che i giudici saranno chiamati a valutare.
A definire l'ambito di trattamento delle informazioni sensibili interviene l'art. 28, c. 2:

> «Solo per specifiche finalità e sufficienti necessità, e qualora siano state adottate rigorose misure di protezione, il responsabile del trattamento può trattare dati sensibili».

in cui sono fissate condizioni dettagliate riguardo al trattamento dei dati sensibili: in primo luogo, uno scopo specifico; in secondo luogo, una necessità suficiente; in terzo luogo, l'adozione di misure di protezione rigorose. Il principale riferimento tra questi elementi sembra essere la finalità specifica: solo in presenza di una finalità specifica le informazioni personali sensibili possono essere trattate secondo la legge. Tuttavia quello di "specifica finalità" è un concetto incerto e la sua semantica ha un ampio spazio interpretativo per cui è necessario definire ulteriormente ed effettuare una ulteriore analisi. Di aiuto è l'art. 6 della Legge che fissa il principio della limitazione delle finalità del trattamento, vale a dire che qualsiasi trattamento delle informazioni personali deve avere una finalità chiara e ragionevole e il criterio si applica anche alle informazioni sensibili. Tuttavia, vi sono alcune differenze tra le due disposizioni, e lo standard della finalità specifica è più elevato di quello della finalità chiara e ragionevole. Emerge quindi che: i) la finalità specifica nel trattamento delle informazioni personali sensibili debba essere intesa quale finalità specifica e chiara, non una finalità generale; ii) la finalità specifica può essere quella esplicitamente fissata dal legislatore e dalle forze dell'ordine; iii) in base alla finalità fissata dal legislatore, il responsabile del trattamento delle informazioni può trattare le informazioni sensibili in conformità alla legge; iv) il giudizio sulla specificità della finalità non può essere generalizzato. Nel giudicare una finalità specifica, occorre considerare anche l'occupazione e la natura delle attività del responsabile del trattamento e se il trattamento dei dati personali sensibili sia finalizzato a fronteggiare emergenze ed a realizzare interessi pubblici. Naturalmente, anche in queste circostanze, il responsabile del trattamento deve trattare le informazioni sensibili dell'individuo entro i limiti necessari, configurandosi diversamente una condotta illecita, impostazione adottata anche dall' art. 9 del GDPR.
Un ultimo rilievo riguarda il consenso separato. La differenza tra il trattamento delle informazioni personali sensibili e quello delle informazioni personali generali risiede nel fatto che, nel caso in cui si risponda a una finalità specifica, è necessario ottenere anche il consenso e l'autorizzazione individuale dell'interessato, mentre non è previsto il consenso tramite autorizzazione implicita. Le norme generali sul trattamento delle informazioni personali si basano sul consenso dell'interessato, mentre il trattamento delle informazioni personali sensibili prevede che «solo in presenza di uno scopo specifico e di una necessità sufficiente e con l'adozione di rigorose misure di protezione, il responsabile del trattamento dei dati personali possa trattare le informazioni personali sensibili». Inoltre, la Legge sulla protezione delle informazioni personali ha introdotto disposizioni più severe sul consenso e sulla divulgazione delle informazioni personali sensibili, richiedendo che il trattamento di queste sia conforme alle norme separate sul

consenso. Le ragioni di questa disposizione sono che, da un lato, i requisiti di obbligo per i responsabili del trattamento delle informazioni sono stati ulteriormente innalzati e la raccolta di informazioni personali sensibili è stata rigorosamente limitata mediante un'autorizzazione separata per prevenire la violazione delle informazioni personali sensibili. Dall'altro, per l'interessato, la modalità di autorizzazione individuale può anche renderlo consapevole dei rischi causati dall'autorizzazione, in modo da agire con cautela e rafforzare la consapevolezza della tutela dei diritti.
L'art. 29 della Legge migliora i requisiti del principio del consenso informato nella protezione delle informazioni personali. Secondo questa disposizione, il consenso per il trattamento delle informazioni personali sensibili deve essere individuale secondo questi tre aspetti: il consenso deve essere separato, pertanto è vietata una autorizzazione generalizzata; la regola del consenso separato richiede che il responsabile del trattamento abbia un chiaro obbligo di informazione; la regola del consenso separato dovrebbe implementare la regola della restrizione del rifiuto di fornire servizi.

8. Privacy con caratteristiche cinesi

Lo studio della materia, i principi, i requisiti ed i contenuti delle disposizioni della normativa della Repubblica Popolare Cinese mostrano come si sia attinto a modelli preesistenti. Tuttavia, alcuni profili della Legge, tra cui quello della localizzazione dei dati, sono tra i caratteri maggiormente distintivi della impostazione adottata dalla Cina, ambito in cui la normativa mostra la maggior parte della propria specificità. L'approccio del modello degli Stati Uniti, tra i più forti oppositori alla localizzazione dei dati, percepita come una barriera commerciale, risulta essere il più semplice, in quanto non esistono requisiti specifici per il trasferimento di informazioni personali ad un Paese terzo. L'approccio del modello dell'Unione europea seppur maggiormente restrittivo, non prevede l'obbligo di localizzazione dei dati, i trasferimenti transfrontalieri di dati potendo avvenire, infatti, solo qualora rispettino il livello di protezione stabilito dal GDPR, quindi, verso Paesi terzi con un livello di protezione dei dati che la Commissione europea riconosce come equivalente a quello dell'Unione europea, o utilizzando garanzie appropriate quali clausole contrattuali standard o attraverso le *binding corporate rules*. La Cina, attraverso una lettura di insieme della normativa, ma in modo particolare degli artt. 1 e 37 della Legge sulla sicurezza della rete imposta il proprio modello:

> «La presente legge è elaborata al fine di garantire la sicurezza informatica, di proteggere la sovranità del ciberspazio, la sicurezza nazionale e l'interesse pubblico, di salvaguardare i legittimi diritti ed interessi dei cittadini, delle persone giuridiche e delle altre organizzazioni e di promuovere un sano sviluppo dell'informatizzazione dell'economia e della società».
> «Gli operatori di infrastrutture di informazioni essenziali che raccolgono e generano o producono informazioni personali e dati sensibili all'interno della Repubblica Popolare Cinese devono assicurarne l'archiviazione e la memorizzazione all'interno della Repubblica Popolare Cinese. Se per concrete esigenze commerciali, è

> necessario fornirli o trasmetterli al di fuori dei confini nazionali è richiesta un'opportuna valutazione sulla sicurezza dell'operazione, effettuata secondo le modalità formulate congiuntamente dall' Amministrazione per la sicurezza del ciberspazio e dal dipartimento competente del Consiglio degli Affari di Stato. Nel caso leggi o regolamenti amministrativi dovessero prescrivere diversamente, si applicheranno questi ultimi».

L'impostazione prescelta non è presente né nella normativa della Unione europea né in quella degli Stati Uniti ma diversamente in quella Russa – riferimento strico del legislatore cinese in particolare in alcune fasi di costruzione dell'ordinamento giuridico - specificatamente nella Legge federale Russa n. 242 FZ, in vigore dal 1° settembre 2015, successivamente emendata il 2 dicembre 2019 ed in vigore dal 13 dicembre 2019. La posizione proclamata dal legislatore cinese sulla localizzazione dei dati è che essa protegge la privacy delle persone ma al medesimo tempo la propria sovranità, lo sviluppo economico della Cina e riduce al minimo la sua esposizione a fattori esterni. Tratto saliente è, tuttavia, la disuguaglianza tra il rafforzamento della protezione delle informazioni personali rispetto ad azioni di entità private e il contestuale e parallelo aumento dell'intromissione da parte del governo. Mentre il diritto alla riservatezza e alla tutela delle informazioni personali è stato oggetto di una evoluzione a favore dei singoli e dei consumatori, criticità e fragilità persistono nel rapporto cittadino - governo[64]: la normativa tutela sempre più i diritti delle persone contro le entità private che detengono i loro dati e ne garantisce un maggiore controllo ma i benefici derivanti da questi progressivi miglioramenti sono attenuati dall'accresciuto accesso del governo ai dati dei singoli, impostazione confermata dall'art. 28 della Legge sulla sicurezza della rete, art. 28:

> «Gli operatori di rete devono fornire supporto tecnico e assistenza alle autorità di pubblica sicurezza e alle autorità di sicurezza nazionale che, in conformità della legge, operano a salvaguardia della sicurezza della nazione e che indagano sulle attività criminali».

La *ratio* alla base della normativa cinese è diversa da quella dei due modelli dell'Unione europea e degli Stati Uniti: la prima obbligata ad adottare un elevato livello di protezione dei dati, tutela garantita quale diritto fondamentale sia verso entità private sia verso il governo; negli Stati Uniti la protezione della privacy, diversamente, è concepita prima di tutto, quale protezione verso le attività governative, verso il potere dello Stato, ancor prima che verso le entità private. Quello che emerge è il diverso concepimento in Cina dei diritti dei singoli in cui il riconoscimento di questi ultimi è comunque superato dall'interesse superiore dello Stato. La Cina, anche in questo settore del diritto, ha varato una propria normativa con "caratteristiche cinesi". I macro poli che hanno orientato il legislatore sono, come di consueto i due sistemi di Civil law e Common law,

[64] Sul diritto amministrativo cinese di interesse le relazioni di studiosi cinesi contenute in E. Toti, *Leggi tradotte della Repubblica Popolare Cinese, XIII, Legge sul processo amministrativo, Legge sulle sanzioni amministrative, Legge sul riesame amministrativo*, Milano, 2021.

nello specifico ambito rappresentati da Europa e Stati Uniti da cui si è attinto, sempre in modo selettivo e ragionato, al fine di varare un proprio modello in grado di mantenere bilanciati i diversi interessi coinvolti in questo complesso macrosistema.

Note a sentenza

Le azioni collettive tra *data protection* e tutela consumeristica al vaglio della Corte di giustizia

Lavinia Vizzoni

Corte di giustizia, 28 aprile 2022, C-319/20, *Meta Platform Ireland c. Associazione federale delle organizzazioni e associazioni di consumatori, Germania*

L'art. 80, par. 2, 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 (regolamento generale sulla protezione dei dati), deve essere interpretato nel senso che esso non osta ad una normativa nazionale che consente ad un'associazione di tutela degli interessi dei consumatori di agire in giudizio, in assenza di un mandato che le sia stato conferito a tale scopo e indipendentemente dalla violazione di specifici diritti degli interessati, contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali, facendo valere la violazione del divieto di pratiche commerciali sleali, la violazione di una legge in materia di tutela dei consumatori o la violazione del divieto di utilizzazione di condizioni generali di contratto nulle, qualora il trattamento di dati in questione sia idoneo a pregiudicare i diritti riconosciuti da tale regolamento a persone fisiche identificate o identificabili.

Sommario

1. Premessa: dalla "commercializzazione" alla "consumerizzazione" dei dati personali – 2. Il caso di specie – 3. *Segue*. Le conclusioni della Corte – 4. Diritto dei consumatori e *data protection* – 5. Il rilievo della direttiva (UE) 2019/770 e della *privacy by design* – 6. Le ragioni di una tutela collettiva integrata ... e non solo.

Keywords

data protection – azioni collettive – consumatori – privacy *by design* – tutela integrata

[*] Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

1. Premessa: dalla "commercializzazione" alla "consumerizzazione" dei dati personali

Il dibattito sulla protezione dei dati personali si è sensibilmente evoluto e sta oggi vivendo una nuova stagione.

Dopo che, sull'onda di spinte provenienti essenzialmente dal legislatore unionale, il dato personale è stato inserito a pieno nella dinamica negoziale, la discussione si concentra ora sulla riconduzione dell'operazione economica rappresentata dal rilascio del consenso al trattamento in cambio della concessione di un servizio o di scontistica sul prezzo dello stesso nell'ambito di un rapporto di consumo[1]. Dal fenomeno studiato dalla dottrina e descritto come "commercializzazione" o "patrimonializzazione" dei dati personali[2] si è passati dunque allo studio dell'intersezione tra *data protection* e *consumer protection* – un tempo considerate discipline separate e oggi invece alleate nella prospettiva di garantire una "tutela multilivello" dell'interessato-consumatore[3] – che presenta molteplici risvolti di estrema rilevanza: dalla contestualizzazione dei dati personali nell'ambito delle dinamiche contrattuali, alle sovrapposizioni e/o integrazioni sul versante rimediale.

La sentenza della Corte di giustizia dell'UE in commento[4] è di recente intervenuta a

---

[1] G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, 137 ss., P.F. Giuggioli, *Tutela della privacy e consumatore*, in E. Tosi (a cura di), *Privacy digitale*, *Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, 264 ss., C. Alvisi, *Dati personali e diritti dei consumatori*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 669 ss. Di recente, con specifica attenzione alla garanzia di conformità, v. R. Grisafi, *Il dato personale come presunto corrispettivo economico e le nuove fonti di integrazione eteronome del contratto nella fornitura di contenuti e servizi digitali. Il caso della disciplina della garanzia di conformità*, in *Judicium*, 2022.

[2] Il tema è particolarmente discusso in dottrina. Fra i vari contributi in materia cfr. V. Ricciuto, *L'equivoco della* privacy. *Persona Vs dato personale*, Napoli, 2022, 105 ss., R. Senigaglia*, La dimensione patrimoniale del diritto alla protezione dei dati personali,* in *Contr. impr.*, 2020, 760 ss., V. Ricciuto, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, 95 ss., G. Resta, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la direttiva (UE) 2019/770 e il regolamento (UE) 2016/679, in* A. D'Angelo - V. Roppo (a cura di), *Annuario del contratto 2018*, Torino, 2019, 128 ss.*,* G. Resta - V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, 411 ss., A. De Franceschi, *La circolazione dei dati personali tra* privacy *e contratto*, Napoli, 2017, *passim*.

Correlato anche se non integralmente sovrapponibile al profilo della commercializzazione è il tema della "proprietarizzazione" dei dati personali, su cui v. N. Purtova, *The Illusion of Personal Data as No One's Property: Reframing the Data Protection Discourse, in Law, Innovation and Technology*, 2015, 87 ss., C. Camardi, *Cose, beni e nuovi beni, tra diritto europeo e diritto interno*, in *Eur. dir. priv.*, 2018, 955 ss.; H. Zech, *Data as a Tradeable Commodity*, in A. De Franceschi (a cura di), *European Contract Law and the Digital Single Market*, Cambridge-Antwerp-Portland, 2016, 51 ss., V. Janeček. - G. Malgieri, *Commerce in Data and the Dynamically Limited Alienability Rule*, in *German Law Journal,* 2020, 929 ss.

[3] A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2017, 2 ss., F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. impr.*, 2019, 34 ss., Id., *La «compravendita» di dati personali?*, in *Dir. Internet*, 2020, 521 ss.

[4] Per un riferimento a questa specifica pronuncia proprio nel quadro della «c.d. dottrina delle protezioni multilivello, già sposata dalle corti ed autorità di vigilanza nazionali», v. R. Montinaro, *I sistemi di raccomandazione nelle interazioni tra professionisti e consumatori: il punto di vista del diritto dei consumi (e non solo)*, in *Pers. mercato*, 2022, 354.

La decisione è stata di recente oggetto di analisi da parte di M. Federico, *Rappresentanza degli interessati, diritti individuali e* group data protection, in *Pers. mercato*, 2022, 674 ss.

meglio definire le interferenze e sovrapposizioni che si manifestano fra le due discipline, aggiungendo nuovi spunti di riflessione a quelli già offerti, sul piano del diritto interno, da altre pronunce giurisprudenziali[5] nonché da decisioni delle autorità amministrative competenti[6].

Di particolare interesse è l'angolatura affrontata dalla decisione, che consente di considerare un aspetto ancora poco analizzato, relativo all'estensione collettiva della tutela in favore del consumatore-*data subject*. La pronuncia interviene proprio a meglio definire la portata della legittimazione che le associazioni a tutela dei consumatori hanno ad agire, e nello specifico ad avviare azioni inibitorie, contro possibili lesioni della protezione dei dati personali degli interessati, ponendo il problema della tutela rappresentativa in prospettiva preventiva.

2. Il caso di specie

Nel caso in esame, dinanzi al giudice nazionale si contrapponevano Meta Platform Ireland – già Facebook Ireland, titolare del trattamento dei dati personali degli utenti del relativo *social network* nell'ambito dell'UE – e l'Unione federale delle associazioni dei consumatori tedesca, che, sulla scorta di una legge nazionale entrata in vigore antecedentemente al regolamento (UE) 2016/679 (GDPR)[7], aveva intrapreso un'azione contro Meta, ritenendo illegittima la modalità di raccolta del consenso al trattamento

[5] Si v. la nota Cass. civ., sez. I, 2 luglio 2018, n. 17278, in *Nuova giur. civ. comm.*, 2018, 1775 ss., con commento di F. Zanovello, *Consenso libero e specifico alle email promozionali*, e in *Giur. it.*, 2019, 530 ss., con nota di S. Thobani, *Operazioni di* tying e *libertà del consenso*. Per un'ampia e meditata indagine sul tema C. Irti, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, 61 ss.

[6] Cfr. il provvedimento dell'AGCM Facebook-condivisione dati con terzi, 29 novembre 2018, n. 27432, con il quale l'autorità ha confermato che l'uso dei dati degli utenti per finalità di *marketing* configura un «rapporto di consumo tra il professionista e l'utente che utilizza i servizi di [Facebook] (tramite sito e app), anche in assenza di corrispettivo monetario» e ha contestato a Facebook due condotte ritenute pratiche commerciali scorrette. Sulla vicenda si sono pronunziate le sentenze coeve Tar Lazio, Sez. I, 10 gennaio 2020, n. 260 e Tar Lazio, Sez. I, 10 gennaio 2020, n. 261, in *Giur. it.*, 2021, 321 ss., con nota di C. Solinas, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*. Alle sentenze gemelle del Tar è seguita poi la pronuncia del Cons. Stato, Sez. VI, 29 marzo 2021, n. 2631, che ha confermato la decisione del Tar, anche se con argomentazioni che appaiono in parte divergenti.
Ampie riflessioni sulle decisioni dei giudici amministrativi in v. F. Bravo, *La «compravendita» di dati personali?*, cit., 2020, 521 ss. L'A. esamina le due pronunce del Tar Lazio e, pur apprezzando proprio la coesistenza e compatibilità, rilevata da esse, di discipline diverse (*data protection*, diritto contrattuale generale e diritto consumeristico *sub specie* di disciplina in materia di pratiche commerciali sleali), tale da dar luogo a una cumulabilità delle tutele in favore dell'interessato-contraente-consumatore, critica però la riconduzione, operata dalle pronunce stesse, della pattuizione in oggetto allo schema della compravendita, che viene ritenuta semplicistica e fuorviante. Sulla decisione del Consiglio di Stato v. inoltre R. Pardolesi - A. D'Avola, *Protezione dei dati personali, tutela della concorrenza e del consumatore (alle prese con i 'dark pattern'): parallele convergenti?,* in *Foro it.*, 2021, 338 ss. e G. Scorza, *Facebook non è gratis*? in *Dir. Internet*, 2021, 547 ss.

[7] Secondo la legge tedesca del 2001, chiunque violi disposizioni volte a tutelare i consumatori (leggi sulla tutela dei consumatori), può essere soggetto a un'ingiunzione di astensione dalla condotta lesiva per l'avvenire nonché ad un ordine di cessazione immediata della condotta lesiva nell'interesse della tutela dei consumatori. Per leggi sulla tutela dei consumatori si intendono in particolare le disposizioni che disciplinano la liceità: a) della raccolta dei dati personali di un consumatore da parte di un'impresa, o b) del trattamento o dell'utilizzo di dati personali di un consumatore raccolti da un imprenditore.

operato da Facebook di tali dati degli utenti.
In particolare, l'associazione consumeristica lamentava una violazione della normativa tedesca in materia di protezione dei dati personali, costituente al tempo stesso una pratica commerciale sleale ai sensi dell'art. 5 della direttiva 2005/29/CE, una violazione di una legge in materia di tutela dei consumatori[8] e una violazione del divieto di utilizzazione di condizioni generali di contratto nulle[9].
Premesso che Facebook ospita regolarmente app che mettono gratuitamente a disposizione dell'utente giochi forniti da terzi, previo consenso da parte dell'utente medesimo al trattamento di alcuni dati personali, come ad esempio il punteggio ottenuto, la versione tedesca del *social network* ospitava una app che induceva l'utilizzatore, accettando le condizioni generali dell'applicazione, ad autorizzare anche la pubblicazione di informazioni ulteriori, quali il proprio *status*, le proprie foto e il proprio nome. Da questa specifica situazione ha avuto origine l'azione inibitoria dell'associazione contro Meta, rivolta ad interrompere la prosecuzione delle condotte consistenti nella pubblicazione dei suddetti dati personali aggiuntivi.
Dopo due gradi di giudizio favorevoli all'associazione rappresentativa dei consumatori, davanti alla Cassazione tedesca (*Bundesverfassungsgericht*) si è posta la questione relativa alla capacità dell'associazione stessa di intraprendere un giudizio pur senza aver ricevuto uno specifico mandato da parte di un utente, alla luce dell'entrata in vigore del GDPR nelle more del giudizio.
Soprattutto, ci si domandava se la legittimazione ad agire dell'associazione consumeristica – che secondo il giudice del rinvio sussisteva alla data della presentazione del suo ricorso ai sensi della legge tedesca – fosse venuta meno in corso di giudizio, a seguito dell'entrata in vigore del GDPR ed in particolare del relativo art. 80.
Pertanto, la Corte nazionale ha sospeso il procedimento principale e ha sottoposto alla Corte di giustizia la questione pregiudiziale relativa alla possibilità o meno, per una associazione a tutela dei consumatori, di agire in giudizio contro l'autore di atti anche solo potenzialmente pregiudizievoli rispetto alla tutela dei dati personali, operando così in via anticipata rispetto alla concreta violazione dei dati personali di una persona anche in difetto di uno specifico mandato.
La vicenda ha dunque ad oggetto il seguente nodo centrale: se l'associazione tedesca a tutela dei consumatori possa o meno agire contro Meta pur in assenza di un mandato che le sia stato conferito a questo scopo e indipendentemente da che siano avvenute in concreto violazioni di specifici diritti degli interessati.

3. *Segue*. Le conclusioni della Corte

Nella propria decisione, la Corte offre *in primis* un'efficace ricognizione del pure scarso

[8] In particolare era contestata la violazione dell'art. 13, par. 1, del *Telemediengesetz* (legge sui media elettronici), del 26 febbraio 2007, applicabile, secondo quanto rilevato dalla decisione in commento, fino all'entrata in vigore del GDPR, e poi sostituita proprio dagli art. da 12 a 14 del GDPR stesso. È significativo, nella vicenda in questione, come la violazione consumeristica contestata coincida in effetti a pieno con la lesione di diritti del *data subject*.

[9] Il divieto è sancito dal par. 307 del BGB.

contesto normativo delineato dal GDPR, il cui capo VIII disciplina i mezzi di ricorso che consentono la protezione dei diritti dell'interessato.

Come noto, la tutela dei diritti dell'interessato può essere reclamata direttamente da questi oppure da un ente legittimato, in presenza o in assenza di un mandato a tal fine, ai sensi dell'art. 80. Inoltre, in base al par. 2 di tale norma, gli Stati membri possono prevedere che qualsiasi organismo, organizzazione o associazione, indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre un reclamo dinanzi all'autorità di controllo, ai sensi dell'arti. 77, e di esercitare i diritti di cui agli artt. 78 e 79, qualora esso ritenga che i diritti di cui un interessato gode a norma del regolamento siano stati violati[10].

Come ricordato dalla pronuncia, in forza dell'articolo 288 TFUE, ma *in primis* in ragione della natura stessa dei regolamenti in quanto fonti del diritto dell'UE, le disposizioni dei regolamenti producono un effetto immediato negli ordinamenti giuridici nazionali e non richiedono misure di applicazione o recepimento. Ciò non esclude comunque che talune previsioni, pur inserite in regolamenti, possano richiedere, per la loro attuazione, l'adozione di misure di applicazione da parte degli Stati membri[11].

Proprio questo è il caso dell'art. 80, par. 2, GDPR, il quale lascia agli Stati membri un margine di discrezionalità relativamente alla sua attuazione. In particolare, come rilevato dalla Corte di giustizia, affinché l'azione rappresentativa senza mandato in materia di protezione dei dati personali possa essere esercitata, è necessario che gli Stati membri facciano uso della facoltà loro offerta di prevedere nel loro diritto nazionale tale modalità di rappresentanza degli interessati.

Ovviamente, come osservato anche dall'avvocato generale nelle sue conclusioni, gli Stati membri che si avvalgano di tale facoltà dovranno farlo in modo da non pregiudicare il contenuto e gli obiettivi del regolamento.

Nel caso di specie, il legislatore tedesco non aveva adottato, a seguito dell'entrata in vigore del GDPR, alcuna disposizione di attuazione interna dell'art. 80, par. 2. In effetti, la normativa nazionale in discussione nel procedimento principale era in vigore già nel 2001, e permetteva alle associazioni di tutela degli interessi dei consumatori di agire in giudizio contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali. Si trattava dunque di verificare se tale normativa nazionale rientrasse nel margine di discrezionalità riconosciuto a ciascuno Stato membro dall'art. 80, par. 2, GDPR.

Ora, come ricordato dalla Corte, tale disposizione fissa determinati requisiti relativi all'ambito di applicazione *ratione personae* e *ratione materiae* che gli Stati membri – i quali disciplinino un meccanismo di azione rappresentativa contro il presunto autore di

---

[10] Sull'art. 80 GDPR, v. F. Casarosa, *La tutela aggregata dei dati personali nel Regolamento UE 2016/679: una base per l'introduzione di rimedi collettivi?*, in A. Mantelero - D. Poletti (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, 235 ss.

[11] CGUE, C-645/19*, Facebook Ireland e a.* (2021), § 110 nonché la giurisprudenza ivi citata. Questa evenienza, infatti, è stata da tempo giudicata compatibile con l'art. 249 TCE dalla Corte di giustizia la quale ha stabilito che «l'applicabilità diretta di un regolamento non impedisce che il testo stesso del regolamento conferisca il potere a una istituzione comunitaria o a uno Stato membro di adottare misure di esecuzione». CGUE, C-230/78, Ue, *Eridania* (1979). Sulla non autosufficienza dei regolamenti cfr. F. Astone, *Il processo normativo dell'Unione Europea e le procedure nazionali per l'esecuzione degli obblighi comunitari*, Torino, 2008, 109.

un atto pregiudizievole per la protezione dei dati personali – dovranno rispettare. A siffatto vaglio viene dunque sottoposta la legislazione tedesca in questione, la quale, benché precedente all'entrata in vigore del GDPR, ad avviso della Corte deve risultare conforme alle norme da quest'ultimo dettate.

Per quanto riguarda l'ambito di applicazione *ratione personae*, la legittimazione ad agire spetta ad un organismo, ad un'organizzazione o ad una associazione che soddisfi i criteri elencati indicati all'art. 80, par. 1. In particolare, si fa riferimento a «un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali»[12]. E la Corte di giustizia ritiene che un'associazione di tutela degli interessi dei consumatori come l'Unione federale, «può rientrare in tale nozione in quanto persegue un obiettivo di interesse pubblico consistente nell'assicurare i diritti e le libertà degli interessati nella loro qualità di consumatori, posto che la realizzazione di un tale obiettivo può essere correlata alla protezione dei dati personali di questi ultimi».

La Corte riconosce esplicitamente il profondo collegamento che unisce, da un lato, le violazioni a danno dei consumatori e/o le istanze di contrasto alle pratiche commerciali sleali – che possono essere perseguite tramite il ricorso ad azioni inibitorie collettive – e dall'altro, le violazioni della normativa in materia di protezione dei dati personali dei consumatori coinvolti da questo tipo di pratiche.

Relativamente all'ambito di applicazione *ratione materiae* del meccanismo di cui all'art. 80, par. 2, GDPR, la Corte segnala la necessità che l'ente che agisce, indipendentemente da qualsiasi mandato che gli sia stato conferito, ritenga violati i diritti di un interessato, a seguito di un trattamento di dati a cui il *data subject* è stato sottoposto, e evidenzia come ai fini dell'esercizio dell'azione rappresentativa da parte dell'ente non si possa richiedere che l'ente stesso proceda alla previa identificazione della persona specificamente interessata da un trattamento di dati asseritamente contrario alle disposizioni del GDPR.

A tal fine, viene significativamente richiamata la nozione di «interessato», ai sensi dell'art. 4, punto 1 GDPR, che comprende non soltanto una «persona fisica identificata», ma anche una «persona fisica identificabile». Secondo la pronuncia, la semplice individuazione di una categoria o di un gruppo di persone pregiudicate dal trattamento lesivo può essere sufficiente ai fini della proposizione di suddetta azione rappresentativa.

Inoltre, aggiunge la decisione, l'esercizio di questa azione rappresentativa non è neppure subordinato all'esistenza di una violazione concreta dei diritti dell'interessato produttiva di conseguenze pregiudizievoli, bensì presuppone soltanto che l'ente di cui trattasi «ritenga» che i diritti di un interessato siano stati violati da un trattamento dei suoi dati personali contrario alle disposizioni del GDPR. Non è dunque necessario dimostrare che l'interessato abbia subito un danno reale, in una data situazione, a causa

[12] I requisiti che siffatte associazioni devono possedere presentano una indubbia vicinanza – specie con riguardo all'assenza di scopo di lucro – alle caratteristiche che devono rivestire i nuovi intermediari dei dati previsti dal regolamento (UE) 868/2022 (*Data Governance Act*). In argomento D. Poletti, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 2 ss.

della lesione dei suoi diritti.
D'altronde, come chiarito, una simile interpretazione è conforme allo stesso obiettivo fondamentale del GDPR, che si propone di assicurare un elevato livello di protezione del diritto di qualsiasi interessato alla tutela dei dati personali che lo riguardano.
La conclusione, pacifica, della Corte, è che la violazione di una norma relativa alla protezione dei dati personali può simultaneamente comportare la violazione di norme relative alla tutela dei consumatori o l'applicazione della disciplina sulle pratiche commerciali sleali. Pertanto, l'art. 80 par. 2, GDPR non osta a che le associazioni di tutela degli interessi dei consumatori possano agire contro violazioni dei diritti previsti dal GDPR anche tramite norme aventi per finalità la tutela dei consumatori o la lotta contro le pratiche commerciali sleali, e l'azione collettiva potrà essere esercitata indipendentemente sia dal riscontro di specifiche lesioni dei diritti del *data subject* sia dal conferimento di mandati relativi.

4. Diritto dei consumatori e *data protection*

La questione affrontata dalla Corte di giustizia si era già posta all'attenzione del tribunale commerciale di Vienna, che, con una decisione del 26 maggio 2021 ha stabilito che le azioni promosse da un ente collettivo austriaco per la tutela dei consumatori possono essere basate anche su violazioni del GDPR, nonostante la mancata attuazione dell'art. 80, par. 2, del GDPR in Austria[13]. Nel caso austriaco l'attività con la quale si combinano i dati degli utenti con un *data set* di un altro titolare del trattamento è stata ritenuta una condotta illegittima, a causa, tra l'altro, della mancanza di base giuridica del trattamento[14] e della violazione del principio di accuratezza.
Secondo l'orientamento austriaco, l'art. 80 GDPR si applica direttamente nei singoli stati dell'UE a prescindere dalla sussistenza di una norma nazionale di armonizzazione legislativa. Si tratta di una conclusione ancora più incisiva di quella a cui è giunta la Corte di giustizia nel caso in esame, poiché, come accennato, nell'ordinamento austriaco mancano specifici riferimenti normativi, anche antecedenti al GDPR – presenti invece nell'ordinamento tedesco – che legittimino un'azione collettiva consumeristica diretta contro violazioni della *data protection*.
In sostanza, nel caso austriaco, l'estensione della legittimazione ad agire collettivamente da parte delle associazioni a tutela dei consumatori anche dinanzi alle violazioni in materia dei dati personali è stata ritenuta automatica.
A tale conclusione si è giunti attraverso la valorizzazione del considerando 42 del GDPR, che contiene un esplicito riferimento alla direttiva sulle clausole abusive nei contratti con i consumatori (93/13/CEE). Invero, siffatta valorizzazione appare forse persino eccessiva, dal momento che il richiamo alla direttiva 93/13/CEE è limitato

[13] Una sintesi in inglese della decisione austriaca è reperibile nel sito gdprhub.eu.

[14] Sull'art. 6 del GDPR cfr. M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 221 ss. e L. Bolognini, *Basi giuridiche del trattamento*, in L. Bolognini - E. Pelino - C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 93 ss.

all'affermazione della necessità che la dichiarazione di consenso sia predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e soprattutto che non contenga clausole abusive[15].

Non che manchino, comunque, significativi punti di contatto fra la disciplina consumeristica e quella in materia di dati personali. È ben possibile, ed anzi frequente, la sovrapposizione, o meglio la moltiplicazione di ruoli di un soggetto che sia, al contempo, contraente-consumatore e *data subject*.

Ed in effetti *data protection* e *consumer protection* non risultano così distanti, in termini di *rationes* e tecniche rimediali che improntano le relative discipline; anzi, si riscontra una certa vicinanza fra i due ambiti, e, in tale direzione, come già anticipato, viene da qualche tempo invocata una maggiore compenetrazione, almeno a livello rimediale, fra diritto consumeristico e legislazione in materia di trattamento dei dati personali.

In verità, una differenza di base si riscontrerebbe con riguardo al versante applicativo[16], laddove, se è vero che l'interessato deve essere indefettibilmente una persona fisica – al pari del consumatore – il GDPR presenta un ambito di applicazione più ampio della disciplina consumeristica, in quanto non conosce limitazioni concernenti lo scopo perseguito dall'interessato. È pur vero, però, che nei casi qui in considerazione, la tutela consumeristica si applica al dato quando questo è "ceduto" (*rectius*, quando il consenso al trattamento dello stesso è rilasciato) in cambio di un servizio, quindi proprio quando il *data subject* compie un atto di consumo in senso stretto.

In ogni caso, semplificando, entrambe le normative, quella in materia di *consumer protection* e quella sulla *data protection*, possono essere lette, in ottica unificante, come volte alla regolazione di un mercato in cui occorre garantire un'effettiva tutela tanto dei consumatori, soggetti strutturalmente deboli, quanto dei loro dati personali, nel più ampio contesto finalizzato alla corretta costruzione di un mercato unico digitale[17]. In definitiva, anche la disciplina in tema di protezione dei dati personali, pur avente ad oggetto la proiezione di un diritto fondamentale della persona, nell'intento del legislatore unionale si pone anch'essa nel quadro dell'assicurazione del regolare funzionamento del mercato[18].

---

[15] Lo scrutinio di vessatorietà almeno sulla dichiarazione di consenso dell'interessato appare ulteriormente incoraggiato proprio dal considerando 42 del GDPR, secondo cui «In conformità della direttiva 93/13/CEE del Consiglio è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive». Più in generale, sulla possibilità che anche la *privacy policy* e la dichiarazione di consenso dell'interessato possano contenere clausole da reputarsi vessatorie ai sensi del codice del consumo v. P.F. Giuggioli, *Tutela della* privacy *e consumatore, cit.*, 275, S. Thobani, *I requisiti del consenso al trattamento dei dati personali,* Santarcangelo di Romagna, 2016, 109 e già F. Bilotta, *Consenso e condizioni generali di contratto,* in V. Cuffaro - V. Ricciuto - V. Zeno-Zencovich (a cura di), *Il trattamento dei dati personali*, Torino, 1998, 103.

[16] P.F. Giuggioli, *Tutela della* privacy *e consumatore,* cit.*,* 264 ss.

[17] C. Alvisi, *Dati personali e diritti dei consumatori*, cit., 675-676. In proposito, anche la Comunicazione *Strategia per il mercato unico digitale* della Commissione europea del 6 maggio 2015.

[18] In materia consumeristica, v. la puntuale analisi critica di C. Camardi, *La protezione dei consumatori tra diritto civile e regolazione del mercato. A proposito dei recenti interventi sul codice del consumo*, in *Jus civile*, 2013, 305 ss. Cfr. anche Id., *Contratti con i consumatori e contratti tra imprese. Rilievi critici sul paradigma dell'asimmetria contrattuale*, in Aa.Vv., *Il diritto civile oggi*, Napoli, 2006, 893 ss. Con precipuo riguardo all'avvicinamento al settore della *data protection* cfr. M. Ratti, *Personal Data and Consumer Protection: What do They Have in*

Conferma l'avvicinamento del trattamento dei dati personali al fenomeno consumeristico, nel segno della standardizzazione, il fatto che anche il trattamento stesso – come meglio si dirà in seguito – ha ormai assunto le vesti di un fenomeno di massa[19].
Altro significativo elemento di vicinanza fra le discipline in questione riguarda il rilievo in esse attribuito all'informazione[20]. Quello che da tempo è un principio cardine della materia consumeristica[21], e che già era presente al legislatore della direttiva 95/46/CE, oggi permea significativamente la disciplina del GDPR[22], che fa continui richiami all'esigenza non solo che le informazioni necessarie siano fornite all'interessato, ma anche che tali informazioni siano connotate da semplicità e comprensibilità, con uso di formule che riecheggiano l'approccio paternalistico[23] – pure da taluni ampiamente contestato – caratteristico del settore consumeristico. Come puntualmente osservato, chiarezza e semplicità delle informazioni diventano in tal modo pilastri di un sano sistema informativo, essenziale per la circolazione sia dei beni e servizi di consumo, sia del corretto trattamento de dati personali[24].
Ancora, potrebbe individuarsi un altro fondamento comune tra le due normative nell'attenzione posta alla sicurezza[25]: da un lato il proclamato «diritto fondamentale» dei consumatori alla sicurezza e alla qualità dei prodotti e dei servizi (art. 2, lett. b), cod. cons.)[26], dall'altro l'enfasi posta dal GDPR sull'obbligo del titolare di adottare le opportune misure di sicurezza (art. 32), in un'ottica pienamente conforme al principio di "responsabilizzazione"[27].

5. Il rilievo della direttiva (UE) 2019/770 e della *privacy by design*

Le "interferenze", in ottica di reciproca integrazione fra *consumer protection* e *data protection* si fanno ancor più consistenti se si considera la direttiva (UE) 2019/770, relativa

Common?, in Aa. Vv., *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, Berlino, 2018, 377 ss.

19 S. Thobani, *Diritti della personalità e contratto. Dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Torino, 2019, *passim*.

20 Sui relativi punti di contatto v. P.F. Giuggioli, *Tutela della* privacy *e consumatore*, cit., 268 ss.

21 R. Senigaglia, *Informazione contrattuale nella net economy*, in *Eur. dir. priv.*, 2002, 229 ss., e più di recente l'analisi, sebbene limitata ai contenuti della direttiva 2011/83/UE, di R. Alessi, *Gli obblighi di informazione tra regole di protezione del consumatore e diritto contrattuale europeo uniforme e opzionale*, in *Eur. dir. priv.*, 2013, 311 ss. Cfr. anche, con riguardo all'informazione in fase precontrattuale, T. Febbrajo, *La fase preliminare al rapporto di consumo: informazione, educazione e pubblicità*, in G. Villanacci, *Manuale di diritto del consumo*, Napoli, 2007, 69 ss.

22 Si v. l'art. 7, ma anche i considerando 42 e 58 GDPR.

23 R. Caterina, *Paternalismo e antipaternalismo nel diritto privato*, in *Riv. dir. civ.*, 2005, 771 ss. e Id., *Architettura delle scelte e tutela del consumatore*, in *Cons. dir. mercato*, Argomenti, 2, 2012, 73 ss.

24 P.F. Giuggioli, *Tutela della* privacy *e consumatore*, cit., 273.

25 C. Alvisi, *Dati personali e diritti dei consumatori*, cit., 719 ss.

26 F. Cafaggi, *Product safety, private standard setting and information networks, EUI Working Papers, Law*, 2008, 4 ss.

27 Sull'*accountability* v. G. Finocchiaro, *Il principio di* accountability, in *Giur it.*, 2019, 2778 ss.

a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, attuata, nel diritto interno, col d.lgs. n. 173/2021, che ha inserito nel codice del consumo il nuovo «Capo I-*bis* – Dei Contratti di fornitura di contenuto digitale e di servizi digitali», che contiene gli articoli 135 *octies* e ss.

In realtà il decreto attuativo non sposta, o meglio non implementa i termini della questione dell'intreccio fra *data protection* e *consumer protection*, limitandosi a riprodurre pedissequamente i contenuti degli articoli della direttiva, e perdendo in parte quell'ispirazione più ampia che la direttiva esprimeva anche nei propri considerando.

La direttiva resta comunque solido punto di riferimento per avanzare riflessioni in materia.

L'impianto normativo della direttiva infatti, prendendo atto delle potenzialità, ma anche dei rischi che si profilano per il consumatore, in contesti tecnologicamente avanzati, ha come obiettivo quello di conseguire diritti contrattuali nazionali pienamente armonizzati in determinati settori chiave.

Premesso che la direttiva in esame è connotata da un ambito applicativo più circoscritto della direttiva 93/13/CE – concernente, quest'ultima, tutti i contratti stipulati con i consumatori – essa sembra segnare un'evoluzione della tutela consumeristica.

In effetti, l'articolato normativo allude ad un'ampia valutazione che è da compiersi sul regolamento contrattuale nel suo complesso, il quale dovrà risultare *in primis* conforme ai requisiti fissati dalla direttiva stessa. La valutazione di conformità da operarsi sui contenuti contrattuali non si arresta tuttavia ai requisiti per così dire "interni" alla direttiva, ma si spinge oltre, sino a postulare la piena corrispondenza anche ai requisiti che scaturiscono da un vero e proprio "corpo normativo esterno", ossia il GDPR[28].

La difformità del contenuto o del servizio digitale può provenire dunque anche dal mancato allineamento con la normativa in materia di trattamento di dati personali.

Dunque, la conformità alla direttiva (UE) 2019/770 è conformità anzitutto del contratto di fornitura; e, dal momento che la direttiva fa esplicito riferimento agli obblighi previsti dal GDPR, in caso di conflitto, alla relativa prevalenza di questa disciplina sulla direttiva stessa, se ne ricava che anche la mancata conformità del contenuto/servizio digitale agli obblighi previsti in materia di *data protection* integra una difformità, *sub specie* di difetto di conformità oggettivo, ai sensi della direttiva (UE) 2019/770.

Peraltro, il considerando 48 è esplicito nel fare riferimento proprio ai « ... casi in cui la mancata conformità agli obblighi di cui al regolamento (UE) 2016/679 potrebbe allo stesso tempo rendere il contenuto digitale o il servizio digitale inadeguato alla sua finalità prevista e costituire pertanto un difetto di conformità ai requisiti di conformità oggettivi, che prevedono che il contenuto digitale o il servizio digitale sia adeguato alle finalità per le quali è abitualmente utilizzato un contenuto digitale o un servizio digitale dello stesso tipo».

D'altronde, se l'art. 16, c. 2, della direttiva (UE) 2019/770 (art. 135-*noviesdecies*, c. 3, cod. cons.) definisce il regolamento (UE) 2016/679 vincolante in caso di risoluzione del contratto di fornitura del contenuto o servizio digitale, non si vede perché non rendere altrettanto vincolanti i requisiti della *data protection* già in fase di perfezionamento del contratto.

[28] V. oggi art. 135-*novies,* c. 6, cod. cons.

In tale prospettiva, le irregolarità parametrate su un diverso corpo normativo diverrebbero fonte di difetto di conformità del contenuto/servizio digitale ai sensi della relativa direttiva, con le conseguenti applicazioni dei rimedi da essa previsti. In altri termini, il ripristino della conformità dei beni e dei servizi di consumo garantirà l'esecuzione di prestazioni contrattuali prive di vizi sotto il profilo della protezione dei dati.
I requisiti previsti dalla direttiva (UE) 2019/770 viaggiano dunque su un doppio binario: uno interno alla direttiva stessa (art. 6 ss.) e uno esterno, coincidente con gli obblighi della *data protection*.
Si tratterebbe di una lettura d'altronde a sua volta pienamente conforme con il principio cardine, proclamato dal GDPR, della *privacy by design*[29], nel senso che l'effettiva conformità al GDPR dovrà concretizzarsi innanzitutto nelle scelte di progettazione del servizio o del bene[30], il quale dovrà essere strutturato ad esempio sulla minimizzazione dei dati raccolti, o sull'uso di tecniche di crittografia e/o pseudonimizzazione, per quanto possibile, nella trasmissione degli stessi all'*Internet Service Provider*.
Si tratta allora di immettere sul mercato un prodotto o servizio che risulti non solo rispondente ai requisiti di conformità puntualmente prescritti, ma, più in generale, *compliant* dal punto di vista dei trattamenti dei dati.
La *data protection* dovrà dunque acquisire un ruolo autonomo appunto nel *design*, inteso come progettazione ma anche come applicazione di opportune *business policies* o strategie organizzative finalizzate alla realizzazione di un servizio/contenuto digitale conforme.
Da ciò deriverebbe anche un significativo incoraggiamento, in favore dei produttori, verso l'adozione di criteri di tipo proattivo, anziché reattivo, nell'ottica appunto di prevenire potenziali lesioni ai danni degli interessati. In questa direzione, la nozione di sicurezza del prodotto da tenere a riferimento non è più la mera sicurezza informatica o la sicurezza del solo processo di trattamento dei dati, ma, in un'ottica più ampia, la sicurezza che deriva dalla garanzia del rispetto dei diritti e delle libertà fondamentali della persona, che dall'operatività di quel servizio o prodotto possono essere compromessi.

6. Le ragioni di una tutela collettiva integrata … e non solo

La necessità di adottare un approccio non escludente, ma integrato, che combini principi e tutele consumeristiche e della *data protection*, è confermata significativamente anche un passaggio della direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio del 25 novembre 2020 relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE[31]. Nel considerando 13

[29] Sulla c.d. *privacy by design*, v. G. D'Acquisto - M. Naldi, Big Data *e* Privacy by Design. *Anonimizzazione, Pseudonimizzazione, Sicurezza*, Torino, 2017, 31 ss.

[30] Nonostante i più scarsi richiami al GDPR, simili considerazioni possono considerarsi valevoli anche per i beni digitali di cui alla direttiva (UE) 2019/771, sulla cui attuazione cfr. G. De Cristofaro, *Verso la riforma della disciplina delle vendite mobiliari b-to-c: l'attuazione della dir. Ue 2019/771*, in *Riv. dir. civ.*, 2021, 205 ss.

[31] Tale direttiva, in vigore dal 24 dicembre 2020, deve essere applicata negli Stati membri a partire dal

di tale Direttiva si legge infatti che «nel settore dei servizi digitali il mercato al consumo ha subito un'evoluzione e vi è una crescente necessità di applicare in modo più efficace il diritto dei consumatori, comprese le norme in materia di protezione dei dati» ed è prevista l'applicazione della direttiva stessa nelle ipotesi in cui sia violata una norma del regolamento (UE) 2016/679, che «tuteli l'interesse dei consumatori», e l'interessato sia un consumatore.

La considerazione dell'interessato-consumatore e la logica "combinata" prospettata in termini di tutele, inducono a riflettere sull'angolatura di aggregazione, fortemente incentivata dalla sentenza in esame, che si appunta sulla dimensione collettiva della tutela offerta ai soggetti coinvolti, così da contribuire al raggiungimento dell'obiettivo finale consistente nella strutturazione di un sistema di protezione efficace dell'utente[32].

D'altronde, a monte, è la stessa capacità offensiva della società tecnologica a manifestare uno sviluppo in termini massivi e seriali; ed in tal senso gli eventuali illeciti perpetrati anche dai giganti del *web* sono destinati a colpire folle di danneggiati indefinite, che sfuggono alle maglie dei rimedi a base individualistica come quello aquiliano[33]. La scarsa utilità dell'azione del singolo contro i *Big Players* è poi di tutta evidenza.

La stessa Corte di giustizia, nella decisione in commento, evidenzia la maggiore efficacia di un'azione collettiva, precisando che «l'esercizio di una siffatta azione rappresentativa, consentendo di prevenire un gran numero di violazioni dei diritti degli interessati a seguito del trattamento dei loro dati personali, potrebbe rivelarsi più efficace del ricorso che un'unica persona individualmente e concretamente pregiudicata da una violazione del suo diritto alla protezione dei suoi dati personali può esperire contro l'autore di tale violazione».

Sono in effetti sempre più numerosi gli studi, anche nello specifico settore dei dati personali e specie in materia di *Big Data*, che evidenziano la necessità di guardare all'orizzonte collettivo dell'utilizzo dei dati e delle forme di protezione degli interessati. Ed ancora, nell'ottica della compenetrazione fra *data protection* e *consumer protection*, è l'ingresso dei consumatori nel mercato dei dati personali a portare con sé, inevitabilmente, il ricorso a strumenti di tutela collettiva, i quali traggono origine proprio dal settore consumeristico.

In un contesto in cui il *data subject* è considerato non nella sua individualità, ma come punto di riferimento di informazioni, la cui aggregazione è utile per lo svolgimento di attività ulteriori, come la profilazione di massa, lo scopo delle limitazioni poste alla commercializzazione dei dati personali pare dunque essere, oltre alla tutela del singolo, quello di evitare che grazie alla mole di informazioni raccolte i titolari del trattamento pongano in essere condotte pregiudizievoli per la collettività, al fine di garantire un più corretto funzionamento del mercato[34].

---

25 giugno 2023. Sul punto, cfr. C. Angiolini, *Trattamento dei dati personali e rapporto di consumo: dalla dir. 1993/13 alla dir. 2020/1828*, in G. Salvi (a cura di), *Il diritto contrattuale dei consumi ed i suoi attuali confini*, Napoli, 2022, 27 ss.

[32] Sul punto v. il commento di M. Federico, *Rappresentanza degli interessati, diritti individuali e* group data protection, cit., 676 ss.

[33] Cfr. A. Mantelero, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, in *Computer Law & Security Rev.*, 2016, 245 ss.

[34] Così S. Thobani, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in questa *Rivista*, 3,

È comunque evidente che ad offese "di massa" meglio si risponda con strumenti di azione e tutela a loro volta collettivi.

A maggior ragione una simile conclusione potrebbe valere laddove l'accennato percorso di massificazione e "spersonalizzazione" riguardi i dati stessi che, nei contesti aggregati possono divenire anonimi. La raccolta di grandi quantitativi di dati è infatti idonea a generare il fenomeno del c.d. *Group Privacy*, il quale può condurre persino ad escludere l'applicazione del GDPR, nonché le relative tutele spettanti al *data subject*, posto che può essere difficile identificare la corrispondenza tra il diritto leso e il titolare dello stesso[35]. Laddove venga allora meno lo status di *data subject* e permanga quello di consumatore, resterebbe la possibilità di ricorrere, in generale, almeno a tutele collettive contro le lesioni subite dal consumatore.

Considerato che il quadro normativo in materia di azioni collettive è destinato a mutare nel percorso di recepimento della direttiva (UE) 2020/1828, vi è però, almeno a livello nazionale, un riferimento di sicuro rilievo, dato dalla l. 31/2019[36]. La riforma italiana operata nel 2019 – che interviene anche nel tentativo di correggere i fallimenti della previgente normativa[37] – presenta una portata assai ampia e riscrive, in sostanza, la disciplina di due tipologie di azioni collettive, ossia l'azione di classe e l'azione inibitoria collettiva, entrambe oggi regolate all'interno del codice di procedura civile, agli artt. 840-*bis* ss. La collocazione sistematica delle previsioni in questione rende evidente l'intento di rendere le azioni collettive italiane un rimedio dotato di portata generale, essendo caduti i limiti soggettivi e oggettivi posti dall'art. 140-*bis,* c. 2, cod. cons.

Non a caso, con specifico riguardo all'azione di classe, l'art. 840-*bis* c.p.c. prevede l'azionabilità per la tutela di qualsiasi tipo di diritti individuali, purché non più collettivi ma omogenei. L'azione in questione

realizza l'unione in un unico procedimento di situazioni sostanziali individuali esercitate cumulativamente: l'obiettivo sembra essere quello di istituire una vera e propria complementarità tra azione individuale e azione di classe, senza che le due azioni siano legate da rapporti gerarchici.

Con precipuo riguardo al settore della *data protection*, nonostante la proliferazione delle violazioni diffuse dei diritti degli interessati e, più in generale, delle prescrizioni in materia, e nonostante gli ampi margini applicativi lasciati dall'art. 80 GDPR, la possibilità per i *data subject* di azionare forme di tutela aggregata è disciplinata specificamente soltanto in alcuni Stati membri, fra cui non rientra l'Italia[38].

E allora, la decisione in commento potrebbe valere a prospettare conclusioni significative specie sul versante applicativo della tutela collettiva in favore del consumatore-in-

2019, 131 ss.

[35] B. Mittelstadt, *From Individual to Group Privacy in Big Data Analytics*, in *Philos. Technol.*, 2017, 30, p. 475 ss. V. inoltre, *supra*, nota 33.

[36] Sull'inibitoria v. in particolare M. Stella*, La nuova azione inibitoria collettiva* ex *art. 840* sexiesdecies *c.p.c. tra tradizione e promesse di deterrenza*, in *Corr. Giur.*, 2019, 1453 ss. e, più in generale sull'azione di classe cfr. C. Consolo, *La terza edizione della azione di classe è legge ed entra nel c.p.c. Uno sguardo d'insieme ad una amplissima disciplina*, in *Corr. giur.*, 2019, 737 ss.

[37] A.D. De Santis, *L'azione di classe a dieci anni dalla sua entrata in vigore*, in *Foro it.*, 2019, 2180 ss.

[38] F. Casarosa, *La tutela aggregata dei dati personali nel Regolamento UE 2016/679: una base per l'introduzione di rimedi collettivi?*, cit., 237.

teressato.

D'altronde, come sopra ricordato, la Corte di giustizia ha riconosciuto la legittimazione dell'associazione consumeristica ad agire – pur in assenza di mandato e anche di violazioni concrete – sulla base di una legge tedesca antecedente al GDPR. Addirittura, la corte austriaca, per quanto si tratti di un giudice di merito, ha avallato tale legittimazione persino in assenza di una specifica legge che disciplinasse l'azione collettiva per violazioni della normativa in materia di protezione di dati personali.

Nel nostro ordinamento, si potrebbero trarre argomenti a sostegno di un'interpretazione che consenta di ritenere l'art. 80, par. 2, GDPR direttamente applicabile, pur in assenza di specifiche normative attuative, ma semplicemente sulla scorta delle norme già in vigore, in particolare degli stessi art. 840-*bis* ss. c.p.c. già inseriti nel diritto interno dalla riforma del 2019 – nonostante l'assenza in essi di richiami espressi alle violazioni in materia di dati personali – e, più in generale, in conformità con la sopra delineata ottica integrata di protezione.

La portata della pronuncia in esame potrebbe peraltro risultare più ampia di quanto appaia ad una prima lettura e schiudere ad un'alternativa ulteriore, rispetto al pure valido approccio integrato delle violazioni e delle correlative tutele[39].

In un passaggio delle conclusioni della pronuncia si legge infatti che le associazioni di tutela degli interessi dei consumatori sono legittimate ad agire «contro violazioni dei diritti previsti dal GDPR per il tramite, *eventualmente*[40], di norme aventi per finalità la tutela dei consumatori o la lotta contro le pratiche commerciali sleali». Il passaggio appare di notevole rilevanza: con esso la Corte sembra in effetti alludere al fatto che non necessariamente la tutela collettiva dei diritti degli interessati debba passare attraverso ulteriori, connesse violazioni di norme poste a tutela dei consumatori, anche nella forma delle pratiche commerciali sleali. Se ne potrebbe cioè ricavare che il cumulo delle violazioni – della *data protection* da un lato e, dall'altro, della *consumer protection* e/o della disciplina sulle pratiche commerciali sleali – e dunque la correlativa integrazione delle tutele, sia solo, appunto, eventuale.

Ciò avrebbe ricadute pratiche di non poco conto. Premesso che è quanto mai verosimile che violazioni dei principi della *data protection* concretizzino anche lesioni dei diritti del consumatore e condotte rilevanti ai fini delle pratiche commerciali sleali, si potrebbe ipotizzare che le associazioni rispettose dei requisiti di cui all'art. 80, par. 2, GDPR attive non come nel caso di specie nella materia consumeristica bensì esclusivamente nel settore della protezione dei dati personali, possano agire collettivamente per la tutela dei diritti dei data *subject*, indipendentemente da che le condotte lesive del titolare del trattamento integrino violazioni di ulteriori discipline. D'altronde, come ricordato, lo specifico riferimento dell'art. 80, par. 2, GDPR è proprio a associazioni attive «nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali»[41].

---

[39] Sull'integrazione delle tutele e dei rimedi v. M. Federico, *Rappresentanza degli interessati, diritti individuali e* group data protection*,* cit., 678 ss.

[40] Il corsivo è aggiunto.

[41] È pur vero che anche nei paesi in cui si è provveduto a dare maggiore concretezza alla previsione del regolamento (UE) 2016/679, la normativa di riferimento applicata è quella dedicata alla tutela del

consumatore estesa anche alla tutela dei dati personali. È il caso della *actione de groupe* francese, che, come riporta F. Casarosa, *La tutela aggregata dei dati personali nel Regolamento UE 2016/679: una base per l'introduzione di rimedi collettivi?,* cit., 237.

Diritto alla deindicizzazione e notizie false: la Corte di giustizia precisa i confini tra oblio e libertà di espressione*

Giulia Napoli

Corte di giustizia, 8 dicembre 2022, C-460/20, *TU, RE c. Google*

Nell'ambito del bilanciamento che occorre effettuare tra i diritti di cui agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, da un lato, e quelli di cui all'art. 11 della Carta dei diritti fondamentali, dall'altro, ai fini dell'esame di una richiesta di deindicizzazione rivolta al gestore di un motore di ricerca e diretta a ottenere l'eliminazione, dall'elenco dei risultati di una ricerca, del link verso un contenuto che include affermazioni che la persona che ha presentato detta richiesta ritiene inesatte, tale deindicizzazione non è subordinata alla condizione che la questione dell'esattezza del contenuto indicizzato sia stata risolta, almeno provvisoriamente, nel quadro di un'azione legale intentata da detta persona contro il fornitore di tale contenuto.
Nell'ambito del bilanciamento che occorre effettuare tra i diritti di cui agli artt. 7 e 8 della Carta dei diritti fondamentali, da un lato, e quelli di cui all'art. 11 della Carta dei diritti fondamentali, dall'altro, ai fini dell'esame di una richiesta di deindicizzazione rivolta al gestore di un motore di ricerca e diretta ad ottenere l'eliminazione, dai risultati di una ricerca di immagini effettuata a partire dal nome di una persona fisica, delle fotografie visualizzate sotto forma di miniature raffiguranti tale persona, occorre tener conto del valore informativo di tali fotografie indipendentemente dal contesto della loro pubblicazione nella pagina Internet da cui sono state tratte, prendendo però in considerazione qualsiasi elemento testuale che accompagna direttamente la visualizzazione di tali fotografie nei risultati della ricerca e che può apportare chiarimenti riguardo al loro valore informativo.

Sommario

1. Introduzione. Un nuovo capitolo del filone giurisprudenziale europeo sulla fisionomia del diritto alla deindicizzazione. – 2. I fatti di causa e i quesiti in via pregiudiziale. – 3. La decisione della Corte. – 4. Lo *status quo* e le difficoltà connesse all'*enforcement* privato del diritto alla deindicizzazione. - 5. Considerazioni conclusive.

*Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

1. Introduzione. Un nuovo capitolo del filone giurisprudenziale europeo sulla fisionomia del diritto alla deindicizzazione

Con la sentenza in commento la Corte di giustizia è tornata, a distanza di alcuni anni, a pronunciarsi su un tema che, come pochi altri, affonda le sue radici nella elaborazione giurisprudenziale: lo statuto giuridico del diritto alla deindicizzazione, declinazione del diritto all'oblio o alla cancellazione, secondo la terminologia normativa del regolamento (UE) 2016/679 ("GDPR"). Sebbene il fondamento normativo di questo istituto sia stato individuato dalla stessa giurisprudenza nelle disposizioni della direttiva 95/46/CE, prima che il GDPR lo rendesse ancora più esplicito, è innegabile che la fisionomia del diritto alla deindicizzazione in ambito digitale sia stata plasmata soprattutto grazie al contributo della Corte di giustizia, non a caso ritenuta protagonista di una stagione di "attivismo"[1] che non le ha risparmiato alcune critiche[2]. Se nelle precedenti "puntate" la Corte si era focalizzata sul riconoscimento di un diritto azionabile nei confronti dei motori di ricerca[3] e sulla sua estensione territoriale[4] (tuttora controversa[5]), in quest'ultimo capitolo la Corte si è soffermata più puntualmente su un profilo che era stato denunciato come carente nella precedente giurisprudenza, ossia il rapporto con la libertà di espressione (già additato invero come nodo critico del bilanciamento affidato, in prima battuta, ai motori di ricerca)[6].

L'occasione per questa nuova pronuncia è stata offerta da una domanda in via pregiudiziale sollevata dalla Corte federale di giustizia tedesca che si appuntava proprio su questo delicato crinale finora non affrontato compiutamente dalla Corte di giustizia. Il

[1] O. Pollicino, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della carta di Nizza nel reasoning di Google Spain,* in G. Resta – V. Zeno Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015, 7 ss., spec. 13-14, definisce l'operazione interpretativa operata dalla Corte di giustizia, alla luce di un «dettato normativo rimasto invariato», una «lettura estensiva, o meglio manipolativa» del diritto vigente, volto all'identificazione di un «*digital (Internet based) right to data protection*» in senso quasi assoluto. Sul tema dell'attivismo giurisprudenziale in relazione alla tutela dei diritti nella dimensione digitale, più in generale, v. anche O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet – A Road Towards Digital Constitutionalism?*, Londra, 2021.

[2] O. Pollicino*, Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi.it*, 3, 2014: «Tutte le volte in cui gli stati membri dimostrano di non voler progredire nel percorso di arricchimento dell'acquis comunitario per via legislativa, ecco che la Corte di giustizia indossa, con una certa disinvoltura, va detto, i panni del *judge made law* e accelera per via giurisprudenziale.» scrive Pollicino. «(...) con le due decisioni tra aprile e maggio del 2014 (...) sembra emergere la chiara volontà, da parte degli stessi giudici, di prendere molto (forse troppo) sul serio la protezione di un nuovo *digital right to privacy*». Sul punto, anche M. Bassini - O. Pollicino, *Reconciling right to be forgotten and freedom of information in the digital age. Past and future of personal data protection in the EU*, in *DPCE,* 2, 2014, 641 ss.

[3] CGUE, C-131/12, *Google Spain* (2014).

[4] CGUE, C-507/19, *Google v. CNIL* (2019).

[5] Così Cass. civ., sez. I, ord. 24 novembre 2022, n. 34658, che ne ha ingiunta l'applicazione di fuori dei confini europei. Tra gli altri, v. G. Boschetti*, Diritto all'oblio senza confini territoriali: un'altra sfida del GDPR*, in *ntplusdiritto.ilsole24ore.com,* 1° dicembre 2022.

[6] Tra gli altri, le criticità legate al bilanciamento con il diritto alla libertà di espressione sono state affrontate da F. Paolucci, *La guerra alla disinformazione nella sentenza T-125/2022 della Corte di Giustizia dell'Unione Europea*, in *diritticomparati.it,* 28 settembre 2022; più in generale v. anche O. Pollicino*, La prospettiva costituzionale sulla libertà di espressione nell'era di Internet,* in questa *Rivista*, 1, 2018, 48 ss.

procedimento principale verteva sulla richiesta di due soggetti, avanzata nei confronti di Google, di eliminare il link che, nella ricerca per nome, riconnetteva ad articoli di carattere informativo da loro ritenuti inesatti, e quindi diffamanti. Dinanzi al diniego opposto dal motore di ricerca, i ricorrenti percorrevano tutti i gradi di giudizio interni; avendo ottenuto sempre risposta negativa, giungevano alla Corte federale di giustizia, dalla quale è scaturito il rinvio pregiudiziale. La Corte di giustizia, operando il complesso bilanciamento tra diritto all'informazione e diritto alla protezione dei dati personali, ha affermato che, per evitare di sacrificare *in toto* un diritto a favore di un altro, laddove si adducesse la falsità o l'inesattezza di dati online, occorre che sia l'interessato a fornire una prova della mancata precisione e correttezza dei dati. Tale onere probatorio si deve sostanziare, secondo la Corte, nella dimostrazione della "manifesta inesattezza", adducendo le prove che "ragionevolmente" si ritiene possa portare[7]. Spetterà *in primis* al motore di ricerca il gravoso ma ampissimo onere di decidere se un contenuto sia meritevole o meno di deindicizzazione, in rapporto alla libertà di espressione e informazione. La Corte ha così tracciato le coordinate di un bilanciamento finora rimasto inesplorato[8], con un apporto importante ma non privo di criticità.

2. I fatti di causa e i quesiti in via pregiudiziale

T.U. e R.E., coppia di imprenditori tedeschi, agivano in giudizio nel 2015 lamentando l'avvenuta lesione della loro reputazione, a loro dire imputabile a Google, nella sua qualità di fornitore di un servizio di motore di ricerca. La società statunitense, secondo i ricorrenti, sarebbe stata responsabile del danno così arrecato per essersi opposta alla loro richiesta di deindicizzare i link verso una serie di articoli che si esprimevano negativamente sul loro conto. Le pubblicazioni in questione erano opera del sito web "g-net", gestito dalla società statunitense G LLC, che dichiaratamente si occupa di «contribuire in modo durevole, attraverso un'informazione attiva e una costante trasparenza, alla prevenzione della frode sul piano economico e sociale»[9]. In questo senso

[7] La Corte, al § 68 della sentenza in esame, afferma che al fine di evitare che sull'interessato gravi un onere eccessivo tale soggetto dovrà limitarsi a fornire gli elementi di prova «che, tenuto conto delle circostanze del caso di specie, si può ragionevolmente richiedere» a quest'ultimo di ricercare al fine di dimostrare tale inesattezza manifesta. «A tal riguardo – continua la Corte – tale persona non può essere tenuta, in linea di principio, a produrre, fin dalla fase precontenziosa, a sostegno della sua richiesta di deindicizzazione presso il gestore del motore di ricerca, una decisione giurisdizionale ottenuta contro l'editore del sito Internet in questione, fosse pure in forma di decisione adottata in sede di procedimento sommario». Ma non può essere tenuta neppure a presentare una richiesta di ingiunzione contro l'editore dell'articolo contenente le informazioni in questione, perché costituente parimenti un "onere eccessivo": sul punto, O. Gstrein, *The Right to be Forgotten in 2022: Luxembourg judges keep surfing the legislative void,* in Verfassungsblog, 20 dicembre 2022.

[8] Il tema è stato perlopiù esplorato dalla giurisprudenza della Corte EDU con riguardo alla rimozione, e non tanto alla deindicizzazione, di notizie tratte da archivi online nel bilanciamento tra art. 10 CEDU e art. 8 (inteso come tutela della reputazione). Al riguardo, si veda M. Bassini - O. Pollicino, *Libertà di espressione e diritti della personalità nell'era digitale. La tutela della privacy nella dimensione europea,* in G.E. Vigevani – O. Pollicino – C. Melzi d'Eril – M. Cuniberti – M. Bassini, *Diritto dell'informazione e dei media*, Torino, 2022, spec. 125 ss.

[9] CGUE, C-460/20, cit., §18.

si orientavano anche le tre pubblicazioni oggetto della controversia, volte a presentare «in modo critico il modello di investimento attuato»[10] dalle società amministrate dai ricorrenti. In particolare, il secondo dei due articoli messi in rete era corredato da alcuni scatti in miniatura (*thumbnails*) che ritraevano i due imprenditori intenti in pose poco sobrie, in cui facevano sfoggio di un certo sfarzo, divisi tra elicotteri, automobili di lusso e aeroplani. I due assumevano, senza presentare elementi di prova a sostegno di tale tesi[11], che nei tre articoli si ravvisassero «informazioni inesatte ed opinioni diffamatorie» sul loro conto, domandandone la rimozione dai risultati di ricerca generati di Google, in virtù del loro diritto all'oblio. La richiesta non otteneva però alcun seguito poiché Google, innanzitutto, si appellava al «contesto professionale[12] in cui si inserivano gli articoli e le fotografie controverse nel procedimento principale» (§21), facendo leva sulla natura informativa del sito riportante i dati in questione. Essendo contenuti di carattere informativo, la loro deindicizzazione avrebbe potuto ledere il diritto degli utenti ad accedervi e a essere così informati. Ma non solo: Google sosteneva anche e soprattutto la propria mancata conoscenza in ordine alla «pretesa inesattezza delle informazioni» ivi contenute, in quanto non dovuta e comunque non agevole[13]. Stante il rifiuto del motore di ricerca, nel 2015 T.U. e R.E. adivano il Landgericht Köln, il Tribunale del Land tedesco di Colonia, chiedendo che venisse imposto al motore di ricerca di cancellare dai propri elenchi nei risultati di ricerca i link verso gli articoli controversi, ma anche di non rendere più possibile la visualizzazione delle miniature in cui essi erano ritratti, visibili nella ricerca per loro nome. Tuttavia, nel 2017 il Tribunale si pronunciava negativamente, respingendo il ricorso. Gli imprenditori interponevano quindi appello avverso la sentenza di primo grado, ribadendo le loro richieste all'Oberlandesgericht Köln, il Tribunale superiore del Land, che però con sentenza dell'8 novembre 2018 respingeva a sua volta la domanda. Il giudice d'appello sottolineava come l'onere della prova circa l'esattezza del fatto asserito incombesse in capo al soggetto richiedente la deindicizzazione. Non avendo essi presentato, nel caso di specie, alcuna dimostrazione circa l'inesattezza dei fatti riferiti al loro riguardo, Google sarebbe stata da considerarsi impossibilitata a effettuare una precisa valutazione della veridicità dei contenuti oggetto degli articoli. Per questo motivo, il motore di ricerca non potrebbe ritenersi obbligato a procedere alla loro deindicizzazione. I ricorrenti nel procedi-

[10] *Ibidem*

[11] Corte di giustizia dell'Unione europea, Comunicato stampa n. 61/22, *Secondo l'avvocato generale Pitruzzella, una domanda di deindicizzazione basata sulla pretesa falsità delle informazioni obbliga il gestore del motore di ricerca ad effettuare le verifiche che rientrano nelle sue concrete possibilità*, Lussemburgo, 7 aprile 2022.

[12] Nel quadro del bilanciamento da effettuarsi, ai sensi dell'art. 17, par. 1 e 3, del GDPR, il diritto a informare e il diritto a essere informati possono assumere un peso prevalente rispetto ai diritti fondamentali tutelati dagli artt. 7 e 8 della Carta. «(...) militano nel senso di una tale prevalenza (...) anche il contesto professionale e la natura giornalistica delle pubblicazioni in questione»: così le Conclusioni dell'Avvocato Generale Pitruzzella, 7 aprile 2022, C-460/20, § 29.

[13] La Corte ricorda, infatti, al § 52, che il gestore di un motore di ricerca non è responsabile del fatto che i dati personali compaiano in una data pagina Internet pubblicata da terzi; è responsabile, piuttosto, «dell'indicizzazione di tale pagina e, in particolare, della visualizzazione del link verso di essa nell'elenco dei risultati presentati agli utenti di Internet in esito ad una ricerca effettuata a partire dal nome di una persona fisica». Non può e non deve vagliare l'autenticità e la rispondenza al vero dei contenuti che si limiti a proporre nella ricerca sulla propria rete.

mento principale proponevano allora ricorso per Cassazione (*Revision*) alla Corte federale di giustizia tedesca (Bundesgerichtshof). Quest'ultima riteneva però necessario domandare alla Corte di giustizia la corretta interpretazione del diritto dell'Unione rilevante. Segnatamente, la Corte federale domandava alla Corte di giustizia l'esatta interpretazione da attribuire all'art. 17, par. 3, lett. a), del GDPR, ma anche degli artt. 12, lett. b), e 14, lett. a), della previgente direttiva 95/46/CE[14], letti alla luce degli artt. 7, 8, 11 e 16 della Carta dei diritti fondamentali dell'Unione europea. Il giudice del rinvio ha così chiesto alla Corte di giustizia di pronunciarsi sull'esegesi di queste disposizioni per la risoluzione di due questioni: in primo luogo, quella concernente l'attribuzione dell'onere probatorio rispetto alla *probanda* inesattezza delle informazioni riportate negli articoli di cui si chiedeva la deindicizzazione. «Si porrebbe quindi la questione» – secondo la Corte federale tedesca – «se spettasse loro (i ricorrenti) provare l'asserita inesattezza di tali affermazioni oppure, quantomeno, dimostrare che tale inesattezza è in una certa misura evidente o se, invece, Google avrebbe dovuto o presumere l'esattezza delle affermazioni dei ricorrenti nel procedimento principale oppure cercare di chiarire essa stessa i fatti»[15]. Secondo il Bundesgerichtshof, non potrebbero dirsi egualmente e correttamente bilanciati i diritti fondamentali concorrenti se l'onere della prova finisse per gravare esclusivamente o sugli attori o sui convenuti. La Corte federale proponeva di «adottare una soluzione diretta a imporre all'interessato di risolvere almeno provvisoriamente la questione dell'esattezza del contenuto indicizzato facendo valere in giudizio il suo diritto nei confronti del fornitore di contenuti»[16]. In altri termini, secondo il giudice del procedimento principale, se gli interessati fossero provvisti di un titolo giudiziario, intimante la deindicizzazione dei contenuti controversi, la questione circa l'esattezza o meno delle informazioni ivi riportate potrebbe forse dirsi risolta, almeno temporaneamente.

In secondo luogo, il giudice del rinvio ha chiesto alla Corte di giustizia di esprimersi sulla questione concernente la deindicizzazione delle fotografie in miniatura ritraenti i ricorrenti. Nello specifico, nell'elenco dei risultati di una ricerca per immagini vengono visualizzate soltanto le miniature, le cosiddette "*thumbnails*", difettando in toto gli elementi del contesto nel quale tale pubblicazione si inserisce. La Corte federale ha quindi rilevato che tale circostanza renderebbe la visione delle fotografie priva di ragioni di tutela, poiché, essendo le miniature private del contesto di riferimento, esse non rientrerebbero nell'alveo della tutela del diritto d'informazione. Se però si consi-

[14] Per quanto riguarda il primo articolo citato, ci si trova nell'alveo del diritto all'oblio, in particolare nel rapporto con la libertà di espressione e informazione: il par. 3 eleva quest'ultima, infatti, a limite dello stesso diritto a essere dimenticati, stabilendo la "disapplicazione" dei paragrafi precedenti nel caso in cui il trattamento dei dati sia necessario, tra gli altri, per l'esercizio del diritto alla libertà di espressione e di informazione. L'art. 12 della direttiva 95/46/CE invece, attribuiva a ciascun interessato il diritto di ottenere dal responsabile del trattamento l'accesso ai propri dati personali, potendo richiederne la rettifica, la cancellazione o il congelamento, in particolare proprio a causa del «carattere incompleto o inesatto dei dati». Da ultimo, l'art. 14, lett. a), della medesima direttiva sanciva il riconoscimento del diritto della persona interessata di opporsi al trattamento dei propri dati, in qualsiasi momento, per motivi preminenti e legittimi derivanti dalla sua situazione particolare, salvo disposizione contraria prevista dalla normativa nazionale.

[15] CGUE, C-460/20, cit., § 29.

[16] Ivi, §31.

derasse il contesto iniziale di pubblicazione, quelle immagini assumerebbero un ruolo fondamentale, contribuendo a corroborare il contenuto che gli articoli si proponevano di trasmettere. Per tali ragioni, il giudice del rinvio ha posto alla Corte di giustizia il secondo quesito, volto a comprendere se, nell'ambito di valutazione dell'ammissibilità della domanda di deindicizzazione delle fotografie in miniatura, si debba tener conto "in modo determinante" del contesto originario della pubblicazione. Tali questioni hanno consentito alla Corte di giustizia di esprimersi nei termini già anticipati, anche a proposito del ruolo effettivo del gestore di un motore di ricerca nell'ambito delle richieste di deindicizzazione che, come nel caso di specie, si fondano sulla presunta inesattezza delle informazioni oggetto d'indicizzazione.

3. La decisione della Corte

Con la sentenza dell'8 dicembre 2022, la Corte di giustizia ha dato risposta ai quesiti sottoposti in via pregiudiziale, fornendo un'interpretazione sistematica delle disposizioni rilevanti. Il "BGH", la Corte federale di giustizia tedesca, si era interrogata sull'esatta portata dell'art. 17, par. 3, lett. a) del GDPR, chiedendo in particolare alla Corte di giustizia se tale norma fosse da intendersi nel senso che la deindicizzazione, richiesta a un motore di ricerca, sia «subordinata alla condizione che la questione dell'accuratezza del contenuto indicizzato sia stata risolta, almeno provvisoriamente, in un'azione legale intentata da tale persona contro il fornitore di tale contenuto, laddove esista una ragionevole possibilità di ottenere una tutela giudiziaria di questo tipo»[17]. La Corte ha evidenziato che l'art. 17, al par. 3, implica espressamente la prevalenza, a certe condizioni, del diritto all'informazione sul diritto alla protezione dei dati personali, che non è quindi un diritto assoluto. La premessa è doverosa, perché solo in virtù di tale lettura del rapporto tra questi diritti è possibile comprendere il ruolo del gestore del motore di ricerca che, dinanzi a una domanda di deindicizzazione, dovrà verificare se quel link sia «necessario per l'esercizio del diritto alla libertà di informazione degli utenti di Internet potenzialmente interessati»[18]. La Corte ha quindi fatto riferimento a una serie di criteri[19], stabiliti dalla giurisprudenza della Corte europea dei diritti dell'uomo[20], che devono essere presi in considerazione per effettuare il necessario bilanciamento tra diritto all'informazione e diritto alla privacy. In particolare, la Corte ha richiamato, *inter alia,* fattori quali: il contributo a un dibattito di interesse ge-

[17] Ivi, §48.

[18] Ivi, §55.

[19] Segnatamente, il contributo a un dibattito di interesse generale, la notorietà della persona che tali dati riguardano, l'oggetto del reportage, la condotta anteriore di tale persona, il contenuto, la forma e le conseguenze della pubblicazione, le modalità e le circostanze in cui le informazioni sono state ottenute nonché la loro veridicità (così al § 60 della sentenza). Tuttavia, occorre ricordare che i criteri in questione, fatte salve alcune pronunce più recenti della Corte EDU (come *Biancardi c. Italia,* ric. 77419/16 (2021)), sono stati formulati con riguardo a richieste di rimozione di contenuti archivistici, non di deindicizzazione.

[20] In particolare, v. la sentenza della Corte EDU, ric. 931/13, *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia* (2017).

nerale delle informazioni di cui si chieda la deindicizzazione, la notorietà della persona oggetto di esse, ma anche la loro veridicità. La Corte di giustizia, nel caso di specie, ha ritenuto che il diritto all'informazione possa prevalere sul diritto alla protezione dei dati personali, soprattutto laddove l'interessato sia un personaggio noto, ma ciò solo qualora le informazioni di cui si richiede l'oblio siano corrette. Qualora esse si rivelino inesatte, è il diritto alla tutela della vita privata e dei dati personali a dover prevalere. «In un'ipotesi del genere, infatti − scrive la Corte, ricalcando il ragionamento dell'Avvocato Generale Pitruzzella[21] − il diritto di informazione e il diritto di essere informati non possono essere presi in considerazione, poiché essi non possono includere il diritto di diffondere informazioni di tal genere»[22].

Tuttavia, stante la richiesta di deindicizzazione fondata sulla presunta inesattezza delle informazioni riportate negli articoli oggetto della controversia, la Corte ha dovuto esprimersi sia sull'*an* che sul *quomodo* dell'onere della prova relativo alla inesattezza stessa. A tal proposito, confermando l'orientamento dell'Avvocato Generale Pitruzzella, la Corte ha affermato che spetta all'interessato dimostrare «l'inesattezza manifesta delle informazioni»: invero, l'Avvocato Generale, nelle sue Conclusioni[23], aveva affermato che «un privato ha, in base al RGDP, il diritto di chiedere la deindicizzazione di una pagina *web* contenente dati che lo riguardano e che egli considera non veritieri. L'esercizio di tale diritto comporta tuttavia, a mio avviso, l'onere di indicare gli elementi su cui si basa la richiesta e di fornire un principio di prova della falsità dei contenuti di cui si richiede la deindicizzazione, ove ciò non risulti, in particolare in relazione alla natura delle informazioni di cui trattasi, manifestamente impossibile o eccessivamente difficile».

Infatti, al fine di evitare che su un soggetto gravi un onere eccessivo, ciò che la Corte di giustizia ritiene l'interessato debba fare «è fornire gli elementi di prova che, tenuto conto delle circostanze del caso di specie» si possa «ragionevolmente richiedere a quest'ultima di ricercare, al fine di dimostrare tale inesattezza manifesta»[24].

Ciò significa – ha precisato la Corte - che all'interessato che richiede la deindicizzazione non può essere richiesto di produrre sin dalla fase precontenziosa una decisione giurisdizionale a suo favore circa l'inesattezza dei contenuti di cui si chiede la deindicizzazione. Allo stesso tempo, non potrebbe essere richiesto al gestore del motore di ricerca di indagare sui fatti, organizzando un contraddittorio e fornendo elementi probatori sulla loro esattezza: anche in questo caso ci si troverebbe dinanzi a un onere

[21] Al § 65 della sentenza in esame, la Corte di giustizia afferma: «come rilevato, in sostanza, dall'avvocato generale al paragrafo 30 delle sue conclusioni, se è vero che, in determinate circostanze, il diritto alla libertà di espressione e di informazione può prevalere sui diritti alla tutela della vita privata e alla protezione dei dati personali, in particolare quando l'interessato svolge un ruolo nella vita pubblica, tale relazione è in ogni caso capovolta quando le informazioni oggetto della domanda di deindicizzazione, almeno per una parte che non abbia un carattere secondario rispetto alla totalità del contenuto, si rivelano inesatte. In un'ipotesi del genere, infatti, il diritto di informazione e il diritto di essere informati non possono essere presi in considerazione, poiché essi non possono includere il diritto di diffondere informazioni di tal genere e di avere accesso ad esse».

[22] *Ibidem*. Cfr. Conclusioni dell'Avvocato Generale Pitruzzella, cit., § 30.

[23] Cfr. Conclusioni dell'Avvocato Generale Pitruzzella, cit., § 44.

[24] CGUE, C-460/20, cit., §68.

eccessivo, gravante su un solo soggetto (ancorché di natura imprenditoriale)[25]. Laddove l'interessato presenti tali elementi, il gestore del motore di ricerca dovrà dar seguito alla richiesta di deindicizzazione, che non può dirsi dunque subordinata alla risoluzione definitiva della questione "veridicità" del contenuto indicizzato.

Al contrario, nel caso in cui l'inesattezza delle informazioni non possa considerarsi "manifesta", alla luce degli elementi di prova forniti dall'interessato, il gestore del motore di ricerca non potrà dirsi tenuto ad accogliere la richiesta di deindicizzazione (chiaramente, se non vi sia una decisione giudiziaria in merito).

La seconda questione, invece, interrogava la Corte sull'opportunità di tener conto (o meno) del contesto di pubblicazione delle miniature ritraenti i ricorrenti nell'ottica del bilanciamento tra diritti confliggenti. Occorre prendere in considerazione soltanto il valore informativo delle miniature in quanto tali, nel contesto neutro dell'elenco dei risultati, oppure occorre tener altresì conto del contesto, non emergente dalla sola visualizzazione delle miniature, nel quale la pubblicazione delle immagini è avvenuta? Secondo l'Avvocato Generale, per rispondere a tale interrogativo è fondamentale che siano correttamente identificati oggetto e natura del trattamento, nonché oggetto e natura della domanda di cancellazione. Infatti, la Corte ha ricordato che anche l'attività consistente nel rendere visualizzabili nei risultati di ricerca fotografie ritraenti persone fisiche, ancorché in miniatura, costituisce un trattamento di dati personali, poiché l'immagine rappresenta un'estrinsecazione dell'identità della persona.

Nel giudizio principale i ricorrenti avevano chiesto la deindicizzazione di quattro fotografie in miniatura che li raffiguravano: «tale domanda non ha ad oggetto né le informazioni contenute nel testo dell'articolo né le immagini nella loro funzione di supporto visivo e descrittivo di tale testo»[26], secondo l'Avvocato Generale Pitruzzella. Il motore di ricerca, rendendo visibili quelle miniature nel proprio elenco di ricerca, a prescindere dal contesto nel quale sono inserite, spoglia le foto dell'eventuale valore informativo o descrittivo che era stato assegnato loro inizialmente dal sito-editore. In questo senso, secondo l'Avvocato Generale si sarebbe dinanzi a un trattamento di dati personali peculiare, in cui il motore di ricerca, avendo estrapolato le immagini dal contesto d'origine, non si limita a indicizzare un contenuto pubblicato da un sito terzo, ma pare divenire esso stesso "*content creator*"[27]. Pertanto, l'Avvocato Generale ha ritenuto

[25] Tali conclusioni possono dirsi coerenti con la necessità di contemperare tutti i diritti coinvolti, compresa la libertà di impresa, tutelata dall'art. 16. In questa pronuncia, proprio l'art. 16 della Carta entra a pieno titolo nel bilanciamento di interessi, oltre all'art. 11 e agli artt. 7 e 8: non si tratta di un'innovazione di poco conto, perché nell'"archetipo" sancito da *Google Spain* si era fermi alla protezione dei dati quasi in via assoluta, senza un cenno alla libertà di informazione (eccetto in un passaggio) e senza menzionare la tutela della libertà d'impresa o un qualsivoglia riconoscimento della natura imprenditoriale dei soggetti coinvolti (i *search engine*).

[26] Conclusioni Avvocato Generale Pitruzzella, cit., § 54.

[27] Nel testo della pronuncia si ribadisce infatti, in più passaggi, che il motore di ricerca conduce attività che, pur rientrando a pieno titolo nell'alveo del trattamento dei dati personali, non possano essere definite di tipo "editoriale": «Il trattamento di dati personali effettuato nell'ambito dell'attività di un motore di ricerca si distingue da e si aggiunge a quello effettuato dagli editori di siti Internet, consistente nel far comparire tali dati in una pagina Internet. [...] tale gestore è responsabile non del fatto che i dati personali compaiono in una pagina Internet pubblicata da terzi, ma dell'indicizzazione di tale pagina e, in particolare, della visualizzazione del link verso di essa nell'elenco dei risultati presentati agli utenti di Internet in esito ad una ricerca effettuata a partire dal nome di una persona fisica, potendo una

che, nell'ambito del bilanciamento dei diritti in esame, debba operarsi un distinguo: nel caso in cui il soggetto interessato chieda la rimozione, dai risultati di ricerca per immagini, di fotografie che ritraggano la propria persona, il motore di ricerca dovrà tener conto soltanto del valore informativo delle foto *tout court*; laddove, invece, domandi la deindicizzazione di miniature nel contesto del contenuto pubblicato da una pagina online, dovrebbe essere posto ad oggetto del bilanciamento il valore informativo che esse rivestono nel contesto dell'articolo.

La Corte di giustizia, dopo aver ricordato che la visualizzazione di fotografie può rappresentare un'ingerenza nei diritti alla tutela della vita privata e dei dati personali persino superiore a quella potenzialmente operata da un testo scritto, ha recepito tale orientamento: «Si impone un bilanciamento distinto dei diritti e degli interessi concorrenti a seconda che siano in discussione, da un lato, articoli provvisti di fotografie pubblicate dall'editore della pagina Internet [...] inserite nel loro contesto di origine (...) e, dall'altro, fotografie visualizzate, sotto forma di miniature nell'elenco dei risultati, ad opera del gestore del motore di ricerca al di fuori del contesto Internet in cui esse sono state pubblicate»[28]. Più in generale, la Corte ha stabilito che il gestore del motore di ricerca, nel caso di richiesta di deindicizzazione, debba valutare se la visualizzazione di dette immagini rappresenti un'estrinsecazione del diritto alla libertà di informazione, e sia quindi necessaria per il suo godimento da parte degli utenti potenzialmente interessati ad avervi accesso. Nel bilanciamento di tali diritti, il *search engine* dovrà vagliare la presenza di un elemento in particolare, dalla Corte definito "fondamentale": il contributo a un dibattito di interesse generale. Tuttavia, la Corte ha ritenuto che nel caso di specie le fotografie, poste al di fuori del contesto di riferimento, possedessero di per sé «solo uno scarso valore informativo», apparendo unicamente sotto forma di miniature nell'elenco dei risultati di ricerca. Pertanto, la Corte di giustizia ha risposto alla seconda questione pregiudiziale sostenendo che, nel bilanciamento operato dal motore di ricerca, occorre tener conto del «valore informativo di tali fotografie indipendentemente dal contesto della loro pubblicazione, prendendo però in considerazione qualsiasi elemento testuale che accompagna direttamente la visualizzazione», potendo questo fungere da ausilio nella valutazione circa la sussistenza di un carattere informativo.

4. Lo *status quo* e le difficoltà connesse all'*enforcement* privato del diritto alla deindicizzazione

Con questa sentenza, la Corte di giustizia si è pronunciata sul complesso rapporto tra diritto all'oblio, libertà di espressione e di informazione e "verità" in rete. Il rimedio della deindicizzazione, infatti, non eliminando il dato in sé, ma limitandosi a oscurare dall'elenco di ricerca il *link* che vi conduca, dovrebbe contemperare la necessità di tutelare la reputazione individuale e la libera informazione. Questa la *ratio* nel ragionamento dei giudici della Corte di giustizia dell'Unione europea, che con la celebre sentenza *Google Spain* hanno dato i natali proprio al diritto all'oblio. Con il caso in parola la Corte

visualizzazione siffatta [...] incidere significativamente sui diritti fondamentali della persona» (§§ 50-52).

[28] CGUE, C-460/20, cit., § 101.

aveva di fatto sancito la prevalenza "quasi *tout court*" del diritto alla cancellazione dei dati sulla libertà di informazione: può dirsi così iniziata una cospicua giurisprudenza pressoché unanime a favore del diritto a essere dimenticati. L'unica eccezione menzionata dalla Corte poteva riferirsi alla notorietà del soggetto richiedente la deindicizzazione: in quel caso, in virtù della natura di "personaggio pubblico" dell'interessato, le informazioni sul suo conto avrebbero avuto motivo di permanere[29]. Come ha ricordato anche l'Avvocato Generale Pitruzzella[30], anche nella "sentenza GC"[31] la Corte ha affermato che «sebbene i diritti della persona interessata tutelati dagli articoli 7 e 8 della Carta prevalgano, di norma, sulla libertà di informazione degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona interessata, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica».

Una tale qualifica diviene allora essenziale nel bilanciamento tra i due diritti oggetto di trattazione: il ruolo ricoperto dalla persona nella vita pubblica – lo si è visto - era stato indicato dalla Corte di giustizia quale requisito in grado di giustificare l'ingerenza nei diritti fondamentali della persona, in virtù di un «preponderante interesse del pubblico» ad avere accesso all'informazione[32]. Infatti, è vero che appare fondamentale tutelare l'identità della persona, declinata rispetto alla sua condizione in un determinato momento storico, perché un individuo non può dirsi solo una mera "sintesi statica" di ciò che è stato, ma di come muta col tempo[33]; ma è vero altresì che laddove tale soggetto rivesta, o abbia rivestito, un ruolo pubblico, quel diritto dovrà necessariamente subire una compressione, in ragione dell'altrettanto fondamentale interesse della collettività ad avere contezza delle informazioni che riguardano la vita pubblica.

Il tema dell'importanza della storicizzazione e della contestualizzazione può dirsi centrale, sia per il verosimile interesse del singolo individuo di essere ricordato per ciò che è, e non necessariamente per ciò che è stato, sia per il diritto a essere informati di cui godono i cittadini tutti, perché «una notizia non aggiornata non è una notizia vera e

[29] La sentenza nel caso *Google Spain* così recitava: «Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi» (§ 99).

[30] Conclusioni Avvocato Generale Pitruzzella, cit., § 17.

[31] CGUE, C-136/17, *GC e a. c. CNIL* (2019), § 66.

[32] F. Russo, *Diritto all'oblio e motori di ricerca: la prima pronuncia dei tribunali italiani dopo il caso Google Spain – il commento*, in *Danno e responsabilità*, 3, 2016, 302 ss.

[33] Per una panoramica sulle diverse questioni generate dal "riposizionamento" in ambito digitale di questo diritto v. i contributi raccolti in G. Resta – V. Zeno Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, cit. Per una ricostruzione in chiave storica cfr. anche M. Mezzanotte, *Il diritto all'oblio. Contributo allo studio della privacy storica,* Napoli, 2009; ma v. anche F. Pizzetti, *Il caso del diritto all'oblio,* Torino, 2012.

una verità non aggiornata non è una verità»[34]. Tale *claim* gode di un pregevole supporto giurisprudenziale: la Corte di Cassazione italiana[35], infatti, più volte pronunciatasi in materia di diritto all'oblio, ha spesso fatto leva sulla necessità di "contestualizzazione" delle informazioni, e quindi di aggiornamento delle stesse, da parte del titolare del sito. Le notizie diffuse in rete non possono dirsi paragonabili a quelle presenti sulla carta stampata, se non altro in ordine alla loro permanenza in circolazione: per tale ragione, la giurisprudenza italiana ha definito necessario un intervento volto ad "attualizzare" i dati online da parte del gestore di un sito.

Dal 2016, il diritto all'oblio, e più in generale il diritto di libertà informatica[36], ha ricevuto anche una più chiara e opportuna codificazione nell'art. 17 del GDPR, che sancisce sì il diritto alla cancellazione dei dati personali, ma prevede espressamente anche una serie di fattispecie che fungono da limiti dello stesso in nome della tutela di interessi concorrenti. Non si tratta, quindi, di un diritto *ad nutum*[37]: non era da considerarsi tale neppure dai suoi albori processuali; ma con una più puntuale previsione in materia, di carattere normativo, i suoi confini possono essere evinti con maggiore sicurezza.

Un tema caldo dei giorni nostri, che parrebbe far tornare in modo dirompente, anche in questo caso, l'interrogativo concernente il ruolo svolto dai motori di ricerca, specie nel mondo dell'informazione. Ciò in virtù del sempre più ingente potere di cui godono i *search engine,* potendo, di fatto, incidere anche indirettamente sui diritti fondamentali degli "internauti", cittadini prima che utenti. Nella *opinion* n. 148 del 2008[38], il Gruppo di lavoro Articolo 29 (WP29)[39] considerava i motori di ricerca "semplici" strumenti della società dell'informazione, sostenendo che l'attività di indicizzazione che li caratterizza fosse da interpretarsi come attività di messa a disposizione degli utenti di informazioni: a tutti gli effetti una sorta di intermediario.

In realtà, come afferma anche l'Avvocato Generale Pitruzzella nelle conclusioni rese nella causa in commento, un motore di ricerca non si limita ad ospitare i contenuti prodotti da altri nella rete, ma ha «un ruolo attivo nella diffusione dell'informazione», fungendo da vero e proprio *gatekeeper* della stessa[40].

---

[34] T.E. Frosini, *Google e il diritto all'oblio preso sul serio*, in G. Resta – V. Zeno Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain,* cit., 1 ss.

[35] Tra le altre, Cass. civ., sez. III, 5 aprile 2012, n. 5525; 26 giugno 2013, n. 16111.

[36] Così T.E. Frosini, *Google e il diritto all'oblio preso sul serio,* cit., 3.

[37] G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in G. Resta – V. Zeno Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, cit., 37.

[38] Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines*, adopted on 4 April 2008, 00737/EN, WP148.

[39] Oggi Comitato europeo per la protezione dei dati.

[40] Conclusioni Avvocato Generale Pitruzzella, cit., § 2. La terminologia sopra richiamata – "*gatekeeper* dell'informazione" – trova le proprie radici in due dei più recenti interventi normativi in tema di diritti digitali: Digital Services Act e Digital Markets Act. La declinazione attiva del ruolo di un motore di ricerca nell'ambito dell'informazione è figlia dell'orientamento proprio dei due regolamenti approvati nel luglio 2022 - regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) e regolamento (UE) 2022/1925 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali) - che riconoscono il potenziale ingente impatto che le grandi piattaforme possano generare sui diritti fondamentali. Proprio in ragione di tale notevole potere, tra l'altro, gli atti normativi ora vigenti interpretano i "*VLOSE*" (*very large online search engines*) come

Infatti, i *provider* possono vantare una funzione molto più rilevante, essendo stato loro implicitamente attribuito il compito di verificare, caso per caso, l'eventuale prevalenza del diritto alla protezione dei dati personali sulla libertà di informazione[41]. In sostanza, spetta oggi ai motori di ricerca la funzione di bilanciamento e ponderazione in concreto di diritti e interessi fondamentali, quali quelli in questione. Sia che una notizia debba essere eliminata sia che essa debba permanere online, sarà il motore di ricerca a stabilirlo in concreto. "Il grande passo" compiuto dalla Corte di giustizia nella sentenza *Google Spain* è stato proprio quello di rendere gli operatori statunitensi «gli esecutori, possibilmente anche interpreti, di una sensibilità europea sul rapporto tra due diritti»[42]. Si può parlare, in tal proposito, *di "private enforcement":* con tale espressione si fa riferimento alla crescente ondata di privatizzazione cui si assiste oggi, nelle decisioni che impattano sul godimento di diritti fondamentali[43].

Ciò implica, tra l'altro: da un lato, che si attribuisca ai motori di ricerca un ruolo quasi giudiziario, pur essendo poi considerati "meri intermediari", privi di responsabilità editoriale sui contenuti trasmessi; dall'altro, che la valutazione sulla natura illecita di un contenuto, e la conseguente eventuale previsione di misure sanzionatorie[44], spetti ad attori privati, senza la necessità che vi sia una previa decisione nel merito da parte di un'autorità pubblica. Le regole del gioco, seppur in tema di diritti costituzionalmente garantiti, sono stabilite dai *private actors*.

Una tendenza riconfermata anche dalla pronuncia in esame che, pur fornendo ai cittadini-utenti la possibilità di godere del proprio diritto alla privacy e di vederlo tutelato in concreto con una modalità almeno apparentemente più agevoli, non sembra poter tranquillizzare quella parte della dottrina che, proprio in ragione dei rischi connessi alla nuova egemonia digitale nella fruizione dei diritti fondamentali, teme un tale strapotere delle piattaforme. La volontà di "imbrigliare" il potere privato emerge anche dai più recenti sviluppi normativi a livello europeo: il Digital Services Act e il Digital Markets Act nascono anche in risposta a tale esigenza, figlia del nuovo costituzionalismo digitale[45].

soggetti sottoposti a regole peculiari. Sul punto, si veda M. Borgobello, *Digital Services Act – Piattaforme di grandi dimensioni sotto la lente UE: i risultati del primo "censimento"*, in *Agenda Digitale*, 29 marzo 2023.

41 M. Bassini, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali*, Roma, 2019, 327, p. 329, ma v. anche Id., *Fundamental rights and private enforcement in the digital age,* in *European Law Journal,* 25(2), 2019, 182 ss. In particolare, in quest'ultimo scritto si ricorda che l'applicazione dei diritti fondamentali e il loro godimento effettivo dipendano sempre più dalle attività svolte dalle piattaforme digitali, di fatto investite di un potere che normalmente spetta alle autorità pubbliche, come tribunali o organi amministrativi (si pensi all'Autorità garante della protezione dei dati personali). Tale ruolo, però, appare ancor più impegnativo e degno di nota alla luce della diversa concezione dei diritti fondamentali in gioco in un tale contesto, vale a dire libertà di informazione e privacy: il grado di protezione di tali diritti in Europa e negli Stati Uniti trasuda sensibilità diverse.

42 *Ibidem.*

43 *Ibidem.*

44 Quali la rimozione del contenuto dai servizi del motore di ricerca o la previsione di limitazioni o restrizioni dell'*account*-editore che abbia reso pubblico il contenuto stesso, in ragione del mancato rispetto dei termini e condizioni d'uso del *provider*. Sul punto, M.R. Carbone*, Il rapporto USA – Censura, come funziona e quanto è estesa nel mercato digitale*, in *Agenda Digitale*, 14 febbraio 2022.

45 Sul punto, tra gli altri, G. De Gregorio*, The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 19(1), 2021, 41 ss.

5. Considerazioni conclusive

Con il mutato contesto socioeconomico, il rischio che alcuni beni giuridici, quali il diritto alla privacy o all'informazione, vengano lesi dall'azione o, come nel caso oggetto della pronuncia, dall'inazione dei motori di ricerca è ingente. Suonerà forse ridondante ricordare come l'utilizzo di sistemi algoritmici consenta ai vari *search engine* di trattare dati personali indicizzando, e quindi di fatto promuovendo, alcuni contenuti rispetto ad altri[46].

Appare allora piuttosto agevole comprendere come ciò sia in grado di generare un notevole impatto sulla circolazione di alcune notizie a discapito di altre, potendo così produrre un indotto sia sulla sfera individuale dei soggetti interessati, nel caso in cui le informazioni ivi contenute abbiano carattere diffamatorio, sia sulla "corretta" informazione di tutti gli internauti, influenzando anche l'opinione pubblica[47]. Il complesso rapporto tra libertà di informazione (e di espressione) e diritto alla tutela dei dati personali (e alla privacy) in rete, affrontato dalla Corte di giustizia nel giudizio in esame, porta con sé la necessità di operare alcune riflessioni.

Innanzitutto, va notato come la Corte, nel ponderare tali diritti, abbia scelto ancora una volta di non ricorrere alla censura, a conferma dell'attuale *trend* europeo, atto a scongiurare l'uso di tale periglioso strumento. Afferma la necessità, per l'interessato, di provare la presenza di elementi di "inesattezza manifesta" nel contenuto di cui si chiede la deindicizzazione: solo nel caso in cui le informazioni in oggetto siano *manifestamente* inesatte - e ciò va debitamente dimostrato - si potrà allora procedere all'eliminazione di quel contenuto dai risultati della ricerca. Tale assunto rappresenta probabilmente l'elemento di carattere maggiormente innovativo della sentenza. Se così non fosse stato deciso dalla Corte, Google (così come ogni altro motore di ricerca) avrebbe potenzialmente potuto dar seguito all'unilaterale richiesta di deindicizzazione degli articoli oggetto della controversia, che tuttavia godevano di scopo (anche) informativo. In questo modo si sarebbe sacrificato il diritto a essere informati, in nome di un diritto alla protezione dei dati personali evidentemente prevalente *tout court*.

---

[46] Si tratta, ovviamente, di un tema che riguarda varie piattaforme e non soltanto i motori di ricerca, come dimostra l'interessante causa *Gonzalez c. Google* pendente avanti alla Corte Supreme statunitense e relativa alla riconducibilità all'esenzione sancita dalla Section 230 del Communications Decency Act (CDA) dell'attività di raccomandazione di contenuti di terzi eventualmente svolta dai prestatori di servizi (nel caso di specie, da Google in veste di gestore di YouTube, dunque quale *hosting provider*). V. altresì la causa *Twitter Inc., v. Taamneh* incentrata sul medesimo punto di diritto.

[47] Il motore di ricerca, che era stato descritto come un semplice intermediario di contenuti postati da terzi, si rivela a tutti gli effetti un attore nella gestione di essi. Se il ruolo che era stato immaginato alle origini per questi soggetti era effettivamente quello di meri intermediari tecnici, e il regime giuridico introdotto (sia negli Stati Uniti che in Europa) rifletteva questo intendimento, oggi forse la piattaformizzazione della sfera pubblica (secondo il linguaggio di M. Sorice, *La «piattaformizzazione» della sfera pubblica*, in *Comunicazione politica*, 3, 2020, 371 ss.) ha reso effettivamente maggiormente incisivo il ruolo in questione grazie anche alla maggiore capacità diffusiva e dunque di interferire sull'opinione pubblica. La non totale neutralità della rete può rappresentare un fattore di rischio per la salute delle democrazie, per il corretto esercizio del diritto al voto, per l'informazione, per la tutela dell'immagine delle persone fisiche e così via. Non a caso, anche gli sviluppi normativi più recenti confermano la presa di consapevolezza di tale ingente potere: il Digital Services Act, tra le altre cose, impone obblighi particolari e più dettagliati ai prestatori di servizi di grandi dimensioni, proprio in virtù del maggiore potenziale di rischio che essi dimostrano.

Un tale orientamento, in realtà, non rappresenterebbe poi un'evenienza così improbabile; invero, e ciò spinge verso il secondo motivo di riflessione, in dottrina si parla in proposito di "paradosso della privacy"[48]: un diritto nato negli Stati Uniti e poi esportato in Europa, dove si sofistica fino a inglobarvi il diritto alla protezione dei dati. Un diritto d'importazione, dunque, che tuttavia pare abbia assunto nel Vecchio Continente un valore spesso persino preponderante rispetto a quella libertà, sancita dall'art. 11 della Carta dei diritti fondamentali dell'Unione europea, che negli Stati Uniti difficilmente trova limiti. Tali dicotomiche impostazioni domestiche si rendono ancor più evidenti e paradossali se si pensa al ruolo assunto oggi dai motori di ricerca nella gestione delle richieste di deindicizzazione. Come si è detto in precedenza, è proprio a costoro che spetta il potere-dovere di verificare se, in un ipotetico caso di specie, a prevalere sia il *right to be not found easily*[49] oppure la libertà di informare ed essere informati.

Non può non lasciare perplessi il fatto che i giudici europei, nel caso Google Spain, abbiano scelto di attribuire un compito di tale portata a operatori privati, i quali peraltro affondano le loro radici negli Stati Uniti, con una sensibilità nettamente differente da quella europea rispetto a quei diritti[50]. Si assiste all'acquisizione di uno strapotere da parte di tali piattaforme, che con il *private enforcement* operano come se godessero di una sorta di "delega" del potere giudiziario, come se fosse stato loro attribuito «un ruolo para-costituzionale», divenendo a tutti gli effetti veri e propri "arbitri" dei conflitti tra diritti fondamentali[51]. Affidare simili operazioni di bilanciamento, almeno in prima battuta, a un privato, costituisce un aspetto critico di per sé[52], considerata l'importanza degli interessi in gioco, aventi rango costituzionale. In simili fattispecie, quella ponderazione tipica del diritto costituzionale dovrà essere operata non dalla magistratura *super partes*, bensì dei gestori del motori di ricerca, privati che coltivano anche interessi diversi. Il rischio è che il motore di ricerca si tramuti in un «arbitro della fruibilità dell'informazione online»[53].

In terzo luogo, non può non notarsi come con questa sentenza si abbia la riprova giurisprudenziale del fatto che «il diritto di informazione e il diritto di essere informati non possono essere presi in considerazione», nel bilanciamento con altri diritti di pari rango, qualora le informazioni presenti sul *web* siano inesatte, «poiché essi non possono includere il diritto di diffondere informazioni di tal genere»[54]. Azzardando un'interpretazione forse lata di tale assunto, potrebbe dirsi visibile una certa apertura da parte dell'ordinamento europeo a considerare le informazioni false un non-valore, incapaci di essere incluse nell'alveo della libertà di manifestazione del pensiero.

Ma cosa accade se, come nel caso di specie, al motore di ricerca venga avanzata richie-

---

48 M. Bassini, *Internet e libertà di espressione*, cit., 325

49 A. Palmieri – R. Pardolesi, *Dal diritto all'oblio all'occultamento dei dati in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi quaderni del Foro italiano,* 2014, 5 ss.

50 V. ancora M. Bassini, *Internet e libertà di espressione,* cit., 328

51 O. Pollicino, *Limitare il diritto all'oblio è un rischio*, in *Il Sole 24 Ore*, 24 settembre 2019.

52 V. ancora F. Russo, *Diritto all'oblio e motori di ricerca,* cit.

53 A. Mentelero, *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella digital economy*, in *Diritto dell'informazione e dell'informatica,* 4-5, 2014, 687.

54 CGUE, C-460/20, cit., § 65.

sta di deindicizzazione, a tutela della vita privata e personale, asserendo la falsità di contenuti di matrice informativa circolanti in rete sul proprio conto? Si è dato conto del dovere del motore di ricerca di operare un bilanciamento tra interessi confliggenti, ma di fronte al *fumus* di falsità delle informazioni la questione si complica. Qui il motore di ricerca non poteva avere contezza della veridicità di quei dati. Avrebbe dovuto averne? Avrebbe dovuto agire in prima persona cercando elementi a favore della posizione della coppia, che provassero quindi l'inesattezza dei dati? Il motore di ricerca - lo si è detto - viene definito anche *gatekeeper* dell'informazione[55]: si occupa di raccogliere e filtrare le notizie in base a criteri stabiliti *ex se,* effettuando una «scelta unilaterale rispetto alle informazioni che vengono rese accessibili agli utenti»[56]. Che abbia un ingente ruolo nel settore appare innegabile; ma lo è altrettanto che demandare a piattaforme come Google l'indagine sulla sedicente inesattezza di determinati dati possa quantomeno perplimere.

La Corte di giustizia ha fatto luce anche in merito a tale incertezza, chiarendo che l'onere della prova circa la presunta accuratezza o meno dei dati e delle informazioni ivi contenute sia da attribuire agli interessati, non al motore di ricerca, che non ha alcun dovere di cercare elementi di fatto al fine di vagliare la corrispondenza al vero di quanto affermato dai richiedenti. Qui possono evidenziarsi talune criticità.

La Corte, con riferimento all'onere probatorio, si esprime in termini di "inesattezza manifesta" delle informazioni presenti nel contenuto da deindicizzare, affermando che «al fine di evitare di far gravare su tale persona un onere eccessivo […] essa è tenuta unicamente a fornire gli elementi di prova che, tenuto conto delle circostanze del caso di specie, si può ragionevolmente richiedere a quest'ultima di ricercare al fine di dimostrare l'inesattezza manifesta»[57]. Un nodo da sciogliere parrebbe essere allora proprio quello relativo alla più filosofica natura manifesta di detta inesattezza: quando potrà dirsi integrata? In base a quali criteri?

Lo stesso interrogativo potrebbe porsi in relazione all'altrettanto ambiguo riferimento a quanto e cosa sia "ragionevole" richiedere come elemento di prova. Ciò genera incertezze correlate ai non meglio precisati termini di cui sopra, anche e soprattutto in relazione al potenziale accrescimento dello già smisurato potere di piattaforme come Google, che si troveranno a dover operare, sulla base di definizioni dai contorni sfumati, ponderazioni di interessi di rango costituzionale. L'augurio è che tale *decisum* possa consentire di rendere più "afferrabile" e trasparente il procedimento di deindicizzazione che, ribattezzato dall'Avvocato Generale, "*procedural data due process*"[58], è stato così reso sempre più extragiudiziale e innovativo da questa Corte, in modo del tutto inedito.

---

[55] Conclusioni dell'Avvocato Generale Pitruzzella, C-460/20, cit.

[56] F. Paolucci, *(Don't) remember my name*: *il diritto all'oblio nella recente pronuncia C-460/2020 della Corte di Giustizia dell'Unione Europea*, in *dirittocomparati.it*, 19 gennaio 2023.

[57] CGUE, C-460/20, cit., § 68.

[58] Conclusioni dell'Avvocato Generale Pitruzzella, C-460/20, cit., §§ 42-50. Tuttavia, occorre ricordare come tale concetto trovi le proprie fondamenta nella dottrina soprattutto statunitense: un tale approccio pare riscontrabile in K. Crawford – J. Schultz, *Big data and due process: toward a framework to redress predictive privacy harms*, in *Boston College Law Review*, 55(1), 2014, 93 ss., e poi è stato ripreso da A. Huq, *Constitutional Rights in the Machine Learning State*, in *Cornell Law Review*, 105, 2020, 1875 ss.

Sul diritto all'oblio e obblighi di deindicizzazione globale.

Sabrina Peron

Corte di Cassazione, sez. I civile, 15 novembre 2022, n. 34658

In tema di trattamento dei dati personali, la tutela spettante all'interessato, strettamente connessa ai diritti alla riservatezza e all'identità personale e preordinata a garantirne la dignità personale dell'individuo, ai sensi dell'art. 3 Cost., c. 1, e dell'art. 2 Cost., che si esprime nel cosiddetto "diritto all'oblio", consente, in conformità al diritto dell'Unione europea, alle autorità italiane, ossia al Garante per la protezione dei dati personali e al giudice, di ordinare al gestore di un motore di ricerca di effettuare una deindicizzazione su tutte le versioni, anche extraeuropee, del suddetto motore, previo bilanciamento tra il diritto della persona interessata alla tutela della sua vita privata e alla protezione dei suoi dati personali e il diritto alla libertà d'informazione, da operarsi secondo gli standard di protezione dell'ordinamento italiano.

Sommario

1. Il caso. - 2. Il diritto all'oblio. - 3. Il diritto all'oblio online. - 4. Il diritto all'oblio online e gli obblighi dei motori di ricerca

Keywords

diritto all'oblio - identità personale - deindicizzazione globale - privacy - motori di ricerca

1. Il caso

Un soggetto adiva all'Autorità Garante della Privacy, lamentando un pregiudizio al proprio diritto all'oblio a causa della perdurante diffusione nel web di notizie non aggiornate attinenti ad una vicenda giudiziaria che lo aveva visto coinvolto. Vicenda poi conclusasi con un decreto di archiviazione del GIP per infondatezza del reato. Al Garante veniva così richiesto di ordinare a Google la rimozione, degli URL della notizia nelle versioni europee e extraeuropee, e ciò sul presupposto che il ricorrente era titolare di interessi personali e professionali, anche fuori dallo spazio europeo.
Il Garante della Privacy, accertato che Google aveva già spontaneamente rimosso gli URL delle versioni europee, in accoglimento parziale del ricorso ne aveva ordinato la rimozione anche nelle versioni extraeuropee del motore di ricerca.

Contro tale decisione Google ricorreva al Tribunale di Milano, il quale con sentenza n. 5560/2020 limitava l'ordine di rimozione degli URL sulle sole versioni nazionali del motore di ricerca corrispondenti agli Stati membri dell'Unione Europea.
Contro tale decisione l'Autorità Garante della Privacy adiva alla Corte di Cassazione che accoglieva il ricorso con la decisione qui in commento.

2. Il diritto all'oblio

È noto che il diritto all'oblio, nasce come il «giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione, dopo un consistente lasso di tempo, di una notizia che in passato era stata legittimamente pubblicata»[1]. In questi casi, si ritiene che prevalga il diritto all'oblio dell'interessato a meno che, per altri eventi nel frattempo sopravvenuti, la notizia ritorni di attualità, rinnovando l'interesse del pubblico all'informazione[2].
Il diritto all'oblio, dunque, quale diritto della personalità, tutelato dall'art. 2 Cost., è strettamente connesso al diritto al rispetto della propria identità personale ed a quello della tutela della propria riservatezza. A tale ultimo riguardo la decisione in commento, ha ribadito che il diritto all'oblio «protegge l'interessato nella pretesa di non veder ulteriormente divulgate notizie, già legittimamente pubblicate, ma ormai superate dal tempo, che ha dissolto l'interesse pubblico alla circolazione dell'informazione»[3]. Mentre per quanto concerne l'identità personale, la sentenza ha precisato che con il diritto all'oblio viene «protetta l'esigenza di contestualizzazione e aggiornamento delle informazioni»[4]. In ogni caso, in una prospettiva evolutiva, tale diritto si traduce «nell'esigenza di evitare che la propria persona resti cristallizzata ed immutabile in un'identità legata ad avvenimenti o contesti del passato, che non sono più idonei a definirla in modo autentico o, quanto meno, in modo completo»[5].

---

[1] Cass. civ., sez. III, 9 aprile 1998, n. 3679, in *Foro it.*, 1998, I, 1834 ss. con nota di P. Laghezza, *Il diritto all'oblio esiste (e si vede)*, 1836 ss. ed in *Danno resp.*, 1998, 882 ss. con nota di C. Lo Surdo, *Diritto all'oblio come strumento di protezione di un interesse sottostante*.

[2] Cass. civ., sez. III, 9 aprile 1998, n. 3679, cit., così testualmente precisa: «quando il fatto precedente per altri eventi sopravvenuti ritorna di attualità, rinasce un nuovo interesse pubblico alla informazione non strettamente legato alla stretta contemporaneità fra divulgazione e fatto pubblico che si deve contemperare con quel principio, adeguatamente valutando la ricorrente correttezza delle fonti di informazione».

[3] Così, testualmente, Cass. civ., sez. I, 15.11.2022, n. 34658, § 11, qui in commento.

[4] Peraltro è stato osservato che l'evoluzione tecnica e quella giuridica che ne è conseguita ha portato all'enucleazione di «nuove sfumature dell'identità personale e una nuova antropologia, che astrae l'individuo dalla sua dimensione naturale, fino a concepirlo come un complesso di dati: la navigazione dell'individuo-utente in rete, infatti, permette di ricostruire un profilo identitario ricavato dalle sue attività svolte (si pensi, ad esempio, alle transazioni online e alla relativa immissione dei dati personali), o dalle preferenze da questi manifestate (attraverso *social network*, *blog*, *online community*, etc.), che non sempre risulta pienamente aderente alla identità fisica reale, in particolare a quella di natura anagrafica», così, testualmente, G. Garofalo, *Identità digitale e diritto all'oblio: questioni aperte all'indomani dell'approvazione del GDPR*, in *Il diritto di famiglia e delle persone*, 3, 2021, 1506.

[5] Cass. civ., sez. I, 31 maggio 2021, n. 15160, in *Foro it.*, I, 1, 2022, 320 ss.

Appaiono in tale delineazione del diritto, due elementi: anzitutto, il fattore tempo e, in secondo luogo, l'interesse per il pubblico a conoscere fatti che, per un motivo o per un altro, sono tornati di attualità. Al fine di meglio delineare tali elementi, la giurisprudenza successivamente formatasi, ha avuto modo di precisare che la «riemersione, di un fatto molto lontano nel tempo - che rivestiva, all'epoca, un sicuro interesse pubblico - non si traduce, ipso facto, nella permanenza dell'interesse anche nel momento attuale»[6]. Difatti, quest'ultimo dev'essere bilanciato con la «legittima aspettativa della persona coinvolta ad essere dimenticata dall'opinione pubblica e rimossa dalla memoria collettiva»[7]. Ciò comporta, da un lato, che, la «diffusione di notizie personali in una determinata epoca ed in un determinato contesto non legittima, di per sé, che le medesime vengano utilizzate molti anni dopo, in una situazione del tutto diversa e priva di ogni collegamento col passato»; dall'altro lato, che il diritto dell'interessato ad essere dimenticato «può cedere il passo rispetto al diritto di cronaca in quanto sussista un interesse effettivo ed attuale alla diffusione della notizia; diversamente argomentando, altrimenti, si finirebbe col riconoscere una sorta di automatica permanenza dell'interesse alla divulgazione, anche in un contesto storico completamente mutato»[8]. Fermo restando, comunque, che per una certa notizia può tollerarsi una sua più lunga permanenza nel tempo, qualora si tratti di eventi che per la «loro eccezionalità e per la efferatezza dei delitti rievocati necessitano di essere ricordati e tramandati»[9]. Difatti, se il «decorso del tempo può attenuare l'attualità della notizia e far scemare, al tempo stesso, anche l'interesse pubblico all'informazione», può nondimeno accadere, che «all'effetto di dissolvenza dell'attualità della notizia non faccia riscontro l'affievolimento dell'interesse pubblico o che - non più attuale la notizia - riviva, per qualsivoglia ragione, l'interesse alla sua diffusione»[10].

3. Il diritto all'oblio online

Con l'affermarsi di nuove forme di comunicazione di massa diffuse online, il diritto all'oblio viene ulteriormente delineato, giacché non si tratta più di valutare la liceità, o meno, della ripubblicazione sulla carta stampata, o la ridiffusione a mezzo radiote-

[6] Cass. civ., sez. III, 26 giugno 2013, n. 16111, in *Dir. inf.*, 6, 2013, 829 ss.

[7] Cass. pen., sez. V, 17 luglio 2009, n. 45051, in *Resp. civ. prev.*, 5, 2010, 1060 ss. con nota di S. Peron, *La verità della notizia tra attualità ed oblio*. Sentenza pubblicata anche in *Critica del diritto*, 2009, 236 ss. con nota di A. Cerri, *Diritto di cronaca, diritto di rievocare fatti passati versus diritto di riservatezza e diritto all'oblio*.

[8] Cass. civ., sez. III, 26 giugno 2013, n. 16111, cit.

[9] Così, Trib. Roma, 1 febbraio 2001, in *Dir. inf.*, 2, 2001, 206 ss.

[10] Cass. pen., sez. V, 17 luglio 2009, n. 45051, *cit.*, che così ulteriormente precisa: «insomma, può non esservi corrispondenza o piena sovrapposizione cronologica tra attualità della notizia ed attualità dell'interesse pubblico alla divulgazione. Nondimeno, in quest'ultima ipotesi, il persistente o rivitalizzato interesse pubblico, che - in costanza di attualità della notizia - doveva equilibrarsi con il diritto alla riservatezza, all'onore od alla reputazione, deve trovare - quando la notizia non è più attuale - un contemperamento con un nuovo diritto, quello all'oblio, come sopra delineato, anche nell'ulteriore accezione semantica di legittima aspettativa della persona ad essere dimenticata dall'opinione pubblica e rimossa dalla memoria collettiva».

levisione, di una notizia risalente nel tempo[11]. Difatti, le notizie – e, più in generale, una qualsiasi informazione riguardante una qualsiasi persona e/o un qualsiasi fatto o avvenimento - una volta immesse nel circuito online rimangono a galleggiare nella rete in una sorta di eterno presente cosicché i motori di ricerca, con l'inserimento di una qualsiasi parola chiave, sono in grado di ripescarle nel giro di pochi secondi e gli utenti possono di riutilizzarle con le più disparate finalità[12]. Il diritto all'oblio deve quindi oggi scontare, sul piano applicativo, e segnatamente su quello del bilanciamento degli interessi, la possibilità di conservare in rete notizie, anche risalenti, spesso superate da eventi successivi, e perciò inattuali»[13].

Per le notizie pubblicate sul web, si ritiene che il bilanciamento con l'interesse pubblico alla conoscenza del fatto, espressione del diritto di manifestazione del pensiero e quindi di cronaca e di conservazione della notizia per finalità storico-sociale e documentaristica, possa trovare soddisfazione anche nella sola deindicizzazione[14] dell'articolo dai motori di ricerca[15]. Deindicizzazione che non è però scontata ed automatica, dovendo il diritto all'oblio dell'interessato controbilanciarsi con il legittimo interesse degli utenti di internet potenzialmente interessati ad avere accesso a quella specifica informazione. Per tale ragione si è precisato che siffatto equilibrio dipende dalle «circostanze rilevanti di ciascun caso, in particolare dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata dell'interessato, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica»[16]. Difatti «l'interessato, quando svolge un ruolo nella vita pubblica, deve dar prova di un maggior grado di tolleranza, poiché è inevitabilmente e con piena consapevolezza esposto al pubblico scrutinio»[17].

---

[11] Per approfondimenti sulle varie declinazioni del diritto all'oblio si rinvia a D. Barbierato, *Osservazioni sul diritto all'oblio e la (mancata) novità del regolamento UE 2016/679 sulla protezione dei dati personali*, in *Responsabilità civile e previdenza*, 6, 2017, 2100 ss.

[12] Correttamente è stato osservato che l'avvento di internet ha fatto emergere «nuovi e inediti pericoli per l'identità personale, a causa della disponibilità di una grande quantità di informazioni decontestualizzate, prive di riferimento temporale, definitivamente disperse online e custodite, in una eterna dimensione di "inconscio digitale", nella memoria della rete. In essa l'identità virtuale resta cristallizzata in una rappresentazione permanente e profilata dei dati personali, precludendone la concreta possibilità di cancellazione per soddisfare la pretesa individuale ad essere dimenticati», così testualmente, A. Alù, *Esiste il diritto all'oblio su internet? La complessa evoluzione di tale figura tra giurisprudenza e legge*, in *Il diritto di famiglia e delle persone*, 1, 2020, 313 ss.

[13] Cass. civ., sez. I, 31 maggio 2021, n. 15160, cit.

[14] La deindicizzazione (o *de-listing*) è un'attività «consistente nell'escludere che il nome di un soggetto compaia tra i risultati di un motore di ricerca in esito a una interrogazione del medesimo; con la deindicizzazione (il punto sarò ripreso in seguito), si elimina una particolare modalità di ricerca del dato, che rimane presente in rete, e che continua ad essere raggiungibile, ma con una ricerca più complessa e più lunga», così Cass. civ., sez. I, 8 febbraio 2022, n. 3952, in *Dir. inf.*, 2, 2022, 369 ss. con nota di P. Sammarco, *Diritto all'oblio e cancellazione delle copie cache del motore di ricerca*, in *Dir. inf.*, 2022, 383 ss. Pubblicata anche in *Dir. fam.*, 1, 2022, 122 ss. con nota di A. Alù, *Cancellazione delle "copie cache" e tutela del diritto all'oblio "digitale": spunti di riflessione sulla sentenza della Corte di Cassazione n. 3952/2022.*

[15] Si vedano in proposito: Cass. civ., sez. I, 31 maggio 2021, n. 15160, cit.; Cass. civ., sez. I, 19 maggio 2020, n. 9147, e Cass. civ., sez. I, 27 marzo 2020, n. 7559, in *Resp. civ. prev.*, 1, 2021 174 ss. con nota di M. Cocuccio, *Deindicizzare per non censurare: il «ragionevole compromesso» tra diritto all'oblio e diritto di cronaca.*

[16] CGUE, C-460/20, *TU, RE c. Google LLC* (2022).

[17] *Ibidem.*

Mentre per quanto concerne gli archivi storico digitali dei giornali usufruibili online[18], si distinguono due ipotesi.

Una prima ipotesi è quella degli articoli di stampa cartacea inseriti nell'archivio storico digitale di un quotidiano, il cui contenuto diffamatorio risulti già accertato con sentenza passata in giudicato: in questo caso «l'inserimento e il mantenimento nel suddetto archivio di quelle stesse informazioni integra una nuova e autonoma fattispecie illecita, ove sussista la lesione di diritti costituzionalmente garantiti (all'immagine, anche sociale, alla reputazione personale e professionale o alla vita di relazione), essendo differenti sia il tempo, sia la forma, sia la finalità della veicolazione di dette notizie. Ne segue che la successiva lesività diffusiva deve valutarsi in concreto, avuto riguardo a tutte le peculiarità del singolo caso, secondo gli ordinari criteri di cui all'art. 2043 c.c., con onere probatorio a carico del soggetto leso, anche, se del caso, in via di presunzioni, di tutti gli elementi costitutivi della fattispecie (condotta, elemento soggettivo, nesso causale, danno), la cui sussistenza necessita di apposita indagine del giudice di merito»[19].

La seconda ipotesi è quella di articoli la cui l'originaria pubblicazione era, a suo tempo, perfettamente lecita. In questi casi il più recente orientamento giurisprudenziale ritiene che la sola deindicizzazione possa non essere sufficiente garantire in modo adeguato il diritto all'oblio dell'interessato, dovendosi apporre anche «una sintetica nota informativa, a margine o in calce», all'articolo che dia «conto dell'esito finale del procedimento giudiziario in forza di provvedimenti passati in giudicato, in tal modo contemperandosi in modo bilanciato il diritto ex art. 21 Cost. della collettività ad essere informata e a conservare memoria del fatto storico con quello del titolare dei dati personali archiviati a non subire una indebita lesione della propria immagine sociale»[20].

---

[18] Cass. civ., sez. I, ord. 11 gennaio 2023, n. 479, ha affrontato il tema della configurazione giuridica dell'archivio storico digitale di un quotidiano, negando che si tratti di un prodotto editoriale su supporto informatico dal momento che, non ne possiede i «tratti caratterizzanti (testata, diffusione o aggiornamento con regolarità, organizzato in una struttura, con un direttore responsabile, una redazione ed un editore registrato presso il registro degli operatori della comunicazione, finalizzato all'attività professionale di informazione diretta al pubblico)». Secondo la Cassazione è dirimente rimarcare che la «finalità dell'archivio è meramente compilativa e storica», tendenzialmente priva di «organizzazione giornalistica con struttura tipica - direttore responsabile redazione e via dicendo», consistendo in una mera «aggregazione di notizie, integralmente trasferite nell'archivio digitale, pubblicate dal quotidiano nel corso di svariati anni». Ne segue, come corollario di detto inquadramento, «l'inapplicabilità della speciale disciplina sulla stampa, posto che solo ove ricorra l'ipotesi di "giornale informatico" con le caratteristiche precisate potrebbe applicarsi integralmente la L. n. 47/1948 e successive modificazioni (per la verità non senza criticità, evidenziate dalla dottrina, anche su detta conclusione) e, in particolare, l'art. 11 sulla responsabilità oggettiva di proprietario ed editore», la cui applicazione va «rigorosamente limitata ai casi previsti, dato che introduce una particolare tipologia di responsabilità oggettiva - del proprietario della testata giornalistica e dell'editore - che, in via speciale e derogatoria rispetto ai principi generali della responsabilità civile, consente di presumere la sussistenza degli elementi costitutivi dell'illecito, e ciò in ragione del rischio d'impresa che grava, per l'appunto, su detti soggetti obbligati, correlato all'elevata diffusività lesiva dello strumento di veicolazione della notizia».

[19] Cass. civ., sez. I, 31 gennaio 2023, n. 2893, in *Foro it.* 2023, 2, I, 391 ss.

[20] *Ibidem*. Si veda anche Cass. civ., sez. III, 5 aprile 2012, n. 5525, in *NGCC*, 1, 2012, 836 ss. nota di A. Mantelero, *Right to be forgotten ed archivi storici dei giornali*: «a fronte dell'esigenza di garantire e mantenere la memoria dell'informazione si pone, come detto, il diritto all'oblio del soggetto cui l'informazione si riferisce. Se del dato è consentita la conservazione per finalità anche diversa da quella che ne ha originariamente giustificato il trattamento, con passaggio da un archivio a un altro, nonché ammessa la memorizzazione (anche) nella rete di Internet (ad esempio, pubblicazione on line degli archivi storici dei giornali), per altro verso al soggetto cui esso pertiene spetta un diritto di controllo a tutela

In proposito le Sezioni Unite hanno precisato che «quando si parla di diritto all'oblio ci si riferisce, in realtà, ad almeno tre differenti situazioni: quella di chi desidera non vedere nuovamente pubblicate notizie relative a vicende, in passato legittimamente diffuse, quando è trascorso un certo tempo tra la prima e la seconda pubblicazione; quella, connessa all'uso di internet ed alla reperibilità delle notizie nella rete, consistente nell'esigenza di collocare la pubblicazione, avvenuta legittimamente molti anni prima, nel contesto attuale e quella, infine, trattata nella citata sentenza Google Spain della Corte di Giustizia dell'Unione Europea, nella quale l'interessato fa valere il diritto alla cancellazione dei dati»[21].

Peraltro, nella sentenza Google Spain, la Corte di giustizia ha ribadito l'esigenza che la nozione di responsabile del trattamento sia soggetta ad un'interpretazione ampia, onde assicurare una tutela quanto il più possibile efficace e completa. Ragion per cui si è fatto ricomprendere in tale categoria anche quei soggetti che, al pari dei responsabili dei motori di ricerca, non esercitano alcun controllo sui dati personali pubblicati sulle pagine web di terzi; chiarendo in proposito che «il trattamento dei dati personali effettuato nell'ambito dell'attività di un motore di ricerca si distingue e si aggiunge a quello effettuato dagli editori di siti web, consistente nel far apparire tali dati su una pagina internet»[22]. In particolare, nel caso "Google Spain", si è statuito che l'attività del motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di internet secondo un determinato ordine di preferenza, deve essere qualificata come "trattamento di dati personali" e il gestore di detto motore di ricerca deve essere considerato come il "responsabile" del trattamento summenzionato[23].

Si è così ritenuto che la giurisprudenza della Corte di giustizia, configuri una «responsabilità concorrente tra gli editori dei siti web e i gestori dei motori di ricerca, in una prospettiva di massimizzazione della tutela dei dati personali quando questi siano diffusi attraverso il web»[24]. Tale principio ha trovato conferma anche nella giurisprudenza della Corte EDU, secondo la quale l'obbligo di deindicizzazione grava non soltanto sui gestori dei motori di ricerca, ma anche sugli amministratori di giornali online[25].

---

della proiezione dinamica dei propri dati e della propria immagine sociale, che può tradursi, anche quando trattasi di notizia vera - e "a fortiori" se di cronaca - nella pretesa alla contestualizzazione e aggiornamento della notizia, e se del caso, avuto riguardo alla finalità della conservazione nell'archivio e all'interesse che la sottende, financo alla relativa cancellazione».

[21] Cass. civ., sez. un., 22 luglio 2019, n. 19681, in *Resp. civ. prev.*, 5, 2019, 1556 ss. con nota di G. Citarella, *Diritto all'oblio: un passo avanti, tre di lat*o. La sentenza data la sua importanza è stata pubblicata anche in *Dir. Famiglia e delle Persone*, 4, 2020, 1260 ss. con nota di A. Spatuzzi, *Diritto all'oblio e rievocazione storica. Il bilanciamento delle Sezioni Unite*; *Cass. pen.*, 2020, 151 ss. con nota di M. Cerase, *Il diritto di espressione tra libertà di ricerca e pretesa alla dimenticanza*; *D&G*, 136, 2019, 3 ss. con nota di A. Mazzaro, *Diritto all'oblio: bilanciamento tra diritto di cronaca, diritto di rievocazione storica e diritto di riservatezza*; *Giur. cost.*, 1, 2020, 349 ss. con nota di M. Mezzanotte, *Il diritto all'oblio secondo le Sezioni unite: cerbero o chimera?*

[22] CGUE, C-131/2012, *Google Spain* (2014), in *Resp. civ. prev.*, 2014, 1159 ss. con nota di S. Peron, *Il diritto all'oblio nell'era dell'informazione on-line*.

[23] In questo senso anche Cass. civ., sez. I, 8 febbraio 2022, n. 3952, cit.

[24] Cass. civ., sez. VI, 30 agosto 2022, n. 25481, in *Foro it.*, 2022, 9, I, 2669 ss.

[25] CEDU, *Biancardi c. Italia*, ric. 77419/16 (2021).

Costoro, tuttavia, non sono tenuti a «provvedere, a seconda dei casi, alla cancellazione, alla deindicizzazione o all'aggiornamento di un articolo di stampa, a suo tempo legittimamente pubblicato, ancorché relativo a fatti risalenti nel tempo, in difetto di richiesta dell'interessato che è la sola a far scaturire in capo al gestore l'obbligo di provvedere senza indugio»[26]. Si ritiene difatti che in «doveroso bilanciamento degli interessi in gioco, sarebbe eccessivamente oneroso accollare al gestore di un archivio digitale di notizie l'onere di un controllo periodico del loro superamento e della loro inattualità, in difetto di qualsiasi parametro temporale fissato dalla legge e sulla base di elementi del tutto sconosciuti come l'evoluzione personale dei soggetti interessati»[27]. Saranno quindi questi ultimi a dover richiedere la deindicizzazione o la cancellazione; nonché - almeno in una certa misura - a dimostrare l'inesattezza manifesta delle informazioni che li riguardano. A tale ultimo proposito, si ritiene che il richiedente sia unicamente tenuto a «fornire gli elementi di prova che, tenuto conto delle circostanze del caso di specie, possono essere ragionevolmente richiesti al fine di dimostrare tale inesattezza manifesta; non è invece tenuto, in linea di principio, a produrre, fin dalla fase precontenziosa, a sostegno della sua richiesta di deindicizzazione presso il gestore del motore di ricerca, una decisione giurisdizionale, anche scaturente da procedimento sommario. Imporre un obbligo siffatto a detta persona avrebbe, infatti, l'effetto di far gravare su di essa un onere irragionevole»[28]. Se, dunque, il soggetto a cui la notizia si riferisce ha il diritto (e l'onere) di attivarsi per chiederne l'aggiornamento o la rimozione o la deindicizzazione; per altro verso, la condotta del gestore del sito e/o del motore di ricerca, in caso di ingiustificato rifiuto o ritardo ad adempiere, è ritenuta idonea a «comportare il risarcimento del danno patito successivamente alla richiesta (fermo l'onere di allegazione e prova del pregiudizio da parte dell'interessato)»[29].

4. Il diritto all'oblio online e gli obblighi dei motori di ricerca

Con specifico riguardo al tema centrale della decisione in commento, concernente i limiti dell'efficacia territoriale dei doveri di rimozione dei motori di ricerca, la Corte di Cassazione anzitutto fa richiamo ai principi espressi dalla Corte di giustizia UE. Quest'ultima, in particolare, ha statuito che il gestore di un motore di ricerca, è responsabile, non del fatto che dei dati personali compaiano su una pagina internet pubblicata da terzi, ma dell'indicizzazione di tale pagina tramite link presenti nell'elenco dei risultati che compaiono all'esito ad una ricerca[30]. In questi casi, osserva la Corte di giustizia, la responsabilità del gestore si attiva quando la persona interessata fa istanza di deindi-

[26] Cass. civ., sez. I, 7 marzo 2023, n. 6806.

[27] *Ibidem.*

[28] Cass. civ., sez. I, 7 marzo 2023, n. 6806, cit., la quale richiama gli insegnamenti di CGUE, C-460/20, *TU, RE c. Google LLC* (2022), cit.

[29] Cass. civ., sez. III, 1 marzo 2023, n. 6116.

[30] CGUE, C-507/17, *Google v. CNIL* (2019) , in *Resp. civ. prev.*, 2019, 1987, la sentenza è nota anche come "caso *CNIL*".

cizzazione e consiste nel valutare se, sulla base di tutte le circostanze del caso (quali la gravità dell'ingerenza nella vita privata e la necessità di protezione dei dati personali), l'inserimento dei link nell'elenco dei risultati sia, o meno, necessario a proteggere la libertà di informazione degli utenti interessati ad accedere a tale pagina mediante la ricerca effettuata tramite il motore di ricerca.

In quest'attività valutativa di bilanciamento dei diversi interessi in gioco (il rispetto della vita privata e la protezione dei dati personali da un lato, e la libertà d'informazione dall'altro lato) il gestore del motore di ricerca deve poi portare particolare attenzione al caso in cui i link rimandino a pagine internet contenenti dati relativi ad un procedimento penale che si riferiscono a una fase precedente di tale procedimento, non più corrispondente alla situazione attuale. Per tale particolare ipotesi la Corte, infatti, precisa come il gestore debba considerare tutte le circostanze concrete, quali ad esempio la natura e la gravità dell'infrazione di cui trattasi, lo svolgimento e l'esito della procedura, il tempo trascorso, il ruolo rivestito nella vita pubblica dalla persona interessata dal procedimento penale, l'interesse del pubblico al momento della richiesta, il contenuto e la forma della pubblicazione, nonché le sue ripercussioni sulla persona cui si riferiscono i dati pubblicati.

Osserva, inoltre la Corte di Cassazione come la citata decisione sul "caso CNIL", che limita l'obbligo di deindicizzazione del gestore del motore di ricerca al solo territorio dell'Unione Europea, precisa purtuttavia che è ben possibile - bilanciando opportunamente i contrapposti diritti – ordinare, se del caso, al «gestore del motore di ricerca di effettuare la deindicizzazione su tutte le versioni del suddetto motore» e, dunque, anche al di fuori del territorio dell'Unione Europea disponendo un ordine globale (come ad esempio era già stato deciso dalla Corte di giustizia nel c.d. "caso Glawischnig"[31]).

Del resto sempre la Corte di Cassazione aveva già avuto modo di chiarire che le «disposizioni nazionali in tema di protezione di dati personali e poteri del garante, dettate in attuazione della normativa europea in materia, si applicano anche al gestore di un motore di ricerca estero, quando il trattamento di dati personali (consistente nel reperimento, indicizzazione, memorizzazione e pubblicazione in rete di informazioni contenenti dati personali) sia effettuato nel contesto dell'attività pubblicitaria e commerciale di uno stabilimento del predetto gestore presente sul territorio italiano»[32].

In ogni caso, secondo la decisione in commento, da ciò consegue che ciascun Stato membro è «libero di effettuare nella sua disciplina nazionale, conformemente agli standard nazionali di protezione dei diritti fondamentali, un bilanciamento tra il diritto della persona interessata alla tutela della sua vita privata e alla protezione dei suoi dati personali e il diritto alla libertà d'informazione, per richiedere all'esito al gestore di tale motore di ricerca di effettuare una deindicizzazione su tutte le versioni del proprio

[31] Sull'obbligo di estensione a livello mondiale, la decisione in commento fa espresso richiamo alla decisione nota come "caso *Glawischnig*": CGUE, C-18/18, *Glawischnig-Piesczek* (2019). In proposito osserva la Corte di giustizia che la direttiva 2000/31/CE (ossia la direttiva sul commercio elettronico) non prevede «alcuna limitazione, segnatamente territoriale, alla portata dei provvedimenti che gli Stati membri hanno diritto di adottare conformemente alla direttiva in parola». Di conseguenza, essa «non osta a che detti provvedimenti ingiuntivi producano effetti a livello mondiale».

[32] Cass. civ., sez. I, 8 febbraio 2022, n. 3952, cit.

motore, incluse quelle extraeuropee»[33]. Osservando in proposito che, se un lato, la «tesi dell'inammissibilità degli ordini di rimozione/deindicizzazione globale (ossia destinati a produrre effetti anche su motori di ricerca extra UE)»[34], appare in «contrasto con il diritto della Unione europea come interpretato dalla Corte di Giustizia»[35]; dall'altro lato, il diritto alla protezione dei dati personali e il suo fondamento costituzionale, non tollerano «limitazioni territoriali nell'esplicazione della sera di protezione, tanto più che nella specie tale diritto si sovrappone e si accompagna ai diritti dell'identità, alla riservatezza e alla contestualizzazione delle informazioni»[36]. Tanto più che tramite internet la circolazione dei dati avviene con «modalità liquide e pervasive»[37], ragion per cui non sarebbe sufficiente alla tutela costituzionale dei diritti dell'interessato, limitare la «deindicizzazione alle sole versioni dei motori di ricerca corrispondenti a tutti gli Stati membri dell'Unione Europea»[38].

Con riguardo poi allo standard valutazione da effettuare nel bilanciamento tra diritto della personalità e diritto all'informazione, la Corte osserva che questo «non può essere che quello europeo e nazionale e non viene invece in considerazione il quadro giuridico di contemperamento fra i due diritti, previsto in altri Paesi il cui diritto nazionale non è applicabile al rapporto giuridico oggetto della pronuncia per il solo fatto che al destinatario sia imposto di provvedere alla deindicizzazione anche sulle versioni di quel Paese del suo motore di ricerca»[39].

Da ultimo, la decisione in commento ha ritenuto di censurare la sentenza del Tribunale nella parte in cui ha reputato insufficienti le prove offerte dal richiedente per giustificare la propria tutela del diritto all'oblio con riferimento ai motori di ricerca extraeuropei. Ha osservato in proposito la Corte di cassazione che il richiedente aveva invece fornito «tutti gli elementi necessari e sufficienti per giustificare il proprio interesse alla deindicizzazione extraeuropea dell'informazione». In particolare, il richiedente aveva provato di risiedere e di esercitare la propria professione fuori dall'Europa: dati questi non contestati e, ad avviso della Cassazione, «non suscettibili di rilevanti integrazioni ai fini della qualificazione dell'interesse all'estensione globale dell'ordine di protezione e in particolare dell'accertamento del possibile pregiudizio sui motori di ricerca extraeuropei»[40].

---

33 Così, testualmente, Cass. civ., sez. I, 15.11.2022, n. 34658, § 17, qui in commento.

34 Ivi, § 18.

35 *Ibidem.*

36 Ivi, § 19.

37 *Ibidem.*

38 *Ibidem.*

39 Ivi, § 22.

40 Ivi, § 26.

Il contrasto europeo alla disinformazione nel contesto della guerra in Ucraina: riflessioni a margine del caso *RT France*[*]

Pietro Dunn

Tribunale UE, 27 luglio 2022, causa T-125/22 *RT France c. Consiglio dell'Unione europea*

Dal momento che la propaganda e le campagne di disinformazione sono tali da mettere in discussione i fondamenti delle società democratiche e fanno parte integrante dell'arsenale di guerra moderna, le misure restrittive di cui trattasi [divieto temporaneo di radiodiffusione di contenuti] si inseriscono anche nel contesto del perseguimento da parte dell'Unione degli obiettivi assegnatile dall'art. 3, parr. 1 e 5, TUE.
Tenuto conto del fatto che l'esercizio della libertà di espressione comporta doveri e responsabilità, che sono tanto più importanti per quanto riguarda gli organi d'informazione audiovisivi, non si può sostenere che il trattamento delle informazioni in questione, che comporta iniziative di propaganda intese a giustificare e sostenere l'aggressione militare illegale, non provocata e ingiustificata dell'Ucraina da parte della Federazione russa, sia tale da richiedere la tutela rafforzata che l'art. 11 della Carta conferisce alla libertà di stampa, specialmente laddove tale tutela è invocata da un organismo d'informazione che sostanzialmente è sotto il controllo diretto o indiretto dello Stato aggressore, come avviene nel caso di specie.

Sommario

1. Premessa. – 2. Ricostruzione dei fatti. – 3. Sulla violazione della libertà di espressione e informazione della ricorrente. – 4. Gli altri motivi di ricorso. – 5. *RT France* quale legittimazione giurisprudenziale delle politiche di contrasto europee alla disinformazione? – 6. Rilievi conclusivi.

Keywords

disinformazione – propaganda bellica – servizi di media audiovisivi – libertà di espressione e di informazione – Carta dei diritti fondamentali dell'Unione europea

[*] Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

1. Premessa

La decisione analizzata, resa dal Tribunale dell'Unione europea nel luglio 2022, si pone nel contesto della strategia euro-unitaria di contrasto alla disinformazione e alla propaganda originate da e a favore di Paesi terzi. In particolare, la decisione concerne la conformità delle misure restrittive adottate dal Consiglio a carico dell'emittente ricorrente con i diritti e le libertà fondamentali oggetto di tutela da parte della Carta dei Diritti Fondamentali dell'Unione europea (Carta di Nizza).
In tal senso, di particolare interesse sono le riflessioni operate dai giudici di Lussemburgo con riferimento al rapporto tra la libertà di espressione e di informazione, da una parte, e il perseguimento delle finalità di interesse pubblico promosso dalle misure limitative adottate, dall'altra parte. Con riferimento a questo punto, la decisione riveste un ruolo significativo in quanto sembra offrire una copertura di carattere "costituzionale" alle opzioni e scelte operate dalle istituzioni euro-unitarie nel campo del contrasto alla disinformazione mediatica. Tematica, questa, che ha del resto trovato terreno sempre più fertile nel dibattito politico e legislativo interno all'Unione non solo nel contesto dell'adozione di misure sanzionatorie nei confronti della Federazione russa (almeno a partire dal 2014), ma, più in generale, nell'ambito della regolamentazione dei servizi audiovisivi.

2. Ricostruzione dei fatti

Il 1° marzo 2022, a seguito delle ostilità avviate dalla Federazione russa nei confronti dell'Ucraina a partire dal precedente 24 febbraio, il Consiglio dell'Unione europea adottava, su proposta dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, la decisione (PESC) 2022/351[1], la quale, nel modificare la precedente decisione 2014/512/PESC[2], adottava alcune misure e sanzioni volte a sostenere «senza riserve la sovranità e l'integrità territoriale dell'Ucraina»[3].
In particolare, rilevando l'attuazione in anni recenti di una «sistematica campagna internazionale di manipolazione dei media e di distorsione dei fatti»[4], la Decisione del Consiglio mira per l'appunto a contrastare tali pratiche da parte della Russia e l'impatto delle stesse sulla società civile dell'Unione europea e dei Paesi a quest'ultima limitrofi: a tal fine, essa introduce all'interno della decisione 2014/512/PESC un art. 4-*octies*, il quale vieta agli operatori «la radiodiffusione, ovvero il conferimento della capacità di diffondere, l'agevolazione della radiodiffusione o altro concorso a tal fine, dei contenuti delle persone giuridiche, delle entità e degli organismi elencati nell'allega-

[1] Decisione (PESC) 2022/351 del Consiglio del 1° marzo 2022 che modifica la decisione 2014/512/PESC concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina, OJ L 65/5.

[2] Decisione 2014/512/PESC del Consiglio, del 31 luglio 2014, concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina, OJ L 229/13.

[3] Decisione (PESC) 2022/351, cit., considerando 2.

[4] Ivi, considerando 6.

to IX, anche sotto forma di trasmissione o distribuzione»[5] attraverso qualsiasi mezzo tecnico (cavo, satellite, IP-TV, fornitori di servizi internet, piattaforme o applicazioni di condivisione di video su internet). Inoltre, la nuova norma prevede la sospensione di qualsiasi licenza o autorizzazione di radiodiffusione, nonché qualsiasi accordo di trasmissione e distribuzione con tali soggetti[6]. Per di più, la nuova Decisione ha previsto la modifica dello stesso allegato IX, contenente la lista di quei fornitori di informazione ritenuti espressione della propaganda di regime russa e, quindi, ritenuti passibili delle nuove misure[7]. Contestualmente alla decisione (PESC) 2022/351, il Consiglio adottava altresì il regolamento (UE) 2022/350[8] il quale modificava in maniera conforme anche il precedente regolamento (UE) n. 833/2014[9].

Tra gli altri, a essere inserita nella lista di persone giuridiche cui "chiudere" tutti i possibili canali di trasmissione di notizie false o manipolatorie, vi è precisamente Russia Today France (RT France), parte ricorrente nel caso in discussione. RT France è una società per azioni semplificata a socio unico, con sede in Francia, il cui capitale sociale è detenuto interamente dall'associazione senza scopo di lucro TV Novosti, priva essa stessa di capitale sociale e finanziata quasi interamente dallo Stato russo[10]. Di conseguenza, ai sensi del nuovo art. 4-octies della decisione 2014/512/PESC, la convenzione conclusa da RT France con il Conseil Supérieur de l'Audiovisuel (CSA), oggi confluito nell'Authorité de Régulation de la Communication Audiovisuelle et Numérique (ARCOM), in data 2 settembre 2015, finalizzata alla diffusione da parte della ricorrente dei propri servizi televisivi, veniva sospesa. La sospensione di tale convenzione, che concerneva peraltro la trasmissione del programma non solo in Francia ma, altresì, in tutti i Paesi francofoni[11], ha pertanto portato al temporaneo divieto di radiodiffusione dei contenuti provenienti da RT France in tutti gli Stati membri dell'Unione[12].

A fronte di tali sanzioni, RT France proponeva ricorso innanzi al Tribunale dell'Unione europea, richiedendo l'annullamento sia della decisione (PESC) 2022/351 sia del regolamento (UE) 2022/350. Il ricorso di RT France, in particolare, si fondava su quattro motivi addotti: violazione del diritto di difesa; violazione della libertà di espressione e di informazione; violazione della libertà di impresa; e violazione del principio di non-discriminazione sulla base della nazionalità.

---

5 Decisione 2014/512/PESC, cit., art. 4-*octies*, par. 1.

6 Ivi, art. 4-*octies*, par. 2.

7 Decisione (PESC) 2022/351, cit., art. 1, n. 2.

8 Regolamento (UE) 2022/350 del Consiglio del 1o marzo 2022 che modifica il regolamento (UE) n. 833/2014 concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina, OJ L 65/1.

9 Regolamento (UE) n. 833/2014 del Consiglio, del 31 luglio 2014, concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina, OJ L 229/1.

10 V. Tribunale UE, T-125/22, *RT France c. Consiglio* (2022), §2.

11 Ivi, §3.

12 Ivi, §27.

3. Sulla violazione della libertà di espressione e informazione della ricorrente

Il secondo, e più rilevante, motivo di ricorso proposto attiene alla supposta violazione, da parte del Consiglio dell'Unione europea, della libertà di espressione e di informazione della ricorrente. Secondo RT France, le misure implementate dagli atti impugnati non sarebbero state adeguate all'effettivo perseguimento degli obiettivi addotti dal Consiglio, ovverosia, da un lato, il contrasto alla "minaccia ibrida" proveniente dalla Federazione russa e, dall'altro lato, la preservazione della pace e il rafforzamento della stessa sicurezza internazionale. Invero, tali misure comporterebbero un pregiudizio eccessivo alla libertà di espressione e di informazione della ricorrente perché il divieto «temporaneo, generale e assoluto di radiodiffusione» renderebbe il servizio di informazione da essa reso inaccessibile in tutto il territorio dell'Unione[13]. Inoltre, secondo RT France, «le misure restrittive di cui trattasi non sarebbero accompagnate da alcun limite temporale chiaro ed oggettivo, in quanto la loro revoca sarebbe subordinata a una valutazione aleatoria, se non addirittura arbitraria, del Consiglio»[14].

Con riferimento a tale motivo di ricorso, i giudici sottolineano innanzitutto le peculiarità del mezzo espressivo utilizzato, ponendo in luce come «i media audiovisivi hanno spesso effetti molto più immediati e potenti della carta stampata»[15] e, pertanto, come il loro utilizzo determini un incremento nella diligenza richiesta ai fornitori di tali servizi audiovisivi nell'espletamento dei doveri e delle responsabilità che l'esercizio della libertà di espressione comporta[16]. Successivamente, la riflessione del Tribunale si concentra sul rispetto, da parte del Consiglio, delle condizioni individuate dall'art. 52, par. 1, della Carta di Nizza per la predisposizione di eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta stessa: ovverosia, la preventiva sussistenza di una legge sulla base della quale le misure siano state adottate; il rispetto del contenuto essenziale del diritto o della libertà soggetto o soggetta a limitazione; il perseguimento di un obiettivo di interesse generale riconosciuto dall'Unione o dell'esigenza di proteggere i diritti e le libertà altrui; nonché il rispetto del requisito della proporzionalità[17].

Di particolare rilievo risultano essere, nella presente sede, i rilievi effettuati dal Tribunale con riferimento al criterio del rispetto del contenuto essenziale del diritto in gioco, nonché quelli relativi alla proporzionalità delle misure adottate. Con riferimento

[13] Ivi, §§ 118-119. Così anche Ivi, §128: «In definitiva, qualunque sia la linea editoriale di un organo di informazione o il suo pubblico, un divieto generale e assoluto di radiodiffusione costituirebbe un vero e proprio atto di censura e non potrebbe essere considerato necessario né proporzionato al fine di conseguire efficacemente gli obiettivi invocati dal Consiglio».

[14] Ivi, §120.

[15] Ivi, §138.

[16] *Ibid.* Il tema della particolare rilevanza dei mezzi tecnologici utilizzati è di particolare interesse nel contesto della giurisprudenza, soprattutto di Strasburgo, relativa all'esercizio della libertà di espressione e di informazione. Così, con particolare riferimento all'utilizzo di sistemi digitali e di internet, si vedano *inter alia* CEDU, *Editorial Board of Pravoye Delo e Shtekel c. Ucraina*, ric. 33014/05 (2011); *Stoll c. Svizzera*, ric. 69698/01 (2007).

[17] *RT France c. Consiglio*, cit., §145.

al primo aspetto, i giudici dell'Unione rigettano primariamente l'argomentazione della ricorrente secondo cui gli atti impugnati non sarebbero accompagnati da confini temporali ben precisi: infatti, sostiene il Tribunale, le misure restrittive esaminate avrebbero carattere sia temporaneo sia reversibile soprattutto alla luce delle condizioni, cumulative, richieste per la loro proroga (da un lato, la cessazione dell'aggressione russa ai danni dell'Ucraina e, dall'altro lato, la cessazione da parte della Federazione russa e degli organi di informazione associati della conduzione di iniziative di propaganda contro l'Unione e gli Stati Membri)[18]. Inoltre, i giudici ritengono che gli atti impugnati non siano tali da incidere sul contenuto essenziale della libertà di espressione e di informazione in quanto, da un lato, essi non impediscono alla ricorrente di svolgere attività diverse dalla radiodiffusione (per esempio, svolgimento di attività di ricerca e di interviste) e, dall'altro lato, non vietano la diffusione di contenuti al di fuori dell'Unione: cosicché «alla ricorrente non è stato impedito né di produrre trasmissioni e contenuti editoriali né di venderle a entità non interessate dalle misure in questione […] che avrebbero potuto quindi diffondere tali contenuti al di fuori dell'Unione»[19].

Per quanto concerne, invece, il rispetto del requisito di proporzionalità, il Tribunale, dopo aver analiticamente appurato la pertinenza e sufficienza degli elementi di prova forniti dal Consiglio per iscrivere RT France nell'elenco delle persone giuridiche sottoposte alle misure restrittive adottate negli atti menzionati[20], si focalizza su tre punti: se le limitazioni siano appropriate; se esse siano, altresì, necessarie; infine, se il Consiglio abbia operato un corretto bilanciamento degli interessi in gioco. In primo luogo, i giudici, dopo aver rilevato l'ampio potere discrezionale di cui il Consiglio gode in materia di definizione della politica estera e di sicurezza comune ai sensi degli artt. 3, par. 5, 21, 23 e 24 del Trattato sull'Unione europea (TUE)[21], sottolineano che «il divieto temporaneo di diffusione dei contenuti della ricorrente, in quanto misura rientrante nell'ambito di una risposta rapida, unificata, graduale e coordinata» rappresenta invero «una misura appropriata per conseguire l'obiettivo di esercitare la massima pressione sulle autorità russe, affinché pongano fine alle loro azioni e politiche che destabilizzano l'Ucraina nonché all'aggressione militare contro tale paese»[22]. In secondo luogo, il Tribunale considera il menzionato divieto necessario alla luce della natura del canale di informazione a ciclo continuo caratterizzante il servizio offerto dalla ricorrente stessa: secondo i giudici, cioè, altre misure meno restrittive non avrebbero consentito di «raggiungere altrettanto efficacemente gli scopi perseguiti dagli atti impugnati […] dal momento che alcune di esse, come il divieto di diffusione di taluni contenuti […] sarebbero state praticamente impossibili da attuare, mentre altre, come l'obbligo di apporre un banner o un'avvertenza, avrebbero avuto efficacia limitata»[23].

Infine, il Tribunale considera corretto il bilanciamento tra gli interessi coinvolti operato dal Consiglio: infatti, la sentenza argomenta che i summenzionati obiettivi di interesse

[18] Ivi, §§ 154-155.

[19] Ivi, §§ 156-157.

[20] Ivi, §§ 170 ss.

[21] Ivi, § 193.

[22] Ivi, § 194.

[23] Ivi, § 197.

pubblico perseguiti dagli atti impugnati sono tali da prevalere sulle conseguenze negative prodotte a carico della libertà di espressione e di informazione della ricorrente[24]. In particolare, secondo i giudici, la diffusione di contenuti di disinformazione e propaganda a favore della Federazione russa non può essere oggetto della speciale tutela accordata dalla Carta di Nizza alla libertà di stampa, «specialmente laddove tale tutela è invocata da un organismo d'informazione che sostanzialmente è sotto il controllo diretto o indiretto dello Stato aggressore, come avviene nel caso di specie»[25]. Peraltro, il Tribunale argomenta altresì che l'attività di propaganda operata dalla ricorrente, essendo riferita a un contesto bellico in corso, ove l'azione della Federazione russa è stata riconosciuta nel contesto internazionale quale un atto di aggressione, costituisce potenzialmente un atto di propaganda di guerra, proibito dall'art. 20, par. 1, del Patto internazionale sui diritti civili e politici del 1966[26].
Alla luce di tali argomentazioni, pertanto, il Tribunale respinge il secondo motivo di ricorso, concludendo che gli atti impugnati non costituiscano una violazione della libertà di espressione e informazione della ricorrente ai sensi dell'art. 11 della Carta di Nizza.

4. Gli altri motivi di ricorso

Con riferimento al primo motivo di ricorso, relativo alla violazione del diritto di difesa a norma degli artt. 41 e, soprattutto, 48 della Carta dei diritti fondamentali dell'Unione europea, RT France muoveva, in particolare, dalla mancata previa notifica, da parte delle istituzioni dell'Unione, dell'adozione delle misure restrittive comportate dagli atti impugnati. Considerato il grave e irreversibile pregiudizio comportato da tali misure[27], l'assenza di una tale notificazione (o di una qualsiasi presa di contatto, anche informale, da parte dei rappresentanti politici e istituzionali dell'Unione) avrebbe privato la ricorrente della possibilità di esercitare efficacemente il proprio diritto di difesa, in particolare nella sua dimensione del diritto ad essere ascoltati nel corso del procedimento di adozione delle misure contestate[28]. Inoltre, a parere della ricorrente, la motivazione contenuta negli atti impugnati sarebbe stata «circolare e tautologica nonché insufficiente rispetto ai requisiti della giurisprudenza del giudice dell'Unione»[29]. Con riguardo alla violazione del diritto della parte a essere ascoltata nel corso del procedimento di adozione degli atti impugnati, peraltro, il Tribunale giustifica l'assenza di

[24] Ivi, § 204.

[25] Ivi, § 206.

[26] Ivi, § 210. A tal proposito, il Tribunale sottolinea altresì che, sulla scorta di quanto detto sopra «risulta che, nell'ambito della sua attività durante il periodo precedente all'aggressione militare dell'Ucraina da parte della Federazione russa e, soprattutto, nei giorni successivi a tale aggressione, la ricorrente ha realizzato un'azione sistematica di radiodiffusione di informazioni «selezionate», comprese informazioni palesemente false o ingannevoli, che rivelavano un evidente squilibrio nella presentazione dei vari punti di vista opposti, al preciso scopo di giustificare e sostenere detta aggressione» (§ 211).

[27] Ivi, §66.

[28] Ivi, §67.

[29] Ivi, §68.

una previa comunicazione alla parte ricorrente sottolineando, da un lato, il preciso contesto storico, di straordinaria ed estrema urgenza, in cui il procedimento stesso si era inserito[30] e, dall'altro lato, l'apprezzamento delle necessità connesse alle minacce "ibride" rappresentate dal potenziale inquinamento informazionale operato da organi di informazione finanziati dalla Federazione russa e ritenuti, in quanto tali, «essere la fonte di un'attività continua e concertata di disinformazione e manipolazione dei fatti», il cui contrasto sarebbe essenziale per «tutelare l'integrità del dibattito democratico in seno alla società europea»[31]. Allo stesso tempo, con riferimento alla supposta insufficienza delle motivazioni addotte dagli atti impugnati, il Tribunale ritiene tale parte del primo motivo infondata, in quanto il tenore letterale dei considerando contenuti negli atti stessi «non costituiscono affermazioni generiche e astratte, bensì motivazioni che si ricollegano direttamente alla ricorrente e alle sue attività e che espongono in modo sufficientemente specifico le ragioni per le quali le misure restrittive in questione sono state adottate nei suoi confronti»[32]. Pertanto, il Tribunale respinge il primo motivo di ricorso[33].

Parimenti, anche il terzo e il quarto motivo di ricorso, concernenti rispettivamente la violazione della libertà d'impresa e la violazione del principio di non discriminazione su base nazionale, sono rigettati dal Tribunale. Per quanto riguarda il terzo motivo di ricorso, infatti, i giudici ritengono il divieto impugnato pienamente giustificato dagli obiettivi di interesse generale perseguiti anche alla luce della libertà d'impresa[34]. Il quarto motivo di ricorso, a sua volta, viene rigettato alla luce del rilievo che la soggezione di RT France alle misure adottate dal Consiglio, sebbene certamente influenzata dall'appartenenza della stessa a un'associazione avente sede legale in Russia, sia stata in realtà determinata primariamente su due criteri differenti rispetto alla nazionalità della ricorrente, vale a dire, da un lato, la sussistenza di un provato controllo della rete televisiva da parte del governo russo e, dall'altro lato, la rilevata attuazione di atti di propaganda favorevoli all'aggressione dell'Ucraina. Pertanto, conclude il Tribunale, «contrariamente a quanto sostiene la ricorrente, la struttura del suo capitale o l'origine del suo finanziamento non costituisce l'unico motivo che ha indotto il Consiglio ad adottare gli atti impugnati», cosicché l'adozione delle discusse misure non è in alcun modo da imputarsi a un atto discriminatorio su base nazionale[35].

[30] Ivi, §86.

[31] Ivi, §88. Il Tribunale prosegue sottolineando che «l'intensa copertura mediatica dei primi giorni dell'aggressione militare dell'Ucraina, quale risulta dai diversi elementi tratti da fonti pubbliche, depositati agli atti di causa dal Consiglio, ha avuto luogo in un momento critico in cui le azioni di un organo di informazione, come la ricorrente, potevano avere un'influenza significativamente deleteria sull'opinione pubblica, creando altresì una minaccia potenziale all'ordine pubblico e alla sicurezza dell'Unione»

[32] Ivi, §109.

[33] Ivi, §115.

[34] Ivi, §228.

[35] Ivi, §239.

5. *RT France* quale legittimazione giurisprudenziale delle politiche di contrasto europee alla disinformazione?

La decisione del Tribunale in *RT France c. Consiglio* si inserisce, in realtà assai coerentemente, all'interno del quadro della strategia dell'Unione di contrasto alla disinformazione.

Tale strategia affonda le proprie radici nel marzo 2015 con l'invito, rivolto dal Consiglio europeo all'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, a costituire un piano d'azione in materia di comunicazione strategica, nonché a istituire una squadra *ad hoc*[36]. L'invito, il cui prodotto fu la costituzione della *task force* "East StratCom", era stato non a caso motivato proprio dallo scoppio, nel 2014, del conflitto russo-ucraino che aveva portato all'occupazione e alla successiva annessione della penisola di Crimea da parte della Federazione russa[37]. La *task force*, orientata in particolare a promuovere forme di comunicazione efficaci nel contesto del vicinato orientale, a rafforzarne il contesto mediatico generale e a migliorare le strategie europee di contrasto alla disinformazione estera, era il frutto della raggiunta consapevolezza, da parte delle istituzioni euro-unitarie, della minaccia insita nel fenomeno della disinformazione e, in particolare, nell'utilizzo della disinformazione da parte di Paesi terzi quale strumento di politica estera ovvero di strategia bellica.

Del resto, sulla scorta delle interferenze riscontrate nel 2016 in occasione del *referendum* britannico sulla *Brexit* e delle elezioni presidenziali statunitensi, gli anni successivi hanno visto un incremento sostanziale delle politiche dell'Unione di contrasto alla disinformazione, in particolare laddove originata da Paesi terzi, sia nel contesto dei tradizionali servizi massmediali, sia nel contesto del nuovo scenario di internet, contesto quest'ultimo ove la particolare rapidità di diffusione dei contenuti, unita alle dinamiche tipiche della comunicazione online (creazione di camere dell'eco, *filter bubbles* e polarizzazione delle posizioni)[38], ha aperto a nuove e significative sfide[39]. Da ultimo, anche la recente proposta della Commissione per un nuovo regolamento sulla libertà dei media

[36] Consiglio europeo, Conclusioni del 20 marzo 2015, EUCO 11/15.

[37] Cfr. European Union External Action, *Domande e risposte sulla task force East StratCom*, in eeas.europa.eu, 27 ottobre 2021. Sull'East StratCom task force, si veda tra gli altri C. Bjola – J. Pamment, *Digital containment: Revisiting containment strategy in the digital age*, in *Global Affairs*, 2-2, 2016, 131 ss., spec. 132-133.

[38] C.R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, Princeton NJ, 2017.

[39] La nuova stagione di contrasto alla disinformazione in rete fu avviata, in particolare, dalla Comunicazione COM(2018) 236 final del 26 aprile 2018 della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Contrastare la disinformazione online: un approccio europeo, 26 aprile 2018, COM(2018)236, nonché dal rapporto dell'High Level Group on Fake News and Online Disinformation: M. de Cock Buning *et al.*, *A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation*, Lussemburgo, 2018. Si veda altresì, da ultimo, il nuovo Codice rafforzato di buone pratiche sulla disinformazione del 2022, in *digital-strategy.ec.europa.eu*, 16 giugno 2022, destinato a rappresentare un innovativo strumento di co-regolazione del fenomeno in discussione nel campo digitale grazie, soprattutto, al coordinamento con il Digital Services Act (regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), GU L 277/1). Si veda, sul tema del nuovo Codice, il simposio dedicato all'interno del blog della presente rivista

(European Media Freedom Act, "EMFA")[40] si muove nella medesima direzione di contrasto al fenomeno della disinformazione, soprattutto laddove operato da fornitori di servizi professionali di informazione. La proposta, in particolare, è volta a incentivare e promuovere l'autonomia e l'indipendenza dei fornitori di servizi di media al fine di garantire il pluralismo e la correttezza dell'informazione, nonché di contrastare la diffusione di disinformazione. A tal fine, la proposta riconosce espressamente i rischi connessi al finanziamento delle testate e/o al loro assoggettamento da parte di Paesi terzi[41] e mira, pertanto, a limitare l'ingerenza di tali Paesi nel processo di formazione dell'opinione pubblica e, di conseguenza, nei processi democratici interni all'Unione e ai Paesi Membri[42].

La decisione del Tribunale per il caso *RT France* in esame, in questo senso, rappresenta un significativo tassello all'interno del quadro del contrasto europeo alla disinformazione e, in particolare, alla disinformazione originata da Paesi terzi. Nel rigettare le censure avanzate dalla ricorrente, motivate dal riferimento al plesso di norme della Carta di Nizza, la sentenza offre chiaramente una copertura, sotto il profilo del quadro europeo di tutela dei diritti fondamentali, non soltanto agli atti impugnati nel caso di specie ma, più in generale, all'insieme delle politiche europee nel settore in esame. In particolare, nell'operare un giudizio relativo alla proporzionalità delle misure adottate rispetto alla supposta violazione dei diritti della ricorrente, il Tribunale sembra offrire un ampio margine di discrezionalità e di azione al Consiglio (e, implicitamente, alle altre istituzioni), in virtù della sostanziale preminenza degli interessi generali perseguiti attraverso tali politiche.

Tale prospettiva emerge in maniera particolarmente significativa dall'articolazione della motivazione resa dai giudici con riferimento al rigetto del secondo motivo di ricorso relativo alla supposta violazione della libertà di espressione e di informazione della ricorrente, laddove, come menzionato sopra, le esigenze legate alla necessità di tutelare l'ordine pubblico dell'Unione, nonché l'integrità territoriale e la sovranità dell'Ucraina, finiscono per essere preminenti rispetto all'esercizio della libertà di espressione.

Non solo: i giudici del Tribunale, infatti, nella loro riflessione negano esplicitamente che l'utilizzo dei sistemi di comunicazione massmediali per finalità collegate alla disseminazione propaganda in favore di Paesi terzi, soprattutto nel contesto di un conflitto bellico in corso, sia meritevole di tutela rafforzata in quanto espressione della libertà di stampa[43]. Si tratta, questa, di una conclusione particolarmente rilevante alla luce del trattamento privilegiato tradizionalmente accordato, soprattutto nel contesto della giurisprudenza di Strasburgo, alla stampa e ai giornalisti, quali "cani da guardia" della democrazia[44].

---

[40] Comunicazione COM(2022)457 final del 16 settembre 2022 della Commissione, Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno (legge europea per la libertà dei media) e modifica la direttiva 2010/13/UE.

[41] Ivi, considerando 4.

[42] Cfr. ivi, art. 17.

[43] *RT France c. Consiglio*, cit., §206. V. *supra*.

[44] Cfr., *inter alia*, CEDU, *Observer e Guardian c. Regno Unito*, ric. 33014/05 (1991); *Jersild c. Danimarca*, ric. 15890/89 (1994)

Invero, il Tribunale non manca di addurre, a sostegno delle proprie conclusioni, importanti argomentazioni relative allo specifico contesto di riferimento delle azioni adottate dal Consiglio. Così, per esempio, i giudici sottolineano come la comunità internazionale si sia pressoché unanimemente schierata contro l'offensiva russa, tanto che, con ordinanza del 16 marzo 2022, la Corte internazionale di giustizia sosteneva che «l'Ucraina avesse un diritto plausibile di non essere oggetto di operazioni militari della Federazione russa»[45], ordinando a quest'ultima di sospendere le operazioni militari. Inoltre, come menzionato sopra, il Tribunale mostra di valutare con attenzione quali siano i risvolti, sotto i profili pratici, determinati dalle misure adottate dal Consiglio in capo alla libertà di espressione della ricorrente: in particolare, il Tribunale nota come a RT France non sia stato vietato l'espletamento di qualsivoglia attività legata alla libertà di espressione e di stampa. I giudici dimostrano, così, di avere condotto un effettivo e approfondito giudizio di bilanciamento nel caso in oggetto.

Sotto questo profilo, è interessante peraltro notare come il Tribunale ponga l'accento sulla necessità di tenere in conto, nel contesto del giudizio di bilanciamento tra gli interessi coinvolti, anche le specifiche modalità comunicative utilizzate e il differente grado di impatto che esse possono determinare. Così, per i giudici, non può essere ignorato che i media audiovisivi hanno spesso effetti molto più immediati e potenti della carta stampata in quanto «attraverso le immagini, gli organi di informazione audiovisivi possono comunicare messaggi che lo scritto non è idoneo a trasmettere»[46]. Per questo motivo, i doveri e le responsabilità che l'esercizio della libertà di espressione comporta «sono tanto più importanti per quanto riguarda gli organi d'informazione audiovisivi […] come la ricorrente»[47].

Non può tuttavia essere ignorata la potenziale portata che la decisione esaminata potrebbe avere *pro futuro* in qualità di precedente giurisprudenziale. Se *RT France* è motivata da ampi riferimenti a elementi di fatto e di contorno che ne supportano e avvalorano le conclusioni, le riflessioni, in astratto, in termini di diritto rappresentano anch'esse un elemento caratterizzante l'ossatura della pronuncia. Invero, l'analisi non si limita a una semplice disamina della singola controversia in esame (sulla base di un approccio *case-by-case*), ma contiene una pluralità di enunciati di principi di diritto, sul piano del diritto costituzionale e dei diritti fondamentali, che potrebbero determinare significative conseguenze nell'ambito del dibattito dottrinario e giurisprudenziale sul rapporto tra disinformazione, libertà di stampa e libertà di informazione. La scelta di rimuovere RT France dall'ambito di protezione della libertà di stampa, in tal senso, suscita in particolar modo perplessità e preoccupazioni in quanto sembra aprire alla possibilità per i giudici di Lussemburgo e, indirettamente, per i giudici nazionali di determinare autonomamente (se non arbitrariamente) i limiti di applicazione della libertà stessa. In tal senso, sembra auspicabile che la decisione *RT France* venga addotta con cautela quale precedente e modello per future pronunce, tenendo in accurato conto il carattere straordinario ed eccezionale dei fatti cui essa si riferisce e, in particolare, alla luce del particolare contesto storico e geo-politico rappresentato dalla violazione da parte della

[45] *RT France c. Consiglio*, cit., §204.

[46] Ivi, cit., §138.

[47] Ivi, §206.

Federazione russa dell'integrità territoriale dell'Ucraina.

6. Rilievi conclusivi

Complessivamente, la decisione del Tribunale per il caso in esame promuove l'approccio dell'Unione europea al contrasto al fenomeno della disinformazione, soprattutto nella forma di atti di propaganda proveniente da Paesi terzi. Nel rigettare i motivi di ricorso, presentati dalla ricorrente ai sensi della Carta di Nizza, la sentenza opera un giudizio di bilanciamento che tende a operare una gerarchia in astratto tra le finalità di interesse pubblico, perseguite dagli atti impugnati, e gli interessi addotti dalla ricorrente quale organo d'informazione di carattere audiovisivo.

Di particolare rilievo è, in tal senso, la conclusione di non ritenere violata la libertà di espressione della ricorrente ai sensi dell'art. 11 della Carta, nonché l'affermazione, assai significativa, secondo cui disinformazione e propaganda non siano da ritenersi in alcun modo coperti dalla specifica declinazione della libertà di espressione rappresentata dalla libertà di stampa.

Sebbene la soluzione adottata dal Tribunale appaia pienamente comprensibile e, in linea generale, condivisibile alla luce dello specifico contesto di riferimento e alla luce dell'urgenza di reagire a un evento contingente quale la violazione dell'integrità territoriale dell'Ucraina da parte della Federazione russa, l'approccio adottato dai giudici di Lussemburgo non manca di sollevare altresì alcune preoccupazioni. In particolare, desta perplessità la scelta di rimuovere, apparentemente *in toto*, dal campo di applicazione della libertà di stampa la produzione di contenuti asseritamente integranti forme di disinformazione e propaganda a favore di Paesi terzi, atteso l'inevitabile carattere discrezionale legato alla definizione di determinati contenuti come tali. Più in generale, sembra dunque auspicabile un atteggiamento cauto da parte dei giudici della Corte di giustizia (nonché dei giudici nazionali) nel seguire il modello offerto dalla decisione in esame: in particolare, dovranno tenersi in conto, *pro futuro*, le particolari e contingenti circostanze relative allo specifico caso affrontato dal Tribunale in *RT France*.

La Corte costituzionale dichiara l'illegittimità costituzionale del divieto, imponibile dal Questore, di possedere ed utilizzare il telefono mobile e riapre il dibattito sulle misure di prevenzione personali*

Davide Galliani e Marco Orofino

Corte costituzionale, 12 gennaio 2023, n. 2

È costituzionalmente illegittimo l'art. 3, c. 4, del decreto legislativo 6 settembre 2011, n. 159 (Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli articoli 1 e 2 della legge 13 agosto 2010, n. 136), nella parte in cui include i telefoni cellulari tra gli apparati di comunicazione radiotrasmittente di cui il questore può vietare, in tutto o in parte, il possesso o l'utilizzo ai soggetti che si trovino nelle condizioni previste dallo stesso art. 3.

Sommario

1. Premessa. – 2. Le ordinanze di rimessione dei giudici a quo e la scelta della Corte costituzionale di procedere alla riunione e decisione con unica pronuncia. – 3. Sull'espressione "qualsiasi apparato di comunicazione radiotrasmittente" e sull'esigenza dopo l'intervento della Corte costituzionale di un rapido intervento normativo. - 4. La violazione della garanzia costituzionale della riserva di giurisdizione prevista dall'art. 15 Cost. come presupposto della dichiarazione di illegittimità costituzionale dell'art. 3, c. 4, del Codice antimafia. - 5. Lo sviluppo contraddittorio del sistema di prevenzione. – 6. Il problema del fondamento costituzionale. – 7. Misure di prevenzione e misure di sicurezza. – 8. La riserva di legge in termini di prevedibilità e di proporzionalità. – 9. Osservazioni conclusive.

* Le osservazioni nel testo sono frutto del confronto tra i due Autori. I paragrafi 2, 3 e 4 sono specificamente ascrivibili a Marco Orofino e i paragrafi 5, 6, 7 e 8 Davide Galliani.

Keywords
libertà di comunicazione - misure di prevenzione - art. 15 Cost. - Codice antimafia - riserva di giurisdizione

1. Premessa

La sentenza della Corte costituzionale n. 2 del 2023 ha dichiarato l'illegittimità costituzionale dell'art. 3, c. 4, del decreto legislativo 6 settembre 2011, n. 159 (Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli artt. 1 e 2 della legge 13 agosto 2010, n. 136), nella parte in cui include i telefoni cellulari tra gli apparati di comunicazione radiotrasmittente di cui il Questore può vietare, in tutto o in parte, il possesso o l'utilizzo. Il parametro costituzionale utilizzato è l'art. 15 Cost. nella parte in cui la norma costituzionale prevede che ogni limitazione della libertà di corrispondenza e di ogni altra forma di comunicazione debba essere disposta, con atto motivato, dall'autorità giudiziaria.
La decisione della Corte ha quindi un impatto diretto su due tematiche di grande interesse.
La prima tematica è quella dell'applicazione delle garanzie previste dall'art. 15 Cost. ai divieti che il Questore può imporre all'utilizzo ed al possesso di mezzi di comunicazione. Il tema è, innanzitutto, quello della portata della riserva di legge e della riserva di giurisdizione previsti dalla norma costituzionale. Di qui però poi il ragionamento si allarga alla questione della necessaria garanzia dei diritti fondamentali nella società digitale. In questo senso, il cellulare o meglio lo *smartphone*, è una delle principali porte d'accesso alla società digitale e, quindi, ogni restrizione alla sua libertà di utilizzo finisce con riverberarsi su altri diritti costituzionali quali ad esempio la libertà di espressione, le libertà di partecipazione politica e le libertà economiche.
La seconda tematica è quella delle misure di prevenzione.
La decisione del giudice costituzionale, da un lato, ha evidentemente effetti immediati sulla legge che disciplina il potere del questore di disporre taluni divieti attraverso il cd. avviso orale. In particolare, la pronunzia cancella i telefoni mobili dal novero dei divieti imponibili dal Questore. Da un altro lato, essa riaccende necessariamente il dibattito sulle misure di prevenzione personali, in specie sulla durata minima e massima dei divieti anche quando imposti dal giudice.

2. Le ordinanze di rimessione dei giudici a quo e la scelta della Corte costituzionale di procedere alla riunione e decisione con unica pronuncia

La pronunzia della Corte scaturisce dalla trattazione riunita delle questioni poste da due ordinanze di rimessione: la prima è un'ordinanza dell'11 marzo 2021 del Tribunale

di Sassari nel procedimento penale a carico di L.A.; la seconda è un'ordinanza del 16 dicembre 2021 della Corte di Cassazione chiamata a pronunciarsi su un decreto con cui il Tribunale di Roma confermava le misure di prevenzione adottate dal Questore avverso B.M.

I casi e le ordinanze meritano un breve approfondimento perché non sono del tutto sovrapponibili.

Nel primo caso, siamo nell'ambito del primo grado di un giudizio penale presso il Tribunale. Il P.M. ha esercitato l'azione penale nei confronti di L.A, ai sensi dell'art. 76, c. 2, del decreto legge n. 159 del 2011, per la violazione del divieto disposto dal Questore di possedere qualsiasi apparato di comunicazione radiotrasmittente, ivi compresi i telefoni cellulari, imposto con avviso orale ai sensi dell'art. 3, c. 4, del medesimo decreto. Il Tribunale, con ordinanza 11 marzo 2021, sospende il giudizio e rimette alla Corte costituzionale la questione di legittimità su due norme.

La prima norma della cui costituzionalità il giudice *a quo* dubita è il c. 4 dell'art. 3 del d.lgs. n. 159 del 2011, nella parte in cui consente al questore di inibire qualunque mezzo di comunicazione radiotrasmittente e, quindi, l'uso del telefono cellulare. I parametri costituzionali invocati sono l'art. 15 Cost. e, nello specifico, la riserva all'autorità giudiziaria con atto motivato di qualunque provvedimento che abbia effetti limitativi sulla libertà in questione, nonché l'art. 3 Cost. sul presupposto che il potere attribuito al Questore, se esteso ai telefoni cellulari, sia irragionevolmente più ampio di quello attribuito all'Autorità giudiziaria nell'ambito delle misure di prevenzione imponibili ai sensi del medesimo atto normativo.

La seconda norma della cui costituzionalità il giudice *a quo* dubita è la fattispecie incriminatrice di cui all'art. 76, c. 2, dalla quale il giudizio penale è scaturito. In questo caso, il giudice *a quo* non argomenta circa il parametro costituzionale che si intende violato.

Nel secondo caso, l'ordinanza è della Corte di Cassazione. Il Tribunale di Roma, in composizione monocratica, aveva rigettato l'opposizione proposta da B.M. avverso l'avviso orale del Questore contenente lo specifico divieto di possesso e uso di "qualsiasi apparato di comunicazione radiotrasmittente" e "di accesso ad Internet", ricomprendendo tra gli strumenti vietati anche i telefoni cellulari. Contro il rigetto, B.M proponeva ricorso in Cassazione.

La norma della cui costituzionalità si dubita è sempre l'art. 4, c. 3, del d.lgs. n. 159 del 2011 con specifico riferimento, in questo caso, alla mancata previsione nella norma in questione di indicazioni circa la durata minima e massima dei divieti imponibili dal Questore. Il dispositivo della seconda ordinanza di rimessione non centra la questione sugli apparati di radiocomunicazione e sui telefoni cellulari, ma si limita all'indicazione della norma. Nel considerato in diritto dell'ordinanza, che secondo la giurisprudenza consolidata della Corte definiscono il *thema decidendum*, l'attenzione è innanzitutto dedicata all'assenza nella normativa in esame della durata minima e massima dei divieti imponibili. Di qui poi le argomentazioni si dipanano con particolare riferimento alla libertà di comunicazione ed alla libertà di espressione creando quella connessione, che la Corte costituzionale ha poi ritenuto preponderante ai fini della riunione dei due casi, con il divieto di possesso ed utilizzo di telefoni cellulari.

Il parametro di costituzionalità, stante anche il diverso fuoco dell'ordinanza, è in que-

sto caso più articolato.
Il giudice *a quo* lamenta, infatti, sia la violazione dell'art. 15 Cost., sia dell'art. 117, c. 1, Cost.
Per ciò che riguarda l'art. 15 Cost., il giudice *a quo* sottolinea come il potere del questore di vietare l'uso dei telefonini violi la garanzia della riserva di giurisdizione ivi stabilita.
Per ciò che attiene all'art. 117, c. 1, il giudice *a quo* utilizza la norma interposta per segnalare come i divieti che secondo la legge il Questore può imporre senza la previsione di alcun limite temporale non superano i test di legittimità che la Corte di Strasburgo ha definito per la valutazione delle restrizioni che impattano sugli artt. 8 (diritto alla vita privata) ed art. 10 (libertà di espressione) della CEDU. Con il riferimento all'art. 10 CEDU viene in considerazione anche l'art. 21 Cost., e di qui l'argomento per cui lo *smartphone* non rappresenta solo un mezzo di comunicazione, ma pure uno strumento, ormai imprescindibile, per essere informato ed informarsi.
Nello specifico, per il giudice *a quo* la mancanza di una qualsivoglia indicazione legislativa sui termini di durata dei divieti imponibili conduce al mancato rispetto del primo parametro elaborato dal Corte EDU, ossia l'esistenza di una sufficiente base legale per la restrizione che, secondo la giurisprudenza della Corte stessa, deve essere declinata non solo in senso formale, ma anche come "qualità della legge" e quindi "prevedibilità dell'effettiva restrizione". Inoltre, sempre secondo il giudice *a quo*, la mancata previsione di termini di durata violerebbe anche il criterio di proporzionalità per cui la restrizione deve sempre essere proporzionata allo scopo legittimo perseguito.
La Corte costituzionale, nelle *considerazioni in diritto*, dà conto del fatto che le due ordinanze hanno in comune solo una delle due disposizioni censurate e che soprattutto i parametri costituzionali sono solo in parte coincidenti. Tuttavia, la Corte procede alla riunione valorizzando la supposta violazione in entrambi i casi della garanzia costituzionale della riserva di giurisdizione contenuta nell'art. 15 Cost.
Nel valorizzare questa assonanza però finiscono con rimanere in ombra alcune dissonanze, tra le quali è lecito menzionare il fatto che la seconda ordinanza sembrerebbe tutta centrata sui termini di durata dell'avviso orale rafforzato e che il riferimento al divieto di possesso ed uso "di apparati di comunicazione radiotrasmittente" e del telefonino sembrerebbe piuttosto legato al tentativo di fondare il dubbio di costituzionalità sulla violazione dell'art. 117, c. 1, per mancato rispetto delle norme della convenzione EDU in materia di libertà di espressione e di comunicazione .
Inoltre, ma la questione è effettivamente poco chiara, il giudice *a quo* menziona il divieto di accesso ad Internet come divieto specifico imposto dal Questore e non come conseguenza del divieto di possesso ed uso del telefonino. Su questo punto, occorre però dire che l'ordinanza non offre una sicura ricostruzione dell'avviso orale del Questore e, quindi, la questione potrebbe anche dirsi viziata da inammissibilità.
In ogni caso, la riunione decisa dalla Corte costituzionale comporta la restrizione del *thema decidendum* alla legittimità dell'art. 3, c. 4, che disciplina il divieto di possesso ed utilizzo del telefono mobile come mezzo riconducibile nell'ambito delle espressioni "qualsiasi apparato di comunicazione radiotrasmittente", ai sensi della costante giuri-

sprudenza di legittimità cristallizzatasi in diritto vivente[1].

3. Sull'espressione "qualsiasi apparato di comunicazione radiotrasmittente" e sull'esigenza dopo l'intervento della Corte costituzionale di un rapido intervento normativo

La scelta della Corte costituzionale di riconoscere come diritto vivente la collocazione del telefono mobile tra i mezzi che il Questore può vietare nell'ambito del suo potere di interdire "qualsiasi apparato di comunicazione radiotrasmittente" richiede di analizzare tale espressione.

In proposito occorre dire che essa è certamente ampia, ma, al tempo stesso, tecnicamente precisa.

Per "apparato di comunicazione radiotrasmittente" si intende, secondo la terminologia tecnica, il complesso dei congegni che in un impianto servono allo scopo di comunicare attraverso apparecchi o stazioni radio. Vi rientrano sia gli apparecchi riceventi, sia quelli trasmittenti, sia le stazioni radio sia, infine, tutti i congegni che possono essere utilizzati per la creazione di una rete di comunicazione elettronica. Questo tipo di apparati si basa sull'uso di un trasmettitore radio che invia un segnale radio a una specifica frequenza, e di un ricevitore radio che riceve il segnale e lo converte in informazioni utilizzabili.

Non fa alcuna differenza, da un punto di vista tecnico, che si tratti di apparati di comunicazione radiotrasmittenti che operino su (o costruiscano) reti di comunicazione elettronica private oppure pubbliche.

Le reti private, vale la pena ricordare, sono quelle installate per servizi svolti nell'esclusivo interesse proprio del soggetto che crea la radio. In questo contesto, possiamo collocare radio amatori, ponti radio, Radio-lan ed apparecchiature di debole potenza come, ad esempio, i walkie talkie o le reti wireless di gestione domotica. Le reti pubbliche sono, invece, quelle utilizzate interamente per fornire servizi di comunicazione elettronica accessibili al pubblico, quali ad esempio le reti di comunicazione mobile o reti di accesso ad Internet. Esse sorgono a partire dagli anni novanta, prima in modalità analogica, cd. TACS, poi in modalità digitale, cd. GSM[2]. Oggi vanno sviluppandosi attraverso il 5G nell'ottica di un'integrazione tra reti fisse e reti mobili.

È assai probabile che il Legislatore del 2001, come rilevato dai giudici *a quo* e dalla Corte costituzionale stessa, con l'inserimento dell'espressione "apparati di radiocomunicazione radiotrasmittente" nel novero dei possibili divieti imponibili dal Questore,

[1] Si v., *ex multis,* anche per i riferimenti dottrinari M. Cavino, *Diritto vivente*, in *Dig. Pubbl.*, 2010. Un'interessante analisi dei casi in cui la Corte ha fatto ricorso a tale categoria è quella di L. Salvato, *Profili del diritto vivente nella giurisprudenza costituzionale*, St. n. 276, febbraio 2015, in *cortecostituzionale.it/studiRicerche.do*

[2] La disciplina delle reti private e delle reti pubbliche è oggi estremamente differenziata. Questa distinzione normativa è legata ai processi di liberalizzazione europea che si diffondono negli anni novanta e che hanno un primo consolidamento nel Framework 2002 e una successiva codificazione nel Codice europeo delle comunicazioni elettroniche.

volesse riferirsi solo a quegli apparati di comunicazione radiotrasmittenti che servono reti private proprio perché strumenti eccezionali di comunicazione rispetto a quelli comunemente utilizzati.

Pertanto è lecito supporre che il Legislatore volesse imporre un divieto di possesso ed uso di strumenti di comunicazione non ordinari, per impedire a soggetti "pericolosi" di servirsene per uno scopo criminoso, sfuggendo al contempo ad eventuali indagini e controlli di polizia. D'altra parte, come rilevato dalla Corte stessa e dai giudici *a quo*, la straordinarietà del mezzo è il filo conduttore, unitamente alla loro utilizzabilità per commettere reati, che unisce tutti gli oggetti di cui il Questore può vietare l'utilizzo a soggetti cd. pericolosi ai sensi del c. 4 dell'art. 3 del d.lgs. n. 159 del 2011[3].

Con ampia citazione di pronunce dei giudici di legittimità, la Corte costituzionale ha dato atto del fatto che l'espressione sia stata nel tempo oggetto di un'interpretazione che ha ricondotto sulla base del dato testuale i telefoni mobili – che pure sono apparecchi in grado di inviare e ricevere attraverso le sole reti pubbliche – nell'ambito dei possibili divieti del Questore. Questa interpretazione ha indubbiamente allargato ad un mezzo ordinario il potere di divieto del Questore.

Detto in altri termini, la giurisprudenza di legittimità non ha trovato sufficienti appigli per corroborare una diversa interpretazione volta a valorizzare l'intenzione originaria del Legislatore e superare un dato testuale così tecnicamente chiaro. In questo modo, non ha potuto che fondarsi un diritto vivente per cui i telefoni mobili, rientrando nell'ambito della locuzione di legge, possono essere oggetto di un divieto totale o parziale di possesso ed utilizzo.

Questa capacità espansiva, che la nozione tecnica ha dimostrato, non è, però, priva di conseguenze ed il giudizio in questione può rappresentare solo la punta d'*iceberg* del problema che tale *vis expansiva* comporta. Gli apparati di comunicazione radioelettrici sono oggi utilizzati in una vasta gamma di applicazioni, come la comunicazione tra stazioni radio, la comunicazione tra veicoli e stazioni di controllo, la comunicazione tra aerei e torri di controllo, la comunicazione tra navi e porti, la radiodiffusione, la televisione, la domotica e qualsivoglia trasmissione tra sensori intelligenti. Si considerino quanti nuovi apparecchi radio l'innovazione tecnologia abbia messo a disposizione dei cittadini: oltre agli *smartphone* e ai *tablet*, vi sono *smartwatch* ed ogni altro tipo di sensore di cui le nostre abitazioni e le nostre città ormai abbondano. Per cui se il Questore può vietare ai sensi di legge davvero qualsiasi "apparato di comunicazione radiotrasmittente" (esclusi, dopo la sentenza in oggetto, i telefoni mobili) ci troviamo davanti ad un potere che finirà con essere esorbitante e toccare molteplici tecnologie tra cui anche quelle serventi all'Internet of Things (IoT), all'IA e alla robotica.

Inoltre, occorre anche considerare che la realtà, già oggi con il diffondersi del 5G, è

[3] Non a caso gli altri oggetto di possibile divieto sono, ai sensi di legge, radar e visori notturni, indumenti e accessori per la protezione balistica individuale, mezzi di trasporto blindati o modificati al fine di aumentarne la potenza o la capacità offensiva, ovvero comunque predisposti al fine di sottrarsi ai controlli di polizia, armi a modesta capacità offensiva, riproduzioni di armi di qualsiasi tipo, compresi i giocattoli riproducenti armi, altre armi o strumenti, in libera vendita, in grado di nebulizzare liquidi o miscele irritanti non idonei ad arrecare offesa alle persone, prodotti pirotecnici di qualsiasi tipo, nonché sostanze infiammabili e altri mezzi comunque idonei a provocare lo sprigionarsi delle fiamme, nonchè programmi informatici ed altri strumenti di cifratura o crittazione di conversazioni e messaggi.

quella dell'integrazione tra reti fisse e reti mobili o radiotrasmittenti[4]. Il che finisce per rendere inutile qualsiasi distinzione e certamente ancor meno giustificata un'espressione che si riferisce alle apparecchiature che veicolano gli impulsi solo su reti radioelettriche. Non solo perché non c'è più nulla di eccezionale ma anche perché le reti fisse sono sempre più integrate da pezzi di rete mobile e viceversa.
Infine, sia anche consentito dire che la trasformazione è avvenuta anche con riferimento agli strumenti (o apparecchiature) atti a compiere il disegno criminoso. Per rimanere sulla questione dei telefoni mobili, più che il divieto in sé del possesso ha oggi senso nell'ottica di limitare le capacità di occultamento delle proprie azioni semmai vietare taluni software o talune *app* specifiche che promettono la non captazione dei messaggi. L'art. 3, c. 4, del Codice antimafia già prevede che il Questore con l'avviso orale possa vietare programmi informatici ed altri strumenti di cifratura o crittazione di conversazioni e messaggi. Dobbiamo aspettarci quindi un nuovo diritto vivente che allarghi il potere di divieto ad alcune *app* di messaggistica online?
È evidente dunque allora che, aldilà del diritto vivente che si è venuto a creare nel caso di specie o potrebbe affermarsi in futuro, la pronunzia qui in esame con cui la Corte costituzionale dichiara l'incostituzionalità della norma nella parte in cui include i telefoni cellulari tra gli "apparati di comunicazione radiotrasmittente" mostra anche quanto tale terminologia e la norma in sé meritino una rapida revisione da parte del Legislatore.
Non già perché le espressioni usate non siano chiare quanto piuttosto perché l'evoluzione tecnologia ha finito con ricondurre al loro interno strumenti tutt'altro che straordinari modificandone la portata e la ratio.

4. La violazione della garanzia costituzionale della riserva di giurisdizione prevista dall'art. 15 Cost. come presupposto della dichiarazione di illegittimità costituzionale dell'art. 3, c. 4, del Codice antimafia

La Corte costituzionale fonda, come si è anticipato, l'accoglimento della questione di legittimità costituzionale proposta sull'art. 15 Cost. che, come noto, richiede che ogni limitazione della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione sia disposta dall'autorità giudiziaria, con le procedure, le modalità e i tempi che compete al legislatore prevedere, nel rispetto della riserva di legge assoluta prevista dalla Costituzione.
L'assunto di partenza nel ragionamento della Corte costituzionale è che le regole generali «attinenti al mezzo che, per comunicare, venga di volta in volta utilizzato sono cosa in sé diversa dalla disciplina relativa al diritto fondamentale»[5]. Il che significa che

[4] D'altra parte già oggi, laddove residua un telefono che noi definiamo fisso in quanto collegato alle reti che tradizionalmente indichiamo come reti fisse, siamo, in realtà, davanti a reti ibride. Ciò, in senso tecnico, non è nemmeno una novità se si pensa che i telefoni cordless esistono da venti anni.

[5] Si tratta di un'argomentazione diversa rispetto a quella pacifica in dottrina per cui l'art. 15 Cost. non riconosce al titolare del diritto di comunicare la disponibilità dei mezzi tecnici per farlo (il cd. diritto al mezzo). Tale dottrina si sviluppa soprattutto con riferimento all'art. 21 Cost. e di qui poi è applicata

non tutte le restrizioni normative all'utilizzo di uno specifico mezzo di comunicazione si convertono automaticamente in una restrizione del diritto di comunicare.

Ciò sicuramente accade, per la Corte, quando il mezzo disciplinato riveste, come nel caso del telefono mobile, un particolare rilievo «a livello relazionale e sociale». In questo caso, infatti, la disciplina del mezzo, sempre citando testualmente la Corte, «finisce per penetrare all'interno del nucleo essenziale del diritto», così determinando «evidenti ricadute restrittive sulle libertà tutelate in Costituzione».

In altri termini, le restrizioni all'uso del telefono mobile si convertono sempre, considerata la diffusione dello strumento in ogni ambito della nostra vita lavorativa, familiare e personale, in restrizioni del diritto fondamentale qui oggetto di considerazione.

Tali restrizioni possono essere ritenute legittime, secondo l'argomentare del giudice costituzionale, solo se fondate su interessi pubblici costituzionalmente rilevanti e se sono rispettate le garanzie costituzionali.

Con riferimento al primo profilo, ossia al fondamento sostanziale delle restrizioni disciplinate nell'art. 3, c. 4 del Codice antimafia, la Corte afferma che le esigenze di prevenzione e difesa sociale sono certamente interessi di natura costituzionale astrattamente idonei a fondare restrizioni che incidono sui diritti fondamentali in generale e sulla libertà di comunicazione nello specifico[6].

Del pari, però, le restrizioni all'uso di questo specifico mezzo debbono rispettare le garanzie costituzionali che, ai sensi dell'art. 15 Cost., sono la riserva assoluta di legge e la riserva di giurisdizione che, come noto, impone che la misura limitativa nei confronti del singolo individuo sia disposta «con atto motivato dell'autorità giudiziaria»[7].

La Corte non si esprime sulla base legale della restrizione. In termini formali non può dubitarsi del rispetto della riserva di legge assoluta visto che la fonte su cui si fonda la restrizione è un decreto legislativo. Certo, l'ordinanza della Cassazione poneva in dubbio il fatto che la norma rispettasse il criterio legale posto dal test di legittimità elaborato dalla CEDU, nella misura in cui l'art. 3, c. 4, non consente la prevedibilità della restrizione, mancando i termini massimi e minimi della misura del Questore. Qui c'è tutta la distanza che intercorre tra la riserva di legge assoluta che in ambito interno è formale e il criterio di legalità ricostruito dalla Corte di Strasburgo che è, invece, tutto sostanziale[8].

---

all'art. 15 Cost. V. in proposito C. Esposito, *La libertà di manifestazione del pensiero*, Milano, 1958, 27, nt. 58 e V. Crisafulli, *Problematica della libertà d'informazione*, in *Il Politico*, 1964, 291 Argomento però sempre temperato, dal *favor* per la «tendenziale espansione della possibilità di comunicazione» come ricorda M. Olivetti, *Diritti fondamentali*, Torino, 2020, 235, citando a questo proposito la sentenza della Corte cost. n. 1030/1988.

[6] Si rinvia sul punto alle osservazioni di D. Galliani nei prossimi paragrafi.

[7] Secondo alcuni anche la riserva di giurisdizione dovrebbe essere considerata assoluta perché non tollererebbe alcuna eccezione. Si v. la ricostruzione di M. Olivetti, *Diritti fondamentali,* cit., 236 e, in particolare, l'analisi dell'unico caso in cui la Corte costituzionale nella sent. 1114/1966 sembrò orientarsi in maniera diversa nello scrutinio della legge che consentiva all'amministrazione postale il fermo provvisorio (non il blocco né l'apertura) della corrispondenza (v. art. 13 Cod. post).

[8] Questa differenza ha come rovescio della medaglia il fatto che ai sensi della Convenzioni restrizioni ai diritti fondamentali possano discendere da norme giuridiche non di rango primario, purché sia rispettato il principio di prevedibilità, mentre la nostra Costituzione, a maggior garanzia in taluni casi richiede la fonte primaria. V. sulla distinzione M. Betzu, *La riserva assoluta di legge come principio politico e la legge come principio gnoseologico*, *in Costituzionalismo*, 2, 2013, 10. Sia consentito rinviare sul punto anche M. Orofino,

In ogni caso, la Corte costituzionale evidenzia come certamente la riserva di giurisdizione di cui all'art. 15 Cost. non possa dirsi rispettata, posto che l'avviso orale, con cui si vieta l'uso ed il possesso del mezzo, è disposto dal questore che è, a tutta evidenza, un'autorità amministrativa. Ciò viola, secondo la Corte costituzionale, l'obbligo secondo il quale deve essere il giudice con atto motivato ad imporre la limitazione. Tale obbligo per costante giurisprudenza è sempre da intendersi a monte del provvedimento e non a valle del medesimo, nel senso di un controllo giurisdizionale. Questo vale in ogni caso in cui la Costituzione prevede una riserva di giurisdizione, ma a maggior ragione per l'art. 15 Cost., che proprio a fini di estrema garanzia, non prevede nemmeno la possibilità, come ad esempio per la libertà personale o per la libertà di stampa, che le forze di pubblica sicurezza o gli ufficiali di polizia giudiziaria possano procedere alla limitazione, salvo conferma successiva del giudice[9].

Per cui, anche il fatto come rammenta l'Avvocatura di Stato nelle sue difese, che avverso l'avviso orale sia possibile ricorso davanti al Giudice – ed una delle ordinanze di rimessione scaturisce proprio da tale ricorso – non è di per sufficiente a superare la censura proposta[10].

La decisione della Corte costituzionale che dichiara l'incostituzionalità della legge nella parte in cui, per diritto vivente, include il telefono mobile tra gli oggetti che il Questore può vietare è ovviamente ampiamente condivisibile e sana un'illegittimità che ha negli anni recenti ingiustamente ristretto la libertà di comunicazione di soggetti destinatari di tale divieto disposto in via amministrativa.

Del pari assai opportuno è il ragionamento della Corte (e dei giudici *a quo*) con cui si sottolinea la necessità di valutare con estrema attenzione le restrizioni all'uso di terminali (quali i telefoni mobili) che rappresentano oggi la porta d'accesso alla società digitale. Questo diverrà sempre più importante, e non solo nell'ambito delle misure di prevenzione, quando si riuscirà a far emergere nel dibattito quanto possa essere afflittivo oggi il divieto dell'utilizzo delle rete. In questo senso la pronunzia della Corte segna un passaggio fondamentale per l'emersione della questione.

Ciò non toglie però che dall'argomentare della Corte costituzionale, per giungere alle sue conclusioni, possano sorgere alcune rilevanti perplessità soprattutto laddove alcuni passaggi del *reasoning* divenissero un *modus operandi*.

La prima perplessità è legata alla distinzione che la Corte sembra operare tra mezzi che hanno un particolare rilievo, a livello relazionale e sociale, e mezzi che ne sono privi. Per i primi, ogni divieto d'uso comporterebbe una restrizione del diritto (per la Corte del suo nucleo essenziale) che, invece, non vi sarebbe per i secondi o, almeno, non sarebbe "automatico". Solo nel primo caso sembrerebbe allora sorgere l'obbligo di rispettare le garanzie costituzionali, per imporre la restrizione ossia la riserva di legge assoluta e la riserva di giurisdizione.

La libertà di espressione tra Costituzione e Carte europee dei diritti, Torino, 2014, 46-48.

[9] V. sull'interpretazione della scelta del Costituente come orientata dalla necessità di offrire alla libertà di comunicazione maggiori garanzie di tutela perché nel caso della comunicazione esiste per definizione anche un terzo coinvolto v. A. Pace, *Problematica delle libertà costituzionali,* II, Padova, 1992.

[10] Ben potrebbe il Questore, afferma la Corte – quasi suggerendo al Legislatore una possibilità di intervento – suggerire l'adozione di un tale provvedimento, ma dovrebbe essere il giudice ad adottarlo.

Per cui, se si interpreta correttamente l'argomentare della Corte, eventuali restrizioni all'uso di altri mezzi di comunicazione, che certamente oggi non sono così rilevanti a livello relazionale, familiare e lavorativo, come, ad esempio, i walkie talkie, non comporterebbero restrizioni del diritto e, quindi, sarebbero esentate dal rispetto delle garanzie dell'art. 15 Cost.

Una tale lettura non sembra essere in linea con quella prevalente in dottrina, secondo cui l'art. 15 Cost., tutela l'uso anche di mezzi arcaici e superati dal progresso tecnico e di mezzi non convenzionali, come sempre si usa esemplificare, sono i segnali di fumo ed i piccioni viaggiatori[11]. D'altra parte che l'intenzione dei Costituenti fosse quella di estendere le garanzie costituzionali all'uso di qualsivoglia mezzo di comunicazione è testimoniato dal fatto che dopo aver centrato la norma sulla corrispondenza inserirono la clausola valvola dell'«ogni altro mezzo di comunicazione»[12].

In questo senso la distinzione tra mezzi rilevanti e non rilevanti che sembra leggersi in controluce nel *reasoning* della Corte parrebbe un criterio di limitazione della clausola aperta dell'art. 15 Cost. Un criterio che però non è corredato di indici di valutazione per ricondurre ogni singolo mezzo in una o l'altra categoria.

La diversa rilevanza sociale e relazionale dei mezzi di comunicazione è certamente da tenere in conto nel senso che il Legislatore, nel disciplinare l'utilizzo di uno specifico mezzo, laddove intenda imporre limitazioni o divieti, deve espressamente valutare come le sue scelte possano incidere, in modo diverso a seconda del mezzo oggetto di disciplina, sui diritti sottostanti. In questo modo verificando l'impatto delle restrizioni sul diritto, anche alla luce dei test di legittimità adottati dalla Corte di Strasburgo. Altra cosa però è ritenere che se il mezzo non è attualmente rilevante dal punto di vista sociale o relazionale allora la restrizione d'uso può essere disciplina da una fonte non legislativa ed imposta da un'autorità amministrativa.

A maggior ragione, il criterio del "particolare rilievo relazionale e sociale" di un mezzo non può comunque, ad avviso di chi scrive, essere ribaltato sulla riserva di giurisdizione prevista nell'art. 15 Cost., poiché essa opera non in astratto, ma in concreto rispetto alla limitazione imposta nei confronti di una specifica persona. Una diversa lettura comporterebbe un'attenuazione della garanzia costituzionale della riserva di giurisdizione che invece opera a presidio delle libertà individuali perché ha lo scopo di verificare, caso per caso, in concreto se ricorrono le condizioni per la limitazione previste dalla legge in astratto[13].

Per cui, ad avviso di chi scrive, come è il giudice a dover vietare al singolo l'uso del tele-

[11] V. sul punto la ricostruzione riassuntiva di F. Donati, *Art. 15*, in R. Bifulco – A. Celotto – M. Olivetti (a cura di), *Commentario della Costituzione*, Torino, 2006, 364.

[12] La «clausola aperta o valvola» aveva come scopo proprio garantire l'applicabilità del paradigma ad ogni mezzo idoneo a realizzare una comunicazione di tipo interpersonale senza dover ricorre a forzature interpretative. V. P. Giocolo Nacci, *La libertà di corrispondenza*, in *Trattato di diritto amministrativo*, diretto da G. Santaniello, vol. XII, Padova, 1990, 121. V. in proposito su come questa apertura sia stato voluta dai Costituenti, anche R. Zaccaria - A. Valastro - E. Albanesi, *Diritto dell'informazione e della comunicazione,* Padova, 2013, 75-76. L'unico limite all'applicazione della clausola potrebbe essere riferito a mezzi o oggetti che non sono specificamente atti a comunicare. V. però anche contro tale possibile limitazione della norma costituzionale P. Barile *I diritti dell'uomo e le libertà fondamentali*, Bologna, 1984, 165.

[13] V. in proposito anche per i rimandi dottrinari, F.G. Pizzetti, *Giurisdizione: riserva di (voce),* in *Dizionario di diritto pubblico*, diretto da S. Cassese, vol. III, Milano, 2006, 2740 ss.

fonino così è il giudice a dover disporre il divieto individuale (a meno che la legislazione non vieti l'uso in sé dello strumento) del walkie talkie o di altro mezzo di comunicazione. D'altra parte, nessuno dubita che un'eventuale limitazione della corrispondenza epistolare debba essere disposta sempre dal giudice – non fosse altro perché essa è l'archetipo della corrispondenza dell'art. 15 Cost., anche se nessuno può sostenere che tale mezzo sia oggi rilevante a livello relazionale e sociale[14].

Naturalmente, la Corte costituzionale, nella pronuncia qui in commento, si limita a pronunciarsi sui telefoni mobili e, quindi, quanto qui sopra detto potrebbe ritenersi solo un "inutile caveat" dell'Autore rispetto all'argomentare del giudice costituzionale. Il fatto però che il giudice costituzionale non abbia optato, come pure forse avrebbe potuto, per una pronuncia di illegittimità consequenziale della norma, nella parte in cui facoltizza il Questore a vietare l'uso di qualsivoglia apparato di comunicazione radio elettrica, impone di porsi almeno il problema[15].

È se, infine, questa scelta fosse stata dettata da una comprensibile linea di prudenza per non privare il Questore di uno strumento significativo, allora questo mostrerebbe ancora di più la necessità di un intervento legislativo di riforma della fattispecie legale per rimettere la medesima in asse sia con l'innovazione tecnologica che con le garanzie costituzionali.

5. Lo sviluppo contraddittorio del sistema di prevenzione

Nel momento in cui l'osservatore si appresta a svolgere qualche riflessione più generale sul *nostro* sistema di prevenzione è colpito da una serie di marcate e inquietanti contraddizioni, che riguardano almeno due lati della questione, uno storico-istituzionale e uno più giuridico. Contraddizioni che, vale la pena insistere, sono tipicamente italiane, senza che questo significhi disconoscere talune tendenze comune rilevabili in altri ordinamenti, riferite a quelle che sono state definitive le misure di *exprisonment*[16].

Da un punto di vista storico-istituzionale, basta porsi una domanda: rispetto al periodo liberale e a quello fascista, pur limitandoci alle misure di prevenzione personali, possiamo dire di essere stati spettatori di una decisa contrazione o anche di una cauta riduzione, oppure lo scenario è di accrescimento, di allargamento? Ancora più specifica, la domanda: se guardiamo al numero di misure di prevenzione personali e ai possibili

[14] Se non per le persone detenute in carcere per le quali, stante l'impossibilità di utilizzare altri mezzi, la corrispondenza epistolare permane il mezzo più rilevante. Il che chiaramente rappresenta un'osservazione che dovrebbe spingere anche ad interrogarsi sugli effetti della privazione totale dell'accesso alle nuove tecnologie per tali persone.

[15] Le opinioni in dottrina sull'illegittimità consequenziale sono oscillanti come d'altra parte la giurisprudenza. Esse riguardano se dare un'interpretazione più o meno ampia all'art. 27 della legge n. 87 del 1953. Così A. Ruggeri - A. Spadaro, *Lineamenti di giustizia costituzionale*, Torino, 2001, 289 Le ragioni a sostegno di un'interpretazione più ampia sono esigenze di economia processuale, certezza del diritto e, soprattutto, la necessità espungere dall'ordinamento costituzionale il maggior numero possibile di norme illegittime per tutela tempestivamente i valori costituzionali. V. sul punto G. Zagrebelsky, *La giustizia costituzionale*, Bologna, 1988, 214

[16] Si veda H. Noorda, *Exprisonment: Deprivation of Liberty on the Street and at Home*, in *Criminal Justice Ethics*, 2023, 1 ss.

destinatari, come siamo messi oggi rispetto a ieri?
Si potrà sostenere, con buone ragioni, che il problema non è di quantità ma di qualità e che, quindi, il legislatore è intervenuto in un'ottica di razionalizzazione, con provvedimenti mirati e specifici, insomma che esistono oggi problemi che non esistevano ieri e che, di conseguenza, l'intervento del legislatore è comprensibile, anche giustificabile. Se esistono più misure di prevenzione personali e più destinatari è perché i problemi da affrontare sono aumentati, non diminuiti.
Questa può essere una chiave di lettura. Non di meno, ed è qui il senso di vertigine che sprigiona una fortissima contraddittorietà, è mai possibile che esistano oggi delle misure di prevenzione che non esistevano ieri e che la platea dei possibili destinatari è cresciuta in modo esponenziale e soprattutto irrazionale, senza che si riesca a comprendere alcun "preciso" disegno di politica criminale?
D'altro canto, le misure di prevenzione personali non costituiscono una eccezione. A chi non verrebbe di accostare la crescita esponenziale dei destinatari delle misure di prevenzione personali alla crescita altrettanto incessante dei reati ricompresi nel catalogo di cui all'art. 4 bis, c. 1, dell'ordinamento penitenziario? Così come non risulta comprensibile prevedere un unico regime, quello ostativo, per l'associazione di tipo mafioso, la tratta di persone, la pornografia minorile, la violenza sessuale di gruppo e la riduzione in schiavitù, allo stesso modo è mai possibile che una specifica misura di prevenzione personale possa essere utilizzata nei confronti di autori di furti, rapine e truffe, verso chi detiene e cede in modo illecito degli stupefacenti, e ancora autori di reati sessuali contro minorenni, di fatti di ubriachezza, di atti osceni, di invasione di edifici e di reati in ambito familiare?
A poco servirebbe sottolineare che nel primo caso (regime ostativo) si tratta di un accostamento voluto da una (precisa?) scelta nel tempo del legislatore, mentre nel secondo (misure di prevenzione personali) l'accostamento è figlio della stessa idea che sorregge la prevenzione, vale a dire la (sospetta) pericolosità, riferendosi a quella generica e a quella rispetto alla sicurezza pubblica[17]. Non servirebbe a molto poiché la conclusione sarebbe identica: qui non sono in discussione gli sforzi tassativizzanti in particolare della Cassazione, e nemmeno la necessità di giungere ad uno statuto unitario dell'apprezzamento della pericolosità sociale[18], quello che si vuole dire è che spostare il fuoco

[17] Se stiamo all'avviso orale, la giurisprudenza dei TAR non lascia alcun dubbio. La misura può essere motivata con riferimento «anche a semplici sospetti a carico del destinatario, purché basati su elementi di fatto che ne facciano ragionevolmente ritenere l'appartenenza a una delle menzionate categorie», vale a dire quelle della pericolosità generica. Non solo: «il giudizio sulla pericolosità sociale del soggetto avvisato non richiede la commissione di specifici reati, essendo sufficiente che l'Autorità di polizia sospetti semplicemente della presenza di elementi tali da ritenere la configurabilità, nel soggetto destinatario dell'avviso, di una personalità propensa a seguire particolari comportamenti antigiuridici». Tanto il giudizio constatativo (quello che inquadra nella pericolosità generica) quanto quello prognostico (quello sulla attuale pericolosità per la sicurezza pubblica) sono quindi basati sul semplice sospetto. Quando l'avviso diviene rinforzato deve esserci stata condanna definitiva per almeno due delitti non colposi: non uno, ma due o più, come si esprime in modo inequivoco l'art. 3, c. 5, del codice antimafia, e come del resto si è espressa la giurisprudenza di legittimità. Si veda per citazioni della giurisprudenza dei TAR, compresi i passaggi sopra citati: F. Basile, *Manuale delle misure di prevenzione. Profili sostanziali*, con la collaborazione di E. Zuffada, II ed., Torino, 2021, 93 ss.

[18] Si veda R. Magi, *Per uno statuto unitario dell'apprezzamento della pericolosità sociale. Le misure di prevenzione a metà del guado?*, in *Diritto Penale Contemporaneo*, 3, 2017.

di mira della prevenzione dallo *status* sociale e politico (oziosi, vagabondi, dissidenti) alla (sospetta) pericolosità ha comportato una gigantesca crescita della platea dei destinatari della prevenzione, peraltro senza che da questo punto di vista possa fare alcuna differenza la competenza questorile o giudiziaria di volta in volta prevista.
Del resto, la cruciale riforma del 2008, grazie alla quale si è reso possibile applicare disgiuntamente misure di prevenzione personali e patrimoniali, aveva solo in teoria tra i propri scopi anche quello di circoscrivere l'utilizzo delle prime (sempre che avesse davvero questo scopo). Lo dimostra la solerzia con la quale il legislatore ha prontamente inventato nuove misure di prevenzione personali, rispetto agli atti persecutori e alla violenza domestica, un legislatore che in ogni caso aveva già introdotto il DASPO in occasione di eventi sportivi, che ad oggi conosce pure la variante del DASPO urbano. Fino ad alcune recenti innovazioni, come l'ammonimento questorile per prevenire e contrastare il *cyberbullismo* (e abbiamo rischiato di avere la sorveglianza speciale anche per gli invasori di terreni per raduni pericolosi…).
Mettiamola in questo modo, senza esasperare alcuna posizione. Se anche fosse vero che non sta scritto da nessuna parte che la prevenzione andrebbe limitata, usarla per le più disparate ipotesi fa solo male alla stessa prevenzione. Anche chi ritiene non debba esplodere, dovrà convenire che così finirà per implodere[19].

6. Il problema del fondamento costituzionale

Esiste anche un altro profilo che restituisce una significativa contraddittorietà. In questo caso il problema è di natura giuridica. Proviamo a riassumerlo. Il punto di partenza non può non essere la Costituzione. Questo non significa che prima non esistevano problemi, al contrario, come dimostrano le posizioni critiche di Francesco Carrara, alle quali si è soliti accostare in posizione più permissiva quelle di Oreste Ranelletti, anche se in certi passaggi cautamente permissiva[20].
La questione è che con la Costituzione davvero cambia tutto, e questo perché il primo problema che non poteva non essere affrontato era costituito dalla compatibilità costituzionale in sé delle misure di prevenzione, delle quali in modo esplicito il testo costituzionale non se ne occupa. In effetti, ieri come oggi, il primo problema rimane questo: le misure di prevenzione, se vogliamo specifichiamo personali, stanno dentro o fuori il perimetro della Costituzione, e se stanno dentro dove cercarne la base giustificatrice? Una avvertenza di cautela è d'obbligo: bisogna far dire alla Costituzione

[19] Si veda R. Bartoli, *Misure di prevenzione: costituzionalmente legittime soltanto per le organizzazioni criminali*, intervista condotta da L. Tombelli, in C. Conti (a cura di), *Criminalità mafiosa: memoria e cultura della legalità. Nel ricordo di Pier Luigi Vigna e Gabriele Chelazzi*, Milano, 2022, 121 ss., secondo il quale le misure di prevenzione possono essere applicate solo alla criminalità organizzata, e questo perché solo qui, una volta che perdura l'organizzazione, si possono ricavare i sospetti di reato dai precedenti, potendosi sganciare la misurazione dell'attualità del pericolo e riferirla alla persistenza o meno di legami con la stessa organizzazione, da accertare in termini reali ed effettivi. Valutare la pericolosità senza l'accertamento di un fatto rischia di girare a vuoto in presenza di reati istantanei e mono-soggettivi.

[20] La più esauriente ricostruzione resta quella di D. Petrini, *La prevenzione inutile. Illegittimità delle misure* praeter delictum, Napoli, 1996, in specie si veda tutto il cap. I dedicato a Carrara e il cap. II al dibattito nella dottrina classica.

quello che non dice in modo esplicito, cosa che si può fare, ma muovendosi appunto con cautela, atteggiamento obbligatorio di fronte al "non normato" costituzionale[21].

Lo scenario contraddittorio che si presenta ai nostri occhi è il seguente, ed è stato come sempre magistralmente evidenziato da Francesco Palazzo[22]. Questa la domanda: ma è mai possibile che, nella ricerca del fondamento costituzionale del sistema della prevenzione, un ruolo di particolare rilievo è stato nel corso del tempo assunto dall'art. 2 Cost., proprio la disposizione che più di altre è in grado di mostrare la consapevole scelta dei nostri costituenti di trovare un pregevole equilibrio tra l'ispirazione liberale e l'ispirazione solidaristica a fondamento dell'intera architettura costituzionale? Se il fondamento costituzionale delle misure di prevenzione è rintracciato nell'art. 2 Cost., cosa ne resta del principio personalista, che si innerva di tutta quella ispirazione liberale-garantistica non certo estranea ai nostri costituenti? Non è forse vero che finisce per assurgere a ruolo tiranno quello della difesa sociale, che pur si può considerare presente nell'istanza solidaristica?

Una vera e propria contraddizione. Plateale, radicale, e questo proprio perché, passi la semplificazione, per richiedere l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale, dentro ai quali si potrebbero pure intravedere le esigenze di prevenzione, si finisce con il sacrificare, in alcuni casi parzialmente, in altri del tutto, quelli che sono i diritti inviolabili della persona, singolarmente considerata e nelle formazioni sociali ove si svolge la sua personalità.

Si potrà anche sostenere che non si realizza alcuno schiacciamento, che non è vero che la difesa sociale finisca con il divorarsi lo sviluppo della personalità dei singoli. Certo, non sempre si arriva a tanto, ma resta che in alcuni casi è esattamente quello che succede (ad esempio, ma solo ad esempio, vietando senza limiti di tempo l'utilizzo di un cellulare), ed appunto trovarne il fondamento costituzionale riferendosi all'art. 2 Cost. è assai contraddittorio.

D'altro canto, il riferimento all'art. 2 Cost. è importante anche sotto un diverso angolo di visuale. Nella ricerca del fondamento costituzionale della prevenzione si è sostenuto che le misure di prevenzione personali applicate dal questore potevano essere disposte proprio dal questore, e non dall'autorità giudiziaria, poiché non andavano ad intaccare diritti e libertà per i quali la Costituzione prevede espressamente, insieme alla riserva di legge, anche la riserva di giurisdizione. Il riferimento correva soprattutto all'art. 16 Cost., ai sensi del quale, per "motivi di sicurezza", è possibile limitare la circolazione e il soggiorno in qualsiasi parte del territorio nazionale, limitazione che può essere disposta in via generale dalla legge, senza alcuna espressa menzione di un obbligatorio e preventivo intervento dell'autorità giudiziaria[23].

---

[21] Si veda A. Ruggeri, *Il "non normato" costituzionale e le sue specie* (2022), ora in Id., *"Itinerari" di una ricerca sul sistema delle fonti. XXVI. Studi dell'anno 2022*, Torino, 2023, 568.

[22] Si veda F. Palazzo, *Per un ripensamento radicale del sistema di prevenzione* ante delictum, in *Criminalia*, 2017, 133 ss.

[23] Si usa il verbo al passato, rispetto al riferimento all'art. 16 Cost., poiché è fuorviante giustificare la competenza questorile dal momento che per limitare la libertà di circolazione e soggiorno è sufficiente la riserva di legge, dichiarandosi soddisfatti dal successivo ed eventuale intervento dell'autorità giudiziaria, la famosa fattispecie a formazione progressiva. Quello che occorre fare è comprendere di volta in volta quale diritto costituzionalmente presidiato finisce con il limitare questo o quest'altro divieto contenuto

Ora, i motivi di sicurezza dei quali discorre l'art. 16 Cost. hanno molto a che fare con la difesa sociale, quanto meno con la pericolosità, possono pertanto ricondurci dentro l'art. 2 Cost., in questo modo facendo riemergere nuovamente la contraddizione. Se ci si "avvicina" all'art. 2 Cost. non è per confermare la sufficienza della sola riserva di legge, semmai per reclamare la necessità anche della riserva di giurisdizione!
Si consideri pure inconsistente il riferimento ai doveri inderogabili di solidarietà, e ci si riferisca all'art. 2 Cost. nella parte in cui assegna alla Repubblica il compito di garantire i diritti inviolabili. Lasciamo anche stare il problema della fattispecie aperta o chiusa. Partiamo dall'assunto che dentro l'art. 2 Cost. esista il fondamento del sistema di prevenzione, proprio perché così la Repubblica garantisce i diritti inviolabili.
Resta che non è questo il modo di ragionare nemmeno della Corte costituzionale, e la sentenza qui in commento è perfettamente coerente con un determinato modo di approcciare la questione, che sembra proprio (non a caso) voler scansare il riferimento all'art. 2 Cost. Si potrà criticare l'approccio da sempre seguito dalla Corte, dalla capostipite e lontanissima sentenza n. 27 del 1959, in base al quale la prevenzione è una esigenza e una regola fondamentale di ogni ordinamento, e come tale pervade la Costituzione, che vuole garantire un ordinato e pacifico svolgimento dei rapporti tra i cittadini[24]. Non di meno, una cosa è sostenere l'immanenza della prevenzione in ogni ordinamento, altra è dire che trova fondamento nel principio personalistico-solidaristico. Non possiamo in definitiva disgiungere l'art. 2 Cost., riconoscere e garantire i diritti formano una endiadi unitaria. E se non è possibile che si disgiunga, allora non aggiunge granché rafforzare il riferimento alle misure di sicurezza contenuto nell'art. 16 Cost. richiamandosi all'art. 2 Cost., il quale ad essere precisi non pare proprio dica che per limitare un determinato diritto sia sufficiente la sola riserva di legge.

7. Misure di prevenzione e misure di sicurezza

Un'ultima osservazione per quanto riguarda il fondamento costituzionale del sistema della prevenzione. Constatate le difficoltà di riferirsi all'art. 2 Cost., e preso atto che il riferimento all'art. 16 Cost. era comunque pur sempre esperibile se limitato ad una delle diverse libertà costituzionalmente presidiate, si è esplorato un diverso tentativo ricostruttivo, rivolto all'art. 25 Cost., il cui c. 3 espressamente si riferisce alle misure di sicurezza, prevedendo unicamente la garanzia della riserva di legge, non anche di giurisdizione.
Questo tentativo ha dalla sua un punto di appoggio più stabile, meno sfuggente, rispetto al riferimento all'art. 2 Cost.: bastava estrapolare la pericolosità a base delle misure di sicurezza ed estenderla a base delle misure di prevenzione e il gioco era fatto. Una

nell'avviso orale rinforzato, per restare alla nostra misura personale. Si potrà anche sostenere che non sempre è necessaria la riserva di giurisdizione, ma ancora una volta questo per caso significa che allora si può prevedere qualsiasi cosa in una legge? Discutere di prevenzione significa discutere pertanto di limiti, anche fuori dalle garanzie della riserva di legge e di giurisdizione, ad esempio di limiti legati alla ragionevolezza e alla proporzionalità.

[24] Si veda M. Ruotolo, *Art. 13*, in R. Bifulco - A. Celotto - M. Olivetti (a cura di), *Commentario alla Costituzione*, cit., 321 ss.

accertata, l'altra supposta, ma sempre di sicurezza si tratta, anche se nel secondo caso sotto forma di prevenzione.

In entrambi i casi, questa la tesi, il legislatore era legittimato dalla Costituzione ad intervenire, e questo proprio perché ciò che contava era la pericolosità della persona, da considerare tanto prima quanto dopo la commissione di un reato. Un concetto onnivoro quello della pericolosità, che si associa al "concetto-sfinge" della difesa sociale[25], ma che riusciva a giustificare l'intervento statale prima e dopo il delitto. La prevenzione e la sicurezza hanno scopi differenti, ma ciò che conta è la possibilità per il legislatore di intervenire a fronte della pericolosità della persona.

Va da sé che anche in questo caso una qualche contraddizione è innegabile, non fosse altro per il fatto che la Costituzione si riferisce alle sole misure di sicurezza, non a quelle di prevenzione, peraltro ben conosciute ai nostri costituenti. Non è mai consigliabile far dire al testo quello che il testo non dice, ma se il testo è la Costituzione non può essere negata cittadinanza a concetti che si riescono a ricavare in via di interpretazione sistematica. Fermo restando che così facendo si dovrebbero anche valutare le conseguenze sul *favor libertatis*, il modo antico per giustificare la più recente massima estensione dei diritti.

Ad ogni modo, questa sorta di fusione tra misure di sicurezza e misure di prevenzione si è prodotta anche a livello di legislazione ordinaria. Ed è proprio il caso di specie oggetto di questo commento a dimostrarlo. Non vi è dubbio che l'avviso orale costituisca una misura di prevenzione (personale), ma quando assume la veste rinforzata è perché le prescrizioni che si possono imporre e che il preposto è tenuto a rispettare, pena la commissione di un reato, possono essere disposte solo nei confronti di persone definitivamente condannate per delitti non colposi. Quali siano questi delitti nessuno lo può sapere in anticipo, così come nessuno può sapere quanto e se conterà il tempo trascorso dalla condanna definitiva, non di meno le condanne (definitive) esistono e quindi si può vietare il possesso e l'utilizzo del cellulare per evitare altri reati a chi potrebbe commetterne di nuovi. Questa è la prevenzione travestita da sicurezza. Il mescolamento è palese[26].

Trova copertura nel c. 3 dell'art. 25 Cost. un siffatto sistema di prevenzione mescolato con un sistema di sicurezza? Una domanda non semplice, sulla quale la Consulta nella sentenza qui in commento non prende posizione, accontentandosi di affermare che «le esigenze di prevenzione e di difesa sociale ben possono giustificare (…) misure restrittive, e queste possono incidere anche sui diritti fondamentali». La Corte poteva non dire alcunché rispetto all'art. 25, c. 3, Cost., non essendo stato invocato come parametro dalle ordinanze di rimessione. Ciononostante, quello appena riportato è l'unico passaggio motivazionale esplicito grazie al quale la Corte "fonda" la legittimità costituzionale delle misure di prevenzione, il che è forse sintomo di un qualche disagio. Non si richiama l'art. 2 Cost., troppo alto il rischio di pervenire ad esiti contraddittori,

[25] Così F. Bricola, *Forme di tutela "*ante-delictum*" e profili costituzionale della prevenzione* (1975), ora in Id., *Politica criminale e scienza del diritto penale*, Bologna, 1997, 35.

[26] Dire che la sicurezza ha un campo più ampio di intervento della prevenzione è dire cosa vera, riferendosi alle ipotesi previste dal legislatore. Ma dirlo significa accedere alla prima contenitore anche della seconda, non solo della seconda, ma anche della seconda.

ma nemmeno ci si riferisce all'art. 25, c. 3, Cost., e questo forse perché si avverte un qualche disagio o, ulteriore ipotesi, perché la prevenzione è immanente nel sistema, quasi a dire che la prevenzione è comunque giustificata, indipendentemente da questo o quest'altro articolo costituzionale al quale ci si vuole riferire.

In altri termini, è come se la Corte sviasse il problema del fondamento costituzionale delle misure di prevenzione, quanto meno in termini di riferimento testuale, per occuparsi in modo spedito della impossibilità di limitare nello specifico la libertà di comunicazione, se non per atto motivato dell'autorità giudiziaria, salva la riserva di legge.

Questa è un'altra possibile interpretazione, la quale però non riesce a mascherare quella che potrebbe essere ancora una diversa prospettiva di interpretazione: non è che la Corte, incardinando tutto il suo ragionamento dentro l'art. 15 Cost., è anche riuscita a non prendere posizione sulla riserva di legge in sé, almeno in termini di garanzia della prevedibilità/proporzionalità della misura, questione che pure era stata espressamente sollevata e che la Corte ha ritenuto assorbita? Non è che la Corte, nel caso in cui si fosse riferita anche alla qualità della legge, intesa in termini di prevedibilità, avrebbe dovuto prendere una qualche posizione in riferimento all'eventuale collocamento delle misure di prevenzione dentro le misure di sicurezza, visto che il c. 3 dell'art. 25 Cost. prevede espressamente solo (appunto) la riserva di legge[27]?

Quelle esposte sono unicamente delle domande, questioni sulle quali riflettere, ma che per l'ennesima volta riconsegnano uno scenario contraddittorio: pochi rimpiangeranno il potere del questore di vietare l'uso del cellulare, non di meno siamo proprio sicuri che quello che non poteva fare il questore ora lo possa fare tranquillamente l'autorità giudiziaria, vale a dire disporre il divieto senza alcuna prestabilita fissazione della sua durata, nel minimo e nel massimo? Una contraddizione: si sposta la competenza dal questore all'autorità giudiziaria, e questo va bene, ma l'oggetto della competenza in discussione rimane del tutto illeso, come se bastasse il giudice a rendere costituzionalmente legittima una misura in sé applicata senza garanzie di prevedibilità, meno che mai di proporzionalità. Leopoldo Elia ci mise in allerta quando, prendendo posizione in tema di misure di prevenzione, discusse del «mito della giurisdizionalità», di «virtù taumaturgiche» dell'intervento giurisdizionale, del «fascino del principio di giurisdizionalità»[28].

Meglio oggi rispetto a ieri, va ripetuto. Ma sembra proprio che "morto il Re, viva il Re", se riguardiamo la questione nell'ottica della prevedibilità e proporzionalità. Nel prosie-

[27] Anche perché nella altalenante giurisprudenza costituzionale sul riferimento testuale dal quale derivare le legittimità della prevenzione è comunque capitato un qualche deciso riferimento al c. 3 dell'art. 25 Cost., dal momento in cui misure di prevenzione e di sicurezza appartengono a «due *species* di un unico *genus*…ferme restando le differenze di struttura, settore di competenza e modalità applicative»: sentenza n. 291 del 2013, che introduce l'obbligo di rivedibilità *ex officio* della pericolosità nel caso di una misura di prevenzione rimasta sospesa per la detenzione della persona). Da ultimo, sulla giurisprudenza costituzionale si vedano G.P. Dolso, *Le misure di prevenzione personali nell'ordinamento costituzionale*, in F. Fiorentin (a cura di), *Misure di prevenzione personali e patrimoniali*, Torino, 2018, 41 ss. e E. Zuffada, *La prevenzione* ante delictum*: alla ricerca di un fondamento costituzionale*, in *Criminalia*, 2020, 253 ss.

[28] Senza determinatezza legislativa, aggiungeva, la giurisdizionalità si trasforma in mito, «anzi in una *species* appartenente alla più ampia categoria del mito della imparzialità»: si veda L. Elia, *Libertà personale e misure di prevenzione* (1962), ora in Id., *Studi di diritto costituzionale (1958-1966)*, introduzione di G. Zagrebelsky, Milano, 2005, 475.

guo vedremo se, in assenza di un intervento del legislatore, il giudice, dopo la sentenza della Corte, può davvero vietare il cellulare entro l'avviso orale rinforzato disposto dal questore. Qui si vuole dire un'altra cosa, evidenziare che il problema forse sta addirittura più in alto, al cuore classico e tradizionale della legalità: una legge può attribuire ad un giudice un potere sconfinato, cosa ne rimane della soggezione del giudice alla legge, nel momento in cui il giudice può decidere quello che vuole rispetto alla durata di un determinato divieto, non di poco momento, come è quello di non poter utilizzare, oggi, un cellulare? Siamo dentro la costituzionalmente ammessa discrezionalità del giudice, oppure siamo più vicini ad un vero e proprio arbitrio, visto che non esiste alcun perimetro entro il quale il giudice è chiamato a decidere? Arbitrio è un termine impegnativo, ma qui lo si utilizza in un preciso significato, vale a dire riferito ad una scelta non perimetrata, senza cornice[29].

Forse questo è il destino più generale del sistema della prevenzione. Lo si giurisdizionalizza e certo non si manca di tassativizzarlo, ma a tutto esiste un limite, che non è tanto la razionalizzazione constatativa e prognostica (l'inquadramento in una delle fattispecie di pericolosità, generica o qualificata, e la attuale pericolosità per la sicurezza pubblica), quanto la possibilità di attribuire un potere ad un organo che non potrebbe proprio avere, vale a dire quello di limitare un diritto garantito dalla Costituzione senza alcuna preventiva conoscibilità da parte dell'interessato di quanto durerà nel tempo siffatta limitazione[30].

Non molto differente da quanto accaduto in tema di pena perpetua. Da parte di molti si è sostenuta la incostituzionalità dell'ergastolo ostativo, e va bene. Alla fine anche la Consulta è stata di questa opinione. Ma ci si dovrebbe oggi accorgere che il prezzo pa-

[29] Questo è il termine impiegato anche da Leopoldo Elia, quando sosteneva che non poteva la giurisdizionalità surrogare o compensare l'attenuazione della legalità, intesa soprattutto come determinatezza. Ad ogni modo, il ragionamento era (ed è) impeccabile, e lo si può riferire anche alla prevedibilità-proporzionalità: «non si può parlare di vera giurisdizionalità laddove non si realizza in pieno il principio di legalità. Altrimenti si riesce piuttosto a dislocare la sede dell'arbitrio, che a creare nuovi strumenti di garanzie per i cittadini» (L. Elia, *Libertà personale e misure di prevenzione*, cit., 497). Arbitrario era il potere del questore, arbitrario è il potere del giudice, nel momento in cui la legge permette di applicare un divieto senza alcun limite prestabilito di durata. Peraltro, analizzando il passato, e proprio in riferimento all'ammonizione, antesignana dell'avviso orale, anche Giuliano Amato ha utilizzato il termine arbitrio. Il riferimento correva al sistema preventivo messo in piedi con il TUPS del 1865, il primo del Regno d'Italia. Una volta che l'individuo rientrava in una delle tre categorie di sospetti suscettibili di ammonizione, il pretore era il *dominus* di tutta la procedura: «nel complesso perciò dominava l'arbitraria segretezza dell'inquisizione dei tempi passati», giustificata richiamandosi all'indole amministrativa del procedimento, e pertanto si confermano i «limiti del nostro rinnovamento liberale, che purificò il processo dall'arbitrio ma, anziché eliminarlo, lo ribattezzò agilità amministrativa» (si veda G. Amato, *Individuo e autorità nella disciplina della libertà personale* (1968), Milano, 1976 (ristampa inalterata), 232).

[30] Un ultimo appunto sul fondamento costituzionale della prevenzione. Sinceramente, il riferimento alla rieducazione è sempre apparso alquanto discutibile. Ma non tanto perché oramai alcune misure di sicurezza non hanno nulla a che fare con la rieducazione (e quindi cade la possibilità di associare sicurezza e prevenzione), quanto perché di concretamente rieducativo il sistema preventivo ha pochissimo, anzi nulla. Una volta si sosteneva che spingeva le persone a commettere reati, e questo oggi non è scomparso, ma resta che, vista con gli occhi di chi incappa nelle maglie del sistema preventivo, realmente la rieducazione è solo un riferimento astratto, teorico, illusorio e beffardo. Si veda quanto riportato in A. Barbano, *L'inganno. Antimafia. Usi e soprusi dei professionisti del bene*, Venezia, 2022 e P. Cavallotti - L. Ceva Valla - M. Romeo (a cura di), *Quando prevenire è peggio che punire. Torti e tormenti dell'inquisizione antimafia*, prefazione di S. D'Elia, Bologna, 2022.

gato è stata la granitica conferma dell'ergastolo in sé. In molti dicevano che il problema non era l'ergastolo, ma l'ergastolo ostativo. Anzi, il secondo era un problema proprio perché il primo non lo era. Speculare accade rispetto alla misura di prevenzione personale qui in discussione. Una delle prescrizioni che prima poteva imporre il questore oggi la può disporre unicamente l'autorità giudiziaria, rimanendo in capo al questore in ipotesi la sola possibilità di proposta. Ma questo non significa una granitica conferma della prescrizione in sé, indipendentemente dalla esistenza di una calibrazione temporale rispetto alla durata?
E se proprio la si vuole dire tutta: così come continua ad essere problematica la possibilità per il giudice della cognizione di pronunciare condanna ad una pena che ha come fine pena il "mai", non dovrebbe apparire problematica allo stesso modo la possibilità per il giudice della prevenzione di prescrivere un divieto senza alcuna durata? La duplice domanda può essere riassunta in una, di straordinaria importanza: se il costituzionalismo è prima di tutto limite al potere, ad ogni tipo di potere, punitivo e preventivo non fa differenza, possiamo ritenerci soddisfatti ogni qual volta osserviamo l'esistenza di un potere che punisce o previene senza alcuna limitazione temporale? Consideriamo anche immanente nel sistema il potere preventivo, ma non dovrebbe essere in ogni caso esercitabile dando la possibilità ai destinatari delle prescrizioni imposte di prevederne la durata, di comprenderne la proporzionalità?

8. La riserva di legge in termini di prevedibilità e di proporzionalità

Vediamo a questo punto qualche ulteriore riflessione a proposito delle argomentazioni della Consulta. In primo luogo, la Corte svolge subito in apertura qualche puntualizzazione per meglio delimitare l'oggetto del sindacato, vale a dire unicamente la possibilità per il questore di vietare in tutto o in parte il possesso o l'utilizzo del cellulare nei confronti del destinatario di un avviso orale rinforzato. Il "piccolo" problema poteva scaturire dal fatto che l'ordinanza della Cassazione, nel dispositivo, censurava l'intero pacchetto di divieti che può disporre il questore, ma la Corte chiarisce che, in realtà, la motivazione dell'ordinanza non lascia alcun dubbio a proposito, e quindi l'oggetto del giudizio costituzionale è solo il divieto riguardante il cellulare, non gli altri. E aggiunge, sempre la Corte: il presupposto «del tutto corretto» dal quale partono entrambe le ordinanze è che il questore possa vietare anche solo uno o alcuni degli oggetti vietabili. Non vi è dubbio che sia così, il questore può decidere di vietare un solo oggetto, più oggetti o anche tutti gli oggetti, quello che fa la differenza è la motivazione riguardante il nesso tra il divieto o i divieti e la pericolosità.
A tale proposito vale la pena aggiungere uno spunto. Ad oggi, nessuno è a conoscenza di come nel corso del tempo i diversi questori hanno deciso di intervenire. Si tratta di una ricerca non ancora portata a compimento, sempre sia possibile compierla, visto che le questure dovrebbero dare la possibilità di analizzare, per motivi di ricerca e di studio, gli avvisi orali rinforzati. Al massimo, ci si può riferire ad alcune pronunce nelle quali i giudici di legittimità hanno annullato con rinvio ordinanze di rigetto della

opposizione avverso un avviso orale rinforzato, il quale applicava in modo congiunto tutti i divieti applicabili. Un esempio, l'ordinanza n. 13765 del 25 febbraio 2020 della I sezione penale della Cassazione: il giudice doveva esprimersi sul divieto di possedere o utilizzare «mezzi di trasporto modificati al fine di aumentare la potenza o la capacità offensiva», applicato dal questore *congiuntamente* a tutti gli altri divieti. Nel caso di specie – che, ripetiamo, non sappiamo se è più o meno frequente nella prassi, in termini di indistinta applicazione di tutti i divieti – prima il questore e dopo il giudice avevano ragionato come si fa con la pesca a strascico, applicando tutti i divieti, e nello specifico non avevano considerato che il ricorrente lavorava presso un'impresa di autosoccorso, che utilizzava mezzi di trasporto appositamente modificati![31].

Come che sia, e dopo aver esaminato il diritto vivente rispetto alla inclusione dei cellulari dentro gli apparati di comunicazione radiotrasmittente ed aver ricostruito il senso complessivo dell'art. 15 Cost.[32], la Corte ritiene che la inviolabilità della libertà di comunicazione significa che il suo contenuto essenziale può subire restrizioni solo quando necessarie alla tutela di un interesse pubblico costituzionalmente rilevante, nel rispetto della riserva assoluta di legge e della riserva di giurisdizione.

In cosa consiste questo interesse pubblico costituzionalmente rilevante? Ecco il passaggio della Corte, già richiamato in precedenza: «Le esigenze di prevenzione e difesa sociale ben possono giustificare, si è detto, misure restrittive, e queste possono incidere anche sui diritti fondamentali».

Non una parola in più. Se si cercasse nella pronuncia della Corte il fondamento costituzionale della prevenzione quello che si troverebbe sarebbe solo questa frase. Certo, si tratta di un assunto che la Corte fa proprio basandosi sulla sua precedente giurisprudenza. Nulla di nuovo. Ma è sufficiente? L'impressione è che la Corte intenda tagliar corto sulla faccenda per giungere velocemente alla (giusta) dichiarazione di incostituzionalità. Il punto è però che in questo modo qualcosa non torna.

Nel momento in cui le esigenze di prevenzione e di difesa sociale giustificano misure restrittive (*rectius* preventive), che possono incidere sui diritti fondamentali, siamo sicuri sia sufficiente la loro giurisdizionalizzazione? E torniamo al problema della assenza di una durata prestabilita dei divieti imposti con l'avviso orale rinforzato. Sicuramente, la Corte esclude in modo molto chiaro la possibilità che il successivo intervento del giudice possa emendare il suo mancato intervento preventivo. La famosa "fattispecie a formazione progressiva" non è quindi sufficiente, il giudice deve intervenire all'atto di limitare il diritto, non (eventualmente) dopo quando il diritto è stato limitato.

Il problema è però che se si rimuove il potere del questore e lo si sostituisce con quello del giudice non si capisce bene come possano stare insieme la riserva (assoluta) di legge e la riserva di giurisdizione. Il giudice assicura il contraddittorio e il diritto di di-

[31] L'auspicata ricerca sulla prassi seguita dai questori in merito all'imposizione nell'avviso orale rinforzato di uno, di più o di tutti i divieti non avrebbe affatto una valenza meramente storico-ricostruttiva. Ad oggi, solo il divieto riguardante il cellulare è stato spostato alla competenza dell'autorità giudiziaria. Una meritevole ricerca sulla prassi delle misure di prevenzione, circoscritta alla prassi milanese, è quella di E. Mariani, *Le misure di prevenzione personale nella prassi milanese*, in *Diritto Penale Contemporaneo*, 10, 2018, entro la quale però, rispetto alle misure personali, non si affronta il tema dei divieti imposti con l'avviso orale rinforzato, immaginiamo per la impossibilità di poter disporre direttamente degli avvisi.

[32] Si vedano i paragrafi precedenti di Marco Orofino.

fesa, questo è certo. Ma in che modo si può valutare un divieto che nasce senza alcuna durata prestabilita, se non come carente di prevedibilità e di proporzione? A queste domande la Corte non risponde, visto che assorbe il dubbio di costituzionalità riferito a siffatto problema, e si limita a dire che «la decisione (di vietare il possesso o l'utilizzo del cellulare, *ndr*) non può che essere dell'autorità giudiziaria, con le procedure, le modalità e i tempi che compete al legislatore prevedere, nel rispetto della riserva di legge prevista dalla Costituzione».

Certo, la Corte chiama in causa un futuro intervento del legislatore, ma a conti fatti lascia in piedi, fino a quando il legislatore deciderà di intervenire, un sistema che non appare affatto rassicurante, essendo ad oggi solo due le alternative immaginabili: o nessuno potrà vietare, dentro un avviso orale, il possesso o l'utilizzo di un cellulare, considerata l'assenza di un qualsiasi modello legale di riferimento, oppure, se lo può fare il giudice, il suo margine di azione appare sconfinato, riferendosi alla possibilità di vietare il cellulare senza alcuna durata prestabilita, nel minimo e nel massimo[33].

Proprio su questo problema serve qualche ulteriore considerazione. Che il problema esista pare fuori discussione. Non sarebbe corretto sostenere che la Corte ha deciso per l'assorbimento perché in qualche modo ora l'autorità giudiziaria sarà in grado di riferirsi ad una disposizione legislativa utile, al fine di porre una durata minima e massima del divieto di possedere o utilizzare in tutto o in parte il cellulare. Non è così, la Corte assorbe e basta, limitandosi a dire che spetta al legislatore prevedere le procedure, le modalità e i tempi dell'intervento dell'autorità giudiziaria.

Il punto è che l'assorbimento deciso dalla Corte appare troppo *tranchant*. Non dice in alcun modo quello che moltissime altre volte ha detto, ossia che il problema esiste ma non può essere il giudice costituzionale ad intervenire, pena violazione della discrezionalità del legislatore. Ben vero che i moniti della Consulta spesso restano inascoltati, non di meno una cosa è evidenziare il problema e poi tirare il freno a mano, altra è assorbire senza spendere alcuna parola sopra una questione di indiscutibile delicatezza.

Si dirà: lasciando in disparte il non potersi sostituire al legislatore (che, ribadiamo, non viene affermato), la Corte ha deciso di assorbire perché non poteva fare altrimenti. Non poteva riferirsi alla durata della sorveglianza speciale, che è misura diversa rispetto all'avviso orale. Non poteva richiamare la precedente durata nel massimo di tre anni dello stesso avviso orale, poiché tutto dipendeva dal fatto che era il presupposto della sorveglianza speciale, che poteva essere disposta al massimo entro tre anni dall'applicazione dello stesso avviso orale[34]. E non poteva certo dire che il divieto di

[33] Si deve ragionare in attesa di un intervento del legislatore, e quindi su quelli che sono gli effetti immediati nel breve periodo della decisione della Corte. Ebbene, o il cellulare si vieta in riferimento però alla sorveglianza speciale (ove esistono limiti minimi e massimi di durata), oppure il questore dentro l'avviso orale rinforzato dovrà chiedere al giudice (collegiale?) di applicare anche il divieto riguardante il cellulare. Ma, in questo secondo caso, senza alcuna possibilità di riferirsi ad alcuna previsione legislativa utilizzabile per limitare nel minimo e nel massimo la durata del divieto. Ripetiamo: in assenza di un intervento del legislatore, questo è lo scenario che consegue all'assorbimento deciso dalla Corte, uno scenario non rassicurante, che forse richiederà di tornare nuovamente alla Consulta.

[34] La storia (recente) dell'avviso orale è certo singolare. Da un lato, diviene autonoma misura di prevenzione personale solo con il codice antimafia, poiché in precedenza era il presupposto per la sorveglianza speciale di pubblica sicurezza disposta nei confronti delle persone inquadrate in una delle fattispecie di pericolosità generica, persone che, nonostante l'avviso, non avevano cambiato condotta.

utilizzare il cellulare non intaccava alcuna libertà costituzionalmente presidiata, e che di conseguenza si poteva non prevedere alcuna prestabilita durata minima e massima. Ancora: non poteva dire che sarà il giudice, caso per caso, a decidere la durata minima e massima del divieto, e questo perché avrebbe significato un implicito accostamento tra potestà punitiva e potestà preventiva. Pochi nutrirebbero dubbi sulla possibilità per il legislatore di prevedere una pena senza alcuna durata prestabilita, nel minimo e nel massimo. Sarebbe una pena sicuramente incostituzionale, sproporzionata per definizione. Ma, appunto, la prevenzione è un'altra cosa, non entrano in gioco direttamente la responsabilità penale, la colpevolezza, la rieducazione.

E però, si potrebbe controbattere: tutto vero, ma il principio di eguaglianza, che genera la proporzionalità, vale sempre, anche nel campo della prevenzione e, del resto, questo era il parere dell'ordinanza di rimessione della Cassazione. D'altro canto: possibile che possa durare per tutta la vita del destinatario un divieto contenuto in un avviso orale, proprio quella che di solito è definita come la più blanda tra le misure di prevenzione personali[35]?

Le Corte, rifacendosi al principio di eguaglianza/proporzione, poteva/doveva valutare la questione della mancanza di una durata prestabilita del divieto. Un divieto è ingiusto quando si applica senza durata prestabilita: se è la legge, anche dopo un intervento della Consulta, a permettere ad un giudice di operare in questo modo, la legge è incostituzionale.

Non si potevano rinvenire agganci ad altre disposizioni legislative presenti nell'ordinamento? La Corte aveva le mani legate? Sta tutto qui il senso dell'assorbimento? La verità è che il motivo dell'assorbimento non lo sapremo mai, la Corte non lo spiega in modo esplicito, limitandosi come detto ad affermare che compete al legislatore stabilire procedure, modalità e tempi dell'intervento dell'autorità giudiziaria.

Si badi però che in realtà l'assorbimento non dipende affatto dalla impossibilità per la Corte di invadere il campo spettante al legislatore, visto che in modo esplicito si dice solo che «la rimozione del potere di decisione spettante al questore, infine, comporta l'assorbimento delle ulteriori questioni di legittimità costituzionale sollevate», tra le quali appunto quella relativa alla possibilità di porre il divieto senza un limite minimo e massimo di durata.

L'assorbimento utilizzato del resto non pare essere figlio di scelte legate ad una qualche economia processuale. E non pare proprio potersi discutere di implicazione né logica né consequenziale tra motivo assorbente e motivo assorbito, visto che l'assenza di durata prestabilita del divieto esisteva prima quando lo poteva imporre il questore

Soprattutto, dall'altro lato, prima del codice antimafia, l'avviso orale aveva durata massima di tre anni, in quanto il questore non poteva più disporre la sorveglianza speciale una volta spirati tre anni dall'avviso orale

[35] Questa la domanda che si pone E. Zuffada, *I divieti connessi alla misura questorile dell'avviso orale al vaglio della Corte costituzionale: verso una nuova censura del sistema* ante delictum*?*, in *Sistema Penale*, 3 febbraio 2022, 11, il quale sostiene la necessità di limitare temporalmente non solo tutti i divieti applicabili, ma direttamente lo stesso avviso orale. Ad ogni modo, nella già richiamata sentenza n. 28551/2020 della I sezione penale della Cassazione, il caso di specie era alquanto significativo. Non sappiamo se è la normalità o l'eccezione, in ogni caso l'avviso orale era stato emesso dal questore il 28 aprile 2014, notificato il 19 novembre 2014 ed era stato assunto violato in data 29 ottobre 2018, quindi a distanza di cinque anni.

ed esiste ora che lo può disporre solo l'autorità giudiziaria. Assorbire come ha fatto la Corte non significa solo non pronunciarsi sul chiesto, ma significa anche lasciare in piedi un sistema che non accontenta nessuno: ci sarà il contraddittorio, ci sarà la difesa, ci sarà ora tutto quello che prima non poteva esserci, non di meno ci sarà un giudice che avrà le mani libere, potrà fare scelte (sulla durata del divieto) da nessuno prevedibili. Dicendo questo non si vuole "attrarre" il sistema preventivo dentro il sistema penale, si vuole unicamente comprendere se il primo in sé sta dentro o fuori il sistema costituzionale, dove l'eguaglianza vale sempre, la riserva (assoluta) di legge deve significare anche prevedibilità e la soggezione del giudice alla legge significa accettazione della discrezionalità e rifiuto dell'arbitrio[36].

In definitiva. Prima che il Parlamento intervenga, il sistema che fuoriesce dalla pronuncia della Consulta è il seguente. Il questore decide l'avviso orale e se del caso anche di imporre una o più restrizioni, tranne quella di vietare il possesso e l'utilizzo in tutto o in parte del cellulare. Per questa sarà l'autorità giudiziaria a decidere, e ad oggi non è nemmeno chiaro se il questore può fare una qualche proposta (si dovrebbe estendere in via analogica la possibilità prevista per la sorveglianza speciale). Il risultato è quindi questo: un avviso orale rinforzato deciso dal questore, che potrebbe contenere un divieto prescritto dal giudice. Un avviso orale rinforzato dal duplice volto, uno questorile e uno giurisdizionale. Ovviamente, il legislatore resta libero di intervenire come meglio ritiene e quindi, ragionando in astratto, può stabilire limiti di durata riguardanti tanto i divieti posti dal questore quanto il divieto prescritto dal giudice. Fino a questo (auspicabile) intervento, rimane in vita una irragionevole possibilità di vietare il cellulare, senza indicare alcuna durata minima e massima. Il che significa la possibilità di limitare la libertà di comunicazione in modo del tutto arbitrario. Per ovviare a questo, senza un intervento del legislatore, non resta che tornare alla Consulta.

9. Osservazioni conclusive

Qualche breve osservazione conclusiva appare necessaria. Da un lato, la sentenza della Corte qui analizzata non può che essere accolta con grande soddisfazione, in quanto realizza insieme due obbiettivi che in pochi potrebbero ritenere di scarsa rilevanza. Rafforza nel suo complesso la tutela costituzionale della libertà e della segretezza della comunicazione, in modo particolare le capitali garanzie rappresentate dalla riserva (assoluta) di legge e dalla riserva di giurisdizione. E lo fa intervenendo in materia di misure di prevenzione personali applicate dal questore, riferendosi all'avviso orale rinforzato e ad un divieto che questo può contenere, quello di possedere e utilizzare il cellulare, davvero oggi uno strumento senza il quale si corre il rischio di essere in qualche modo esclusi dal tessuto sociale, che poi significa mettere a repentaglio lo svolgimento della personalità sia come singolo sia nelle formazioni sociali.

Dall'altro lato, la decisione della Corte apre una serie di interrogativi di rilevante signi-

[36] Si vedano le osservazioni di Leopoldo Elia in precedenza riportate. Parole dure sono anche quelle che Francesco Palazzo ha scagliato contro il sistema di prevenzione italiano, da ultimo in F. Palazzo - F. Viganò, *Diritto penale. Una conversazione*, Bologna, 2018, 42 ss.

ficato, alla cui risoluzione non può che essere preposto in prima battuta il legislatore, tanto per quanto attiene all'intervento su «ogni altra forma di comunicazione» (diversa dal cellulare), quanto per quello che attiene alla garanzia dei principi di proporzionalità e di prevedibilità del limite ora imponibile dell'autorità giudiziaria. Sono questi interventi che il legislatore non può rimandare. A differenza di altri casi, non appare semplice intravedere un qualche "chiarimento" che potrebbe offrire i giudici comuni. Chiaro pertanto che se il legislatore tarderà, non sembra implausibile ipotizzare una nuova chiamata in causa della Corte costituzionale, uno scenario del resto non infrequente in tema di misure di prevenzione, anche rimanendo a quelle personali[37].

[37] Il riferimento obbligato è al seguito della sentenza n. 24 del 2019. Non appare possibile operare in termini di tassatività, a fronte di una disposizione che la stessa Corte giudica «affetta da radicale imprecisione» (cons. dir., § 12.3). Peraltro, la Corte giunge a questo esito proprio sostenendo che la tassativizzazione è invece riuscita sul «vivere abitualmente, anche in parte, con i proventi di attività delittuose». Pertanto, l'incostituzionalità dell'«essere abitualmente dediti a traffici delittuosi» non potrà che estendersi anche all'avviso orale e al foglio di via, una volta che saranno sollevate le rispettive questioni di costituzionalità.

Algoritmo, provvedimento amministrativo e autotutela

Armando Lorusso

Tribunale Amministrativo Regionale della Campania – Napoli, sez. III, 14 novembre 2022, n. 7003

Il ricorso all'algoritmo, in funzione integrativa e servente della decisione umana, ovvero anche in funzione parzialmente decisionale, non può mai comportare un abbassamento del livello delle tutele garantite dalla legge sul procedimento amministrativo, ed in particolare di quelle inerenti alla individuazione del responsabile del procedimento, all'obbligo di motivazione e alla partecipazione al procedimento amministrativo. In caso di decisione fondata su algoritmo si richiede, pertanto, che sia assicurata una declinazione rafforzata del principio di trasparenza, intesa come piena conoscibilità e comprensibilità della regola espressa in un linguaggio differente da quello giuridico, nonché di c.d. non esclusività della decisione algoritmica.

Sommario

1. Premessa. – 2. La vicenda giudiziaria e la decisione del giudice amministrativo. – 3. Quadro normativo e statuto pretorio del provvedimento algoritmico. – 4. L'algoritmo tra natura giuridica, provvedimento amministrativo e autotutela decisoria. – 5. Considerazioni di sintesi.

Keywords

Algoritmo – natura giuridica – provvedimento amministrativo – autotutela decisoria.

1. Premessa

La decisione in commento si pone nel solco di una ormai copiosa giurisprudenza amministrativa[1] che, negli ultimi anni, ha contribuito a delineare uno statuto della decisione amministrativa algoritmica, attraverso il richiamo a principi generali[2] che do-

[1] Cfr., sul punto, Cons. Stato, sez. VI, 8 aprile 2019, n. 2270; Cons. Stato, sez. VI, 13 dicembre 2019, nn. 8472 – 8473 – 8474, relativamente all'algoritmo impiegato dal MIUR per l'assegnazione del personale docente delle scuole secondarie di secondo grado; nonché, Cons. Stato, sez. VI, 4 febbraio 2020, n. 881; Cons. Stato, sez. III, 25 novembre 2021, n. 7891. Più di recente cfr. Cons. Stato, sez. VI, 8 settembre 2022, n. 6236.

[2] In generale sul principio di legalità e sugli altri principi che sovrintendono all'esercizio della funzione amministrativa cfr. V. Caputi Jambrenghi-A. Angiuli, *Forma e sostanza del principio di legalità nell'esercizio di pubblici poteri*, in *Giustamm.it*, 2013, 1 ss.; nonché, più di recente, A. Angiuli-V. Caputi Jambrenghi, *Deprocedimentalizzazione dell'azione amministrativa e conferenza di servizi*, in Aa.Vv., *L'amministrazione nell'assetto*

vrebbero operare inderogabilmente nei
procedimenti svolti attraverso sistemi algoritmici[3] o, in epoca più recente, sistemi di intelligenza artificiale[4].

La riflessione seguente non intende ripercorrere compiutamente l'evoluzione giurisprudenziale sul punto dal momento che la dottrina si è dedicata a tale analisi anche con contributi di carattere monografico[5], ma si propone di individuare alcuni profili

costituzionale dei poteri pubblici. Scritti per Vincenzo Cerulli Irelli, I, Torino, 2021, 275 ss.

[3] In particolare, sull'impiego degli algoritmi nei processi decisionali delle Amministrazioni, resta ineludibile il riferimento al pionieristico studio di A. Masucci, *L'atto amministrativo informatico*, Napoli, 1993. In generale sull'impatto delle nuove tecnologie sull'azione e sull'organizzazione amministrativa cfr., almeno, D. Marongiu, *L'attività amministrativa automatizzata*, Rimini, 2005; F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in *Il diritto dell'informazione e dell'informatica*, 2, 2015, 227 ss.; S. Civitarese Matteucci-L. Torchia, *La tecnificazione dell'amministrazione*, in S. Civitarese Matteucci-L. Torchia (a cura di), *La tecnificazione*, Firenze, 2016, 10 ss.; F. Costantino, *L'uso della telematica nella pubblica amministrazione*, in A. Romano (a cura di), *L'azione amministrativa*, Torino, 2016, 242 ss.; B. Marchetti, *Amministrazione digitale*, in *Enciclopedia del diritto. I tematici*, *Funzioni amministrative*, Milano, 2022, 75 ss.; L. Torchia, *Lo Stato digitale*, Bologna, 2023. Con specifico riguardo all'uso di algoritmi e intelligenza artificiale nell'assunzione delle decisioni amministrative cfr. P. Otranto, *Decisione amministrativa e digitalizzazione della P.A.*, in *Federalismi*.it, 2, 2018, 2 ss.; Id., *Riflessioni in tema di decisione amministrativa algoritmica, intelligenza artificiale e legalità*, in *Federalismi.it*, 7, 2021, 187 ss.; S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Diritto Pubblico*, 1, 2019, 5 ss.; R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in *Diritto Amministrativo*, 4, 2019, 773 ss.; E. Picozza, *Intelligenza artificiale e diritto*, in *Giurisprudenza Italiana,* 2019, 1761 ss.; G. Orsoni-E. D'Orlando, *Nuove prospettive dell'amministrazione digitale:* open data *e algoritmi*, in *Istituzioni del federalismo*, 3, 2019, 593 ss.; A. Simoncini, *Amministrazione digitale algoritmica. Il quadro costituzionale*, in R. Cavallo Perin-D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, 2 ss.; D.U. Galetta, *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, in *Rivista italiana di diritto pubblico comunitario*, 3-4, 2020, 2205 ss.; M. Macchia-A. Mascolo, *Intelligenza artificiale e sfera pubblica: lo stato dell'arte*, in *Giornale di diritto amministrativo*, 4, 2022, 556 ss.

[4] Appare utile rammentare in questa sede la differenza tra algoritmo (ed il relativo programma che lo applica) e intelligenza artificiale (AI). Invero, l'algoritmo può essere definito come una sequenza di operazioni, non ambigue, che permettono di risolvere un problema in un numero finito di passi, rispettando due fondamentali requisiti: i) ad ogni passaggio della sequenza deve essere predefinito il passaggio successivo; ii) il risultato cui la sequenza tende deve essere concreto, reale ed utile. Tra gli algoritmi più semplici emergono i c.d. algoritmi deterministici e probabilistici: nei primi, costruiti secondo una logica causale, ad un certo dato inserito può corrispondere un solo passaggio successivo nella sequenza, tale per cui uno solo è il risultato finale a cui la macchina può pervenire; nei secondi, invece, la singola istruzione inserita ammette diversi possibili passaggi successivi che si svolgono secondo logiche probabilistiche. Ciò permette anche di tenere distinto il programma, e cioè un linguaggio informatico che permette alla macchina di utilizzare l'algoritmo per la soluzione di una classe di problemi. I sistemi di intelligenza artificiale, invece, utilizzano algoritmi ad "apprendimento automatico" (c.d. agenti intelligenti) che danno luogo ad applicazioni di *machine learning* o *deep learning*. In questi sistemi (non semplici), quindi, l'algoritmo fornisce un modello di apprendimento da applicare ai dati cui l'elaboratore informatico ha accesso per pervenire ad una soluzione attraverso l'analisi di esperienze pregresse relative a situazioni simili (vale a dire algoritmi, tecniche, soluzioni in grado di replicare il comportamento umano). Emerge, dunque, che tutti i sistemi di AI presuppongono l'uso di algoritmi, ma non può certo affermarsi che la decisione amministrativa in tutto o in parte automatizzata sia necessariamente derivante dall'impiego di un sistema di intelligenza artificiale. In dottrina cfr. G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione analisi predittiva e nuove forme di intelligibilità*, Napoli, 2019, 5 ss.; nonché, P. Otranto, *Riflessioni in tema di decisione amministrativa algoritmica, intelligenza artificiale e legalità*, cit., 190-191. In giurisprudenza cfr. Tar Lombardia, sez. II, 31 maggio 2021, n. 843.

[5] Cfr., da ultimo, G. Gallone, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione tra procedimento e processo*, Padova, 2023. L'autore attraverso un'analisi ricostruttiva dei profili di maggiore

di interesse per l'analisi giuridica sul rapporto tra decisione algoritmica e autotutela decisoria.

2. La vicenda processuale e la decisione del giudice amministrativo

La vicenda giudiziaria trae origine dal ricorso, promosso dinanzi al giudice amministrativo da un imprenditore agricolo, per l'annullamento delle determinazioni amministrative con le quali l'Agenzia per le erogazioni in agricoltura (d'ora in avanti Agea) aveva provveduto a rideterminare nel *quantum* i contributi, già riconosciuti ed erogati negli anni precedenti in favore del ricorrente[6].

Tanto per la determinazione (in prima battuta) del contributo, quanto per la nuova quantificazione (effettuata a distanza di due anni), l'Amministrazione si era avvalsa di un algoritmo. In particolare, l'importo era stato determinato sulla base di parametri oggettivi indicati nel bando e relativi, specificamente, all'altitudine e alla pendenza del fondo agricolo.

Il ricorrente osservava che i provvedimenti con i quali l'Agea aveva rideterminato le somme erano stati adottati a seguito dell'applicazione di un "algoritmo diverso" rispetto a quello che aveva condotto alla quantificazione degli indennizzi nel procedimento di primo grado.

Il provvedimento di secondo grado (qualificato dal ricorrente quale "revoca implicita") veniva, dunque, impugnato deducendo: i) la carenza di motivazione; ii) la inosservanza delle regole contenute nella *lex specialis*, in quanto la "manovra di ricalcolo" avrebbe comportato una modifica successiva dei criteri di valutazione per il riconoscimento di vantaggi economici; iii) la violazione dell'art. 21-quiquies, l. 241/1990 e dei relativi presupposti per l'esercizio del potere di revoca.

Il Tribunale amministrativo regionale, in accoglimento del ricorso, ha annullato i "provvedimenti di ricalcolo" emanati dall'Agea.

Il Collegio, dapprima, ha ribadito la tesi, da tempo affermata in giurisprudenza, della legittimità dell'impiego di algoritmi nell'ambito del procedimento amministrativo e, in un successivo passaggio argomentativo, ha richiamato, in particolare, i principi di piena conoscibilità e comprensibilità del "modulo algoritmico" utilizzato e dei criteri di elaborazione e di "non esclusività" della decisione algoritmica[7]. Il richiamo alle co-

interesse delle dinamiche che permeano l'impiego di meccanismi automatizzati nello svolgimento dell'attività amministrativa, si sofferma sul concetto di "riserva di umanità", giungendo ad affermare, con riguardo specifico al momento decisorio, la necessità che il risultato prodotto dagli algoritmi o dai sistemi di intelligenza artificiale sia vagliato dal funzionario titolare dell'organo e recepito nel provvedimento amministrativo a garanzia del principio di legalità, delle guarentigie procedimentali e «del principio personalistico della funzione pubblica quale valore fondante del nostro ordinamento» (ivi, 223).

[6] Si trattava, in particolare, di somme riconosciute a titolo di indennità compensativa per le zone montane di cui al Piano di sviluppo rurale della Campania.

[7] In particolare, il Tar Campania ha osservato che «la decisione adottata con ricorso all'algoritmo vede sempre la necessità che sia l'Amministrazione a compiere un ruolo *ex ante* di selezione e verifica, anche per mezzo di costanti test, aggiornamenti e modalità di perfezionamento dell'algoritmo. In tali casi si

ordinate essenziali di teoria generale, tuttavia, vale solo quale premessa – certamente non determinante ai fini del decidere – per sviluppare l'argomento su cui la sentenza si fonda: i provvedimenti impugnati risultavano affetti da vizio di motivazione stante il generico riferimento alla "normativa vigente" e alle "indicazioni della Commissione europea" che avrebbero condotto alla rideterminazione degli importi dovuti in applicazione del nuovo algoritmo.

In relazione agli atti amministrativi ad elaborazione elettronica (o, secondo altra terminologia, "atti amministrativi automatizzati") assume una particolare rilevanza il principio di trasparenza[8] che trova immediata declinazione nell'obbligo di motivazione degli atti[9]. L'obbligatorietà della motivazione nei provvedimenti "tradizionali" costituisce una regola che consente di istituire un raccordo tra procedimento e provvedimento e, dunque, tra forma della funzione[10] e manifestazione del potere funzionalizzato. Essa, com'è noto, costituisce una rilevante declinazione del "diritto ad una buona amministrazione" che nei procedimenti svolti attraverso sistemi automatizzati assolve ad una funzione di garanzia non meno rilevante[11].

Quanto più risulta opaco e difficilmente intellegibile l'*iter* logico-giuridico seguito dall'Amministrazione attraverso l'impiego di sistemi automatizzati, tanto più le regole tecniche che sovrintendono al funzionamento degli stessi devono essere verificabili

deve contemplare la possibilità che sia il giudice a dover svolgere, per la prima volta sul piano umano, valutazioni e accertamenti fatti direttamente in via automatica, con la conseguenza che la decisione robotizzata impone al giudice di valutare la correttezza del processo automatizzato in tutte le sue componenti». Sul punto cfr., altresì, Cons. Stato, sez. VI, 8 aprile 2019, n. 2270; Cons. Stato, sez. VI, 4 febbraio 2020, n. 881; Cons. Stato, sez. VI, 4 giugno 2021, n. 1206.

[8] Cfr., in via generale, A. Police, *La predeterminazione delle decisioni amministrative. Gradualità e trasparenza nell'esercizio del potere discrezionale*, Napoli, 1997; nonché, E. Carloni, *Il paradigma trasparenza. Amministrazioni, informazione, democrazia*, Bologna, 2022.

[9] Considerati i numerosi studi della dottrina, ci si limita in questa sede a ricordare i contributi di C.M. Iaccarino, *Studi sulla motivazione con speciale riguardo agli atti amministrativi*, Roma, 1933; M.S. Giannini, *Motivazione dell'atto amministrativo*, in *Enciclopedia del diritto*, vol. XXVII, Milano, 1977, 257 ss.; A. Romano Tassone, *Motivazione dei provvedimenti amministrativi e sindacato di legittimità*, Milano, 1987; G. Corso, *Motivazione dell'atto amministrativo*, in *Enciclopedia del diritto, Aggiornamento*, vol. V, Milano, 2001, 774 ss.; M. De Benedetto, *Motivazione dell'atto amministrativo*, in *Enciclopedia Giuridica*, vol. XXIII, Roma, 2003; A. Cassatella, *Il dovere di motivazione nell'attività amministrativa*, Padova, 2013; A. Cioffi, *La motivazione del provvedimento amministrativo*, in A. Romano (a cura di), *L'azione amministrativa*, Torino, 2016, 199 ss.; R. Villata-M. Ramajoli, *Il provvedimento amministrativo*, Torino, 2017, 269 ss. Per ulteriori riferimenti bibliografici e per un approfondimento dei profili di maggior interesse dell'istituto, cfr. F. Cardarelli, *La motivazione del provvedimento*, in M.A. Sandulli (a cura di), *Codice dell'azione amministrativa*, Milano, 2017, 374 ss. L'autore, infatti, spiega come la motivazione assolva ad una funzione di garanzia e di tutela del diretto destinatario del provvedimento, e di altri potenziali destinatari, precisando che si tratta di una garanzia formale che riflette il dispiegarsi di garanzie sostanziali per il corretto esercizio dell'azione amministrativa (ivi, 407 ss.).

[10] Secondo la nota definizione di F. Benvenuti, *Funzione amministrativa, procedimento e processo*, in *Rivista trimestrale di diritto pubblico*, 1952, 118 ss., poi in *Scritti giuridici*, II, Milano, 2006, 1117 ss.

[11] Nella sentenza in commento, ad esempio, si ribadisce: «il fatto che il provvedimento venga emanato sulla scorta di una complessa operazione di calcolo produce l'opposto effetto di rafforzare, per certi versi, l'obbligo motivazionale in capo all'Amministrazione, la quale dovrà rendere la propria decisione finale non solo conoscibile, ma anche comprensibile». Ne deriva che in caso di decisione fondata su algoritmo, si richiede che sia assicurata una declinazione rafforzata del principio di trasparenza, intesa come piena conoscibilità della regola espressa in un linguaggio differente da quello giuridico. In tali termini cfr. anche Cons. Stato, sez. VI, 8 aprile 2019, n. 2270.

e decifrabili, al fine di rendere l'algoritmo (ed il programma che dell'algoritmo rappresenta la traduzione) conoscibile, comprensibile e, in ultima analisi, controllabile, e perciò sindacabile in sede giurisdizionale.
Nel caso di specie, infatti, il giudice amministrativo evidenzia come l'Agea, nell'adottare i provvedimenti di secondo grado applicando un ulteriore e diverso algoritmo, avesse violato per un verso le garanzie partecipative, per altro verso l'obbligo di garantire una adeguata conoscibilità delle ragioni logico-giuridiche poste a fondamento della decisione, genericamente identificate dall'Amministrazione quali ragioni di ottemperanza a nome interne e ad indicazioni della Commissione europea.
Appare, invero, questo il punto considerato dirimente dal Collegio in relazione alla illegittimità degli atti impugnati. Gli altri argomenti giuridici sviluppati nella sentenza, infatti, forniscono una ricostruzione del fenomeno del c.d. atto amministrativo automatizzato ma non costituiscono ragione della decisione[12].

3. Quadro normativo e statuto pretorio del provvedimento algoritmico

Al fine di meglio inquadrare le questioni giuridiche poste dalla decisione in rassegna si ritiene indispensabile svolgere una breve analisi del contesto normativo e dei significativi interventi della giurisprudenza nella disciplina dei procedimenti e dei provvedimenti algoritmici.
Occorre anzitutto sottolineare che nel nostro ordinamento – pur in assenza di specifiche norme che riconoscano la possibilità per l'Amministrazione di adoperare sistemi automatizzati nell'adozione dei provvedimenti amministrativi – si segnala da tempo una significativa attenzione verso le regole del c.d. procedimento amministrativo elettronico. Se è vero che all'amministrazione digitale sin dal 2005 si è dedicato addirittura un codice, recante disposizioni che prefigurano l'impatto delle nuove tecnologie in ogni fase del procedimento[13], è con l'introduzione dell'art. 3 bis nella legge generale sul

[12] In proposito si vedano le osservazioni sviluppate dal Tar sul concetto del necessario coinvolgimento di un "agente umano" nel processo che conduce all'adozione della decisione (c.d. *human in the loop*). Nell'ambito del procedimento amministrativo automatizzato, il principio in questione implicherebbe – usando le parole del Collegio – che "il funzionario possa in qualsiasi momento intervenire per compiere interlocuzioni con il privato, per verificare a monte l'esattezza dei dati da elaborare, mantenendo il costante controllo del procedimento". Ciò, in una prospettiva di contenimento del rischio di una "spersonalizzazione" della funzione amministrativa, soprattutto nei casi di ricorso a strumenti automatizzati in funzione "servente" della decisione umana e/o parzialmente decisionale, nonché della deresponsabilizzazione dell'Amministrazione e dei suoi funzionari. In dottrina, sul tema, cfr. M.C. Cavallaro-G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it,* 16, 2019, 1 ss.; M.C. Cavallaro, *Imputazione di responsabilità delle decisioni automatizzate*, in *European Review of Digital Administration and Law*, 1-2, 2020, 73 ss.; E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Diritto amministrativo*, 2020, 283 ss.; B. Marchetti, *La garanzia dello Human in the Loop alla prova della decisione amministrativa algoritmica*, in *Biolaw Journal*, 2021, 367 ss.; D.U. Galetta, *Human-stupidity-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, in *Federalismi.it*, 5, 2023, iv ss.; G. Gallone, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione tra procedimento e processo*, cit., passim.

[13] Come osserva P. Otranto, *Riflessioni in tema di decisione amministrativa algoritmica, intelligenza artificiale e legalità*, cit., 189, «dall'iniziativa, allo svolgimento dell'istruttoria (art. 41), alla partecipazione (art. 4),

procedimento amministrativo[14] e con l'enunciazione del principio del *digital first*[15] che l'impiego di strumenti informatici e telematici si proietta stabilmente verso l'esterno[16]. A livello sovranazionale[17] il regolamento (UE) 679/2016 sulla protezione dei dati personali (c.d. GDPR) ha espressamente previsto (art. 22) la possibilità anche per le Amministrazioni di adottare atti automatizzati, ove una legge delle Stato espressamente lo autorizzi ovvero nei casi in cui la decisione automatizzata sia il risultato di un contratto con l'interessato o di un consenso formatosi con lo stesso.

Si può osservare che, a dispetto della costante diffusione degli algoritmi nell'azione amministrativa, le regole poste a presidio di questa "nuova" forma di esercizio del potere (*recte* a presidio del processo che conduce alla formazione della volontà inverata nel provvedimento espressione del potere) sono delineate solo per via giurisprudenziale. Nelle pronunce della giurisprudenza e nelle riflessioni della dottrina maggioritaria, di contro, resta sullo sfondo la pur rilevante questione giuridica relativa alla stessa ammissibilità, nell'ordinamento vigente, della decisione automatizzata[18].

---

alla forma dell'atto (art. 20) e agli adempimenti necessari per la piena efficacia dello stesso (art. 3 *bis*), lo svolgimento della funzione amministrativa risulta profondamente inciso e conformato dalle nuove tecnologie, attraverso una disciplina legale che pare incentrata sulla dimensione organizzatoria, sul procedimento e sulla forma dell'atto».

14 L'art. 3 bis, l. 241/1990, introdotto con l'art. 12, c. 1, lett. b), d.l. 76/2020 (c.d. semplificazioni), dispone che «le amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, nei rapporti interni, tra le diverse amministrazioni e tra queste e i cittadini».

15 Il riferimento è all'art. 1, c. 1, lett. b), l. 124/2015 che individuava quale principio generale per la semplificazione dei procedimenti amministrativi, in un'ottica di celerità, certezza giuridica e trasparenza dell'azione amministrativa, quello del c.d. *digital-first*, perseguibile mediante la ridefinizione, in chiave digitalizzata, delle procedure amministrative e della stessa organizzazione interna. In dottrina cfr. il contributo monografico di G. Pesce, *Digital first. Amministrazione digitale: genesi, sviluppi, prospettive*, Napoli, 2018.

16 Come aveva lucidamente prefigurato M.S. Giannini, *Rapporto sui principali problemi dell'amministrazione dello Stato*, in *Il foro italiano*, V, 1979, 289 ss.

17 È utile evidenziare, inoltre, che altri ordinamenti hanno già previsto espressamente la possibilità per le Amministrazioni di agire attraverso moduli parzialmente o totalmente automatizzati. Si può fare riferimento, a mero titolo di esempio, alla *Ley de 22 de juno*, *n. 11/2007* (*Actuaciòn adminstrativa automatizada*), poi sostituita dalla *Ley de 1 de octubre*, *n. 39/2015* (*Procedimento Adminstrativo Comun del las Administraciones Publicas*); nonché, per l'ordinamento tedesco, all'§35A della *Verwaltungsverfahrensgesetz* (VwVfG), ove espressamente si prevede che «un atto amministrativo può essere emanato interamente con mezzi automatici, a condizione che ciò sia consentito dalla legge e che non vi sia discrezione». Si veda anche il decreto 733/2018 del Ministero della modernizzazione della Repubblica Argentina attraverso il quale viene incentivato il ricorso agli strumenti digitali e di intelligenza artificiale, al fine di ridurre la complessità delle procedure amministrative. Sul tema cfr., in dottrina, D.U. Galetta-J.G. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3, 2019, 1 ss.; F.J. Lavaca, *Acto administrativo automatico*, Buenos Aires, 2022, 158 ss.

18 Tale profilo, relativo al rapporto tra principio di legalità e decisione automatizzata, è posto, tuttavia, al centro dell'analisi di S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, cit., 34 ss. Cfr. anche P. Otranto, *Riflessioni in tema di decisione amministrativa algoritmica*, cit., 202, il quale afferma condivisibilmente che «la legge non dovrebbe limitarsi ad attribuire alle Amministrazioni il potere di ricorrere all'uso delle nuove tecnologie per adottare provvedimenti che già rientrano nella loro sfera di competenza (in ossequio al principio di legalità formale), ma dovrebbe anche specificare, in ossequio al principio di legalità sostanziale, i principi e le regole che devono essere osservati nella definizione, progettazione e implementazione del sistema che conduce all'adozione della decisione automatizzata e che potrebbero, in concreto, meglio essere adeguati alle peculiarità dei singoli procedimenti anche attraverso norme di rango secondario». In senso contrario cfr. G. Carullo, *Decisione amministrativa e intelligenza artificiale*, in *Diritto dell'informazione e dell'informatica*, 3, 2021, 431 ss., per il quale la

Il giudice amministrativo, dunque, ha enucleato una sorta di "statuto pretorio" della materia, affermando la valenza precettiva di regole e garanzie minime proprie del procedimento amministrativo[19] che nei moduli decisori algoritmici rischiavano di essere *de facto* ritenute recessive innanzi all'interesse alla speditezza dell'azione amministrativa "automatizzata".

Almeno in una prima fase, la giurisprudenza amministrativa si è mostrata restia rispetto all'ipotesi di ammettere il ricorso alla decisione totalmente automatizzata, adottata, cioè, senza il sostanziale apporto del decisore umano[20]. In particolare, i dubbi si fondavano sull'impossibilità che nell'applicazione di tali strumenti, caratterizzati da automatismi e opacità intrinseca[21], si potesse assicurare l'osservanza delle guarentigie procedimentali, sicché, in tale impostazione, l'algoritmo avrebbe tutt'al più una funzione meramente "servente" rispetto all'attività propria del funzionario, unico soggetto chiamato ad adottare una decisione (e ad emanare il provvedimento).

L'elaborazione giurisprudenziale immediatamente successiva[22], sembra mostrare al contrario un certo "apprezzamento" per il ricorso a decisioni automatizzate, ritenute ammissibili (ancorché a livello di *obiter dicta*) anche in presenza di un potere caratterizzato da margini di discrezionalità amministrativa[23].

---

possibilità, per l'Amministrazione, di avvalersi di strumenti automatizzati nell'assunzione delle decisioni amministrative è da ritenersi implicita nella norma attributiva del potere; tale possibilità rientrerebbe – secondo l'Autore – nella libertà di scelta, ispirata ai principi di imparzialità e buon andamento, dei mezzi di cui l'Amministrazione decide di dotarsi per l'esecuzione dei propri compiti.

[19] Non è questa la sede per tentare di ricostruire, neanche sommariamente, il dibattito dottrinale che ha costituito il presupposto teorico per l'introduzione delle regole sul procedimento amministrativo. Basterà solo richiamare le fondamentali riflessioni di A.M. Sandulli, *Il procedimento amministrativo*, Milano, 1940; M.S. Giannini, *Lezioni di diritto amministrativo*, Milano, 1950, 261 ss.; Id., *Diritto amministrativo*, I, Milano, 1994, 81 ss.; F. Benvenuti, *Funzione amministrativa*, *procedimento*, *processo*, cit.; M. Nigro, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano, 1966. Per una compiuta analisi degli studi sul procedimento, cfr. A. Sandulli, *Il procedimento,* in S. Cassese (a cura di), *Trattato di diritto amministrativo, Diritto amministrativo generale*, II, Milano, 2003, 1035 ss. Con specifico riguardo ai procedimenti automatizzati cfr. G. Duni, *L'amministrazione digitale. Il diritto amministrativo nell'evoluzione telematica*, Milano, 2008; A.G. Orofino, *Forme elettroniche e procedimenti amministrativi*, Bari, 2008.; più di recente, D. Marongiu, *Algoritmo e procedimento amministrativo*, in *Giurisprudenza italiana*, 6, 2022, 1515 ss.

[20] Cfr. Tar Lazio, sez. III *bis*, 14 febbraio 2017, n. 3769. Si veda, sul punto, il commento di I. Forgione, *Il caso dell'accesso al software Miur per l'assegnazione dei docenti* (nota a Tar Lazio, sez. III *bis*, 14 febbraio 2017, n. 3769), in *Giornale di diritto amministrativo,* 3 2018, 647 ss. Cfr., altresì, Tar Lazio, sez. III *bis*, 10-13 settembre 2019, n. 10964.

[21] Cfr. G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione analisi predittiva e nuove forme di intelligibilità*, cit., 153, secondo la quale «di fronte agli algoritmi un certo grado di opacità rimane ineliminabile» (ivi, 153). Cfr. anche R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, in *Diritto amministrativo*, 2, 2020, 305 ss.

[22] Cfr., ancora, Cons. Stato, sez. VI, 8 aprile 2019, n. 2270. Sul punto si vedano le riflessioni di G. Fasano, *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica*, in questa *Rivista*, 3, 2019, 234 ss.; nonché, A.G. Orofino, *La semplificazione digitale*, in *Il diritto dell'economia*, 3,2019, 92 ss.

[23] Sulla discrezionalità amministrativa cfr., almeno, M.S. Giannini, *Il potere discrezionale della pubblica amministrazione*, Milano, 1939; V. Cerulli Irelli, *Note in tema di discrezionalità amministrativa e sindacato di legittimità*, in *Diritto e processo amministrativo*, 1984, 463 ss.; L. Benvenuti, *La discrezionalità amministrativa*, Padova, 1986; A. Angiuli, *Studi sulla discrezionalità amministrativa nel quando*, Bari, 1988; Id., *Lineamenti vecchi e nuovi della discrezionalità*, Milano, 1992; G. Barone, voce *Discrezionalità* (*dir. amm.*), in *Enciclopedia giuridica*, vol. XIII, Roma, 1989, 1 ss. Con specifico riferimento al rapporto tra digitalizzazione e discrezionalità cfr., tra i più recenti, A. Cassatella, *La discrezionalità amministrativa nell'età digitale*, in Aa.Vv.,

Il giudice amministrativo[24], tuttavia, ha opportunamente ritenuto di individuare alcuni presupposti, che si traducono in altrettante "prescrizioni", in ordine all'utilizzabilità di moduli decisori automatizzati, enucleando le già richiamate leggi della legalità algoritmica[25], tra le quali rientrano i principi di conoscibilità dello strumento informatico utilizzato[26], di comprensibilità del modulo decisorio[27], di non esclusività della decisione automatizzata (con ciò segnalando l'inderogabile "riserva di umanità" nella decisione amministrativa)[28].

4. L'algoritmo tra natura giuridica, provvedimento amministrativo e autotutela decisoria

Occorre a questo punto interrogarsi sul rapporto tra software (e algoritmo alla sua base) adoperato dall'Amministrazione e provvedimento "a valle" ed in particolare sugli effetti che eventuali errori, imperfezioni o "vizi" del programma, intesi in senso non strettamente giuridico, possono produrre sul provvedimento finale concretamente incidente sulla posizione giuridica del destinatario[29].

Diritto amministrativo: Scritti per Franco Gaetano Scoca, I, Napoli, 2021, 675 ss.; A. Police, *Scelta discrezionale e decisione algoritmica*, R. Giordano-A. Panzarola-A. Police-S. Preziosi-M. Protto (a cura di), *Il diritto nell'era digitale*, Milano, 2022, 493 ss.

[24] In particolare, Cons. Stato, sez. VI, 13 dicembre 2019, nn. 8472 – 8473 – 8474. Su tali sentenze cfr., ancora, le riflessioni di R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, cit., 773 ss.; nonché, S. Vaccari, *Note minime in tema di Intelligenza Artificiale e decisioni amministrative*, in *Giustamm.it*, 2019, 1 ss.

[25] Cfr. E. Carloni, *I principi della legalità algoritmica*, cit., passim.

[26] Cfr. Cons. Stato, sez. VI, 8 aprile 2019, n. 2270, § 8.3., ove si afferma che «il meccanismo attraverso il quale si concretizza la decisione robotizzata (ovvero l'algoritmo) deve essere "conoscibile", secondo una declinazione rafforzata del principio di trasparenza, che ne implica anche la piena conoscibilità della regola espressa in un linguaggio differente da quello giuridico. Tale conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti. Ciò al fine di poter verificare che gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare – e conseguentemente sindacabili – le modalità e le regole in base alle quali esso è stato impostato».

[27] Cfr. Cons. Stato, sez. VI, 8 aprile 2019, n. 2270, § 8.3., ove si legge che «la "caratterizzazione multidisciplinare" dell'algoritmo comporta che la sua comprensione non richieda solo competenze giuridiche, ma anche tecniche, informatiche, statistiche, amministrative, sicché non esime dalla necessità che la "formula tecnica", che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella "regola giuridica" ad essa sottesa e che la rendano leggibile e, quindi non solo «conoscibile», ma anche "comprensibile"». Sul punto cfr., in dottrina, A. Mascolo, *Gli algoritmi amministrativi: la sfida della comprensibilità*, in *Giornale di diritto amministrativo*, 3, 2020, 366 ss.; G. Lo Sapio, *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in *Federalismi.it*, 16, 2021, 1 ss.

[28] Cfr. Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472, § 15.2.; nonché, Cons. Stato, sez.VI, 4 febbraio 2020, n. 881 e 4 giugno 2021 n. 1206. In dottrina cfr., *ex multis*, A. Simoncini, *L'algoritmo incostituzionale, intelligenza artificiale e futuro delle libertà*, in *BioLaw Journal*, 2019, 63 ss.; Id., *Profili costituzionali della amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, 4, 2019, 1149 ss.; più di recente cfr., ancora, D.U. Galetta, *Human-stupidity-in-the-loop? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, cit., iv ss.

[29] Nel caso esaminato dalla sentenza in commento riveste, di contro, un limitato interesse l'esatta

In particolate, si può rilevare come, in dottrina, le tesi tradizionali abbiano variamente ricondotto, con gradazioni differenti, il programma (e l'algoritmo) utilizzato per la gestione informatizzata dei procedimenti amministrativi al vasto *genus* dell'atto amministrativo[30].

Secondo una prima impostazione[31] l'atto-programma sarebbe da qualificare come atto amministrativo attraverso il quale l'Amministrazione indirizza il proprio *agere*, predeterminandone modalità e contenuti; esso non avrebbe una mera rilevanza interna in quanto, benché non immediatamente incidente sulla sfera giuridica del destinatario, assumerebbe una non trascurabile rilevanza esterna perché idoneo a condizionare, concretamente, il contenuto del provvedimento finale[32].

Altra parte della dottrina, di contro, ha ricondotto il programma alla categoria degli atti provvedimentali[33] e, pertanto, aventi una efficacia esterna diretta ed immediata. Secondo quest'ultima ricostruzione, se il potere è esercitato con la predisposizione del programma informatico e l'atto finale è da esso determinato nei presupposti e nei contenuti, allora il primo può dirsi assumere già le connotazioni provvedimentali, con la conseguente idoneità ad incidere sulle posizioni giuridiche dei privati.

Infine, non è mancato chi è giunto a qualificare il programma quale atto avente natura regolamentare[34].

---

qualificazione del provvedimento impugnato. Come si è anticipato, infatti, il ricorrente asseriva che l'Agea, attraverso tale atto, avesse operato una "revoca implicita" del precedente provvedimento. Pare, tuttavia, che i provvedimenti oggetto di gravame possano qualificarsi come atti espressione del potere di annullamento d'ufficio (*ex* art. 21 nonies, l. 241/1990, ss.mm.ii.). Ed infatti, come si legge nella pronuncia in commento, l'Agea avrebbe "rielaborato" la domanda del ricorrente (*recte* qualificato nuovamente il contributo dovuto) in ragione dell'illegittimità del provvedimento favorevole emanato in prima battuta, a sua volta derivante da un algoritmo in qualche misura difforme dal paradigma normativo. La questione, invero, sembra risolversi in radice, poiché – pur in assenza di una pronuncia esplicita sul punto da parte del giudice – la qualificazione dell'atto può ritenersi un'operazione intellettiva, di sussunzione della fattispecie concreta in quella astratta, tipica dell'attività interpretativa del giudice (cfr., *ex multis*, Cons. Stato, sez. V, 5 gennaio 2023, n. 211; nonché, Cons. Stato, sez. VI, 24 settembre 2019, n. 6378; Cons. Stato, sez. II, 30 settembre 2019, n. 6534; Cons. Stato, sez. IV, 5 giugno 2020, n. 3552). Tale operazione richiede di interpretare l'atto amministrativo non solo in base al suo tenore letterale, ma soprattutto "in base al suo specifico contenuto e risalendo al potere concretamente esercitato dall'amministrazione". In dottrina cfr., già, D. Sorace, *Atto amministrativo,* in *Enciclopedia del diritto*, *Annali*, VII, Milano, 2014, 46 ss.

[30] Le tesi dottrinarie sono compiutamente riprese ed analizzate anche da G. Gallone, *Riserva di umanità e funzioni amministrative*, cit., 87 ss.

[31] Cfr. D. Marongiu, *L'attività amministrativa automatizzata*, cit., 18, il quale riprende la tesi dell'atto amministrativo generale a "rilevanza esterna". Cfr., altresì, A. Masucci, *Atto amministrativo informatico*, in *Enciclopedia del diritto, Aggiornamento*, I, 1997, 221 ss.

[32] Tale impostazione si fonda sulla considerazione secondo cui la regola tecnica che governa l'algoritmo, ed il software che ne costituisce la traduzione in linguaggio macchina, è una regola amministrativa generale, costruita dall'uomo ed applicata dalla macchina, con la conseguenza che esso debba qualificarsi come atto amministrativo informatico. Cfr., in giurisprudenza, Cons. Stato, sez. VI, 8 aprile 2019, n. 2270.

[33] Cfr. U. Fantigrossi, *Automazione e pubblica amministrazione*, Bologna, 1993, 56 ss. Cfr., più di recente, le riflessioni di A.G. Orofino, *L'attuazione del principio di trasparenza nello svolgimento dell'Amministrazione elettronica*, in *Judicium*, 19 ottobre 2020, 3 ss.

[34] Questa tesi è sviluppata da A. Boix Palop, *Los algoritmos sono reglamentos: la necesidad de extender las garantias propria del las normas reglamentarias a los programas empleados por la administracìon para la adopcìon de decisiones*, in *Revista de Derecho Pùblico: Teorìa y Metodo*, 2020, 223 ss. Secondo l'autore, infatti, l'algoritmo (e

Queste ricostruzioni sembrerebbero scontare, tuttavia, l'astrazione dal significato, tecnico prima che giuridico, di programma (e, di conseguenza, da quello di algoritmo), la cui corretta perimetrazione rappresenta il presupposto ineludibile per la ricostruzione del rapporto tra strumenti decisori automatizzati e provvedimento amministrativo. Come si è già osservato[35], l'algoritmo – quale procedimento logico che, attraverso un numero finito di operazioni o istruzioni, risolve una classe di problemi – non presenta un contenuto di valutazione, di giudizio o, tantomeno, di decisione (valenza prescrittiva), bensì di mera descrizione dei passaggi logici e di individuazione delle modalità, destinate alla macchina, funzionali alla risoluzione di una classe di problemi in forma automatizzata. Così, il programma è considerato lo strumento, il linguaggio informatico che permette alla macchina di utilizzare l'algoritmo e, elaborando i dati, risolvere i problemi individuati.

In dottrina si è recentemente osservato che le ricostruzioni in termini di atto amministrativo del programma (e dell'algoritmo) possono dirsi legate all'esigenza di risolvere la questione inerente alla compatibilità tra provvedimento automatizzato e discrezionalità amministrativa[36]. In tali teorie, infatti, pur nelle diversità delle ricostruzioni, si affermava che con la scelta di adoperare un programma (avente alla base un algoritmo) per la decisione amministrativa, si realizzasse già una parziale spendita del potere amministrativo con la conseguente insorgenza di un autovincolo[37], con ciò consumando parte dei profili di apprezzamento riconosciuti all'Amministrazione dalla legge.

Il superamento delle tesi "attizie" ha indotto la dottrina più recente a qualificare il programma, riguardato nella sua dimensione dinamica[38], quale strumento dell'azione amministrativa impiegato dall'Amministrazione tra la fase istruttoria e quella decisoria. Si tratterebbe, in particolare, di uno strumento funzionalizzato all'esercizio del potere e alla concretizzazione delle scelte dell'Amministrazione. Seguendo questa impostazione il risultato dell'operazione compiuta dal programma (e dall'algoritmo che esso applica) rappresenterebbe nient'altro che "le risultanze dell'istruttoria" da porre alla base del

il programma) utilizzato dalla pubblica Amministrazione in modo non puramente strumentale produce, materialmente, gli stessi effetti di qualsiasi regolamento, preordinando la decisione finale dell'Autorità pubblica e limitando l'ambito di discrezionalità o la capacità di determinazione sulla base dei postulati contenuti nella programmazione normativa dell'attività amministrativa, e cioè la "regola" contenuta nell'atto normativo.

35 Cfr. *supra* par. 1, nota 4.

36 Cfr., di recente, G. Gallone, *Riserva di umanità e funzioni amministrative*, cit., 89 ss. L'A. evidenzia, inoltre, come l'inadeguatezza di simili ricostruzioni si «appalesa con ancor maggior chiarezza se si guarda alla automazione avanzata a mezzo di intelligenza artificiale; tecnica che risulta fondata su algoritmi a "struttura aperta" che non prevedono la definizione di una classe finita di operazioni e rispetto ai quali non potrebbe ammettersi l'idoneità ad esprimere giudizi o valutazioni».

37 La figura dell'autovincolo è stata applicata in dottrina da A. Masucci, *L'atto amministrativo automatizzato*, cit., 37 ss., per spiegare il progressivo esaurimento dei margini di discrezionalità con riguardo a funzioni amministrative automatizzate. Cfr., altresì, F. Saitta, *Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo*, cit., 7 ss. In generale sul concetto di autovincolo cfr., già, le riflessioni di M.P. Vipiana, *L'autolimite della pubblica amministrazione*, Milano, 1990.

38 G. Gallone, *Riserva di umanità e funzioni amministrative*, cit., 93 ss., guarda al rapporto tra algoritmo e atto amministrativo anche dal punto di vista della sua dimensione "statica", che indurrebbe a contrassegnare il modulo automatizzato quale "oggetto della volizione amministrativa preliminare con cui l'Amministrazione opta per l'automazione".

provvedimento finale[39].

Ciò, conduce alla identificazione di due momenti della volizione amministrativa: il primo, che si colloca nel momento antecedente all'avvio del procedimento, rappresentato dalla scelta da parte dell'Amministrazione (attraverso un atto amministrativo) di utilizzare il programma nell'attività procedimentale; il secondo, invece, si identifica a valle della fase istruttoria, e cioè nel momento in cui l'Amministrazione – adoperando il programma – fa proprio, nel provvedimento finale, il risultato prodotto dalla macchina[40].

Ora, è proprio in relazione a tali diverse ricostruzioni che sorge la questione del rapporto tra il programma informatico e il provvedimento "automatizzato"[41] e degli (eventuali) effetti, sul secondo, derivanti da vizi o mal funzionamenti del primo. In particolare, il provvedimento derivante dall'utilizzo del programma può, ad esempio, ritenersi illegittimo in caso di: difetto di costruzione dell'algoritmo posto alla base del programma; difetto di progettazione e realizzazione del programma; errata imputazione dei dati utilizzati dal software; mal funzionamento dell'hardware[42].

Pertanto, se si ammettesse la natura attizia del programma il problema che si porrebbe sarebbe quello classico, dei rapporti tra atto amministrativo "a monte" (illegittimo) e provvedimento amministrativo consequenziale. Si tratterebbe, a ben guardare, di una invalidità derivata, e cioè prodotta (sul provvedimento applicativo) dalla illegittimità dell'atto (programma) presupposto[43].

Di contro, riconducendo il software (e l'algoritmo) a mero modulo organizzativo, strumento dell'istruttoria amministrativa le cui risultanze sono poste alla base della decisione finale, il vizio dello stesso determinerebbe un vizio dell'istruttoria e, dunque, l'illegittimità del provvedimento per eccesso di potere[44].

Su altro versante si pone poi la questione relativa alla perdurante valenza, anche nei procedimenti di secondo grado, dei principi che informano la decisione amministrati-

---

[39] In giurisprudenza cfr., *ex multis*, Cons. Stato, sez. VI, 13 dicembre 2019, n. 8474, che qualifica espressamente il ricorso all'utilizzo del software in termini di scelta del modulo organizzativo da parte dell'Amministrazione, strumento procedimentale ed istruttorio, soggetto alle verifiche tipiche di ogni procedimento amministrativo.

[40] L'analisi è compiuta da G. Gallone, *Riserva di umanità e funzioni amministrative,* cit., 97 ss., cui si rinvia per i riferimenti agli studi che hanno elaborato tale tesi.

[41] È appena il caso rilevare, tuttavia, che la sentenza in commento non prende in alcun modo posizione su tale rilevante questione giuridica che non pare, d'altro canto, esser stata oggetto di puntuali deduzioni del ricorrente. Ed infatti, il Tar Campania, come osservato, perviene all'annullamento del provvedimento impugnato accogliendo il motivo di ricorso relativo alla carenza di motivazione.

[42] Sulla patologia dell'atto amministrativo elettronico cfr. A.G. Orofino, *La patologia dell'atto amministrativo elettronico: sindacato giurisdizionale e strumenti di tutela*, in *Il foro amministrativo- C.d.S.*, 2002, 2257 ss.; nonché, ancora, F. Saitta, *Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo*, cit., 24 ss.

[43] Cfr., già, A. Masucci, *Atto amministrativo informatico*, cit., 227, secondo il quale «se questo atto si pone come "atto madre" del procedimento decisionale, ne consegue che eventuali illegittimità (dell'atto programma) viziano l'atto finale del procedimento. In forza del "principio di derivazione" si riflettono sull'atto amministrativo finale tutti i vizi relativi ai singoli atti del procedimento». Cfr., altresì, F. Saitta, *Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo*, cit., 20 ss.; L. Carbone, *L'algoritmo e il suo giudice*, in *Giustizia-amministrativa.it*, 2023.

[44] Sul punto R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, cit., 310, osserva che «con il vizio di eccesso di potere i limiti che l'algoritmo assume sono la logicità e la comprensibilità della scelta dell'amministrazione, oltre i quali l'algoritmo procederà a compiere, con imparzialità, disciplina e onore, i concreti atti di gestione in attuazione dell'indirizzo politico-amministrativo degli organi di governo».

va.

È noto che gli istituti espressione di autotutela decisoria consentono all'Amministrazione di incidere unilateralmente su un provvedimento già adottato, ove tale scelta risponda all'interesse pubblico. Ed è altrettanto noto che il provvedimento di secondo grado deve pervenire all'esito di un procedimento amministrativo e deve essere adottato garantendo l'osservanza dei limiti posti dalla legge.

Non è questa la sede per ripercorrere l'articolato dibattito sul fondamento del potere di autotutela[45]. È utile, tuttavia, osservare come, secondo parte della dottrina, l'autotutela "non possa più considerarsi espressione dell'immanenza ed inesauribilità del potere di amministrazione attiva – derivanti dalla necessità di garantire la continua rispondenza dell'attività amministrativa al pubblico interesse – ma debba essere ancorato al principio di legalità"[46].

In tale prospettiva, però, la questione che sembra suscitare maggiore interesse ai fini della presente riflessione è quella inerente alla inderogabilità delle guarentigie procedimentali anche nei procedimenti di secondo grado. Le riflessioni della dottrina[47], infatti, hanno indotto a ritenere che l'assetto normativo che disciplina l'esercizio del potere di autotutela (soprattutto di tipo decisorio) sia espressione di un potere eccezionale attribuito all'Amministrazione, che risulta sempre più conformato non solo all'interesse pubblico, ma anche alla tutela delle posizioni giuridiche dei cittadini sorte o ampliate per effetto del primo provvedimento e suscettibili di essere lese dal provvedimento di secondo grado. Tanto, si desume non solo dalla necessaria considerazione, da parte dell'Amministrazione, degli interessi privati suscettibili di venire in rilievo nel procedimento di riesame, ma anche dalla disciplina del c.d. "termine ragionevole" per l'esercizio del potere, individuati in dodici mesi nei soli casi di provvedimenti autorizzatori o attributivi di vantaggi economici.

Se anche il potere di riesame è un potere esercitato all'esito di un procedimento nel quale deve trovare adeguata tutela il principio del contraddittorio nella sua proiezione

---

[45] Considerata l'ampia produzione scientifica cfr., almeno, F. Benvenuti, voce *Autotutela (diritto amministrativo)*, in *Enc. dir.*, vol. IV, Milano, 1959, 537 ss.; G. Coraggio, voce *Autotutela I) diritto amministrativo*, in *Enciclopedia giuridica*, vol. V, Roma, 1988, 1 ss. Più di recente cfr. G. Corso, *Autotutela (dir. amm.)*, in S. Cassese (a cura di), *Dizionario di diritto pubblico*, I, Milano, 2006, 609 ss.; B.G. Mattarella, *Autotutela amministrativa e principio di legalità*, in *Rivista italiana di diritto pubblico comunitario*, 6, 2007, 1226 ss.; F. Francario, *Autotutela amministrativa e principio di legalità* (nota a margine della l. 124/2015), in *Federalismi.it,* 20, 2015, 1 ss.; Id., *Riesercizio del potere amministrativo e stabilità degli effetti giuridici*, in *Federalismi.it*, 8, 2017, 1 ss.; M. Macchia, *Sui poteri di autotutela: una riforma in senso giustiziale*, in *Giornale di diritto amministrativo*, 5, 2015, 634 ss.; P.L. Portaluri, *Il nuovo diritto procedimentale nella riforma della p.A. L'autotutela (profili interni e comunitari)*, in *Federalismi.it,* 20, 2016, 1 ss.; M.A. Sandulli, *Autotutela e stabilità del provvedimento nel prisma del diritto europeo*, in P.L. Portaluri (a cura di), *L'Amministrazione pubblica nella prospettiva del cambiamento: il codice dei contratti e la riforma Madia*, Napoli, 2016, 125 ss.

[46] Così, P. Otranto, *Dalla funzione amministrativa giustiziale alle ADR di diritto pubblico. L'esperienza dei* dispute boards *e del collegio consultivo tecnico*, Napoli, 2023, 185 ss., cui si rinvia anche per i riferimenti bibliografici essenziali. Cfr., altresì, M. Trimarchi, *L'inesauribilità del potere. Profili critici*, Napoli, 2018.

[47] Considerati i numerosi studi sul tema cfr., tra i più recenti, G. Guzzardo, *Annullamento d'ufficio e comunicazione di avvio del procedimento* (nota a Tar Lombardia, sez. III, 16 gennaio 2006, n. 50), in *Foro amministrativo-T.A.R.*, 2007, 839 ss.; S. D'ancona, *L'annullamento d'ufficio tra vincoli e discrezionalità*, Napoli, 2015; M. Ramajoli, *L'annullamento d'ufficio alla ricerca di un punto di equilibrio*, in *Rivista giuridica di Urbanistica*, 2016, 112 ss.; M. Allena, *L'annullamento d'ufficio. Dall'autotutela alla tutela*, Napoli, 2018; C. Napolitano, *L'autotutela amministrativa. Nuovi paradigmi e modelli europei*, Napoli, 2018.

attuativa inverata dagli istituti che garantiscono la partecipazione, tale peculiare connotazione della funzione nella sua forma procedimentale, non potrà certo venir meno per il sol fatto che il provvedimento di secondo grado abbia ad oggetto un atto ad elaborazione elettronica. Parte della dottrina, infatti, privilegiando le tesi volontaristico-provvedimentali del programma informatico, è giunta a ritenere che l'esercizio dei poteri di autotutela, nei casi in cui abbia ad oggetto provvedimenti automatizzati, assuma "fattezze specifiche e talvolta derogatorie del modello generale"[48], nonché le caratteristiche di una funzione "vincolata" che si rende doverosa ogni qual volta sia necessario correggere il vizio consistente in errori computazionali del programma informatico.
Ricostruendo in tali termini il potere di riesame rispetto a provvedimenti (totalmente o parzialmente) automatizzati, dovrebbe affermarsi che – a fronte di un'autotutela non solo doverosa nell'*an* ma addirittura vincolata nei suoi esiti – non vi sarebbe spazio per il rispetto delle garanzie procedimentali e per la valutazione degli interessi attinti dal provvedimento di secondo grado[49] con evidente ed implicita de-quotazione, operata in via interpretativa, delle guarentigie offerte dalla legge sul procedimento.
Simili prospettive ricostruttive, però, paiono porsi in effettivo contrasto con i principi elaborati dalla scienza giuridica sulla scorta del dato positivo e con i più recenti pronunciamenti giurisprudenziali che escludono ogni possibile "sacrificio" degli istituti partecipativi "sull'altare dell'automazione". Sul punto si richiama il costante riferimento alla "riserva di umanità"[50] che deve sovrintendere all'esercizio della funzione amministrativa, a salvaguardia di quel complesso di prerogative che informano il rapporto collaborativo tra Amministrazione e cittadini. Ciò a maggior ragione può sostenersi ove si osservi che è il legislatore a fissare – attraverso quella che è stata qualificata come vera e propria norma di relazione – il parametro temporale per il ritiro di provvedimenti attributivi di vantaggi economici, sicché la stabilità dell'assetto delineato dal provvedimento amministrativo costituisce un limite all'esercizio dei ridetti poteri[51].

5. Considerazioni di sintesi

Anche nella sentenza in commento il giudice amministrativo, chiamato a supplire alle carenze del diritto positivo, pur riconoscendo i vantaggi derivanti dall'impiego di strumenti di decisione automatizzata da parte delle Amministrazioni, ha evidenziato i possibili rischi cui condurrebbe l'inosservanza dei principi già enucleati dal Consiglio

[48] Cfr. G. Gallone, *Riserva di umanità e decisioni algoritmiche*, cit., 175, che riprende le riflessioni sviluppate in A.G. Orofino-G. Gallone, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, in *Giurisprudenza italiana*, 2020, 1738.

[49] Cfr. R. Chieppa, *Provvedimenti di secondo grado (diritto amministrativo)*, *in Enciclopedia del diritto*, Annali, vol. II, Milano, 2008, 910 ss.

[50] G. Gallone, *Riserva di umanità e decisioni algoritmiche*, cit., 41 ss.

[51] Cfr. P. Otranto, *Autotutela decisoria e certezza giuridica tra ordinamento nazionale e sovranazionale*, in *Federalismi.it,* 14, 2020, 244 ss. e, ivi, gli ulteriori riferimenti bibliografici. La distinzione tra norme di azione e norme di relazione si deve, com'è noto, a E. Guicciardi, *La giustizia amministrativa*, Padova, 1942, 30 ss. Cfr., altresì, A. Romano, *Giurisdizione amministrativa e limiti della giurisdizione ordinaria*, Milano, 1975; F. Volpe, *Norme di relazione, norme d'azione e sistema italiano di giustizia amministrativa*, Padova, 2004.

di Stato in ordine alla necessaria "conoscibilità" del meccanismo informatico impiegato per la decisione, alla "comprensibilità", attraverso la traduzione della formula tecnica in regola giuridica, del funzionamento dello stesso e alla "verificabilità" della correttezza del procedimento automatizzato. Si tratta di principi che sembrano aver trovato collocazione nel nuovo codice dei contratti pubblici[52], in cui il legislatore delegato – recependo l'articolato redatto proprio dal Consiglio di Stato[53] – ha introdotto le richiamate leggi della legalità algoritmica, per come elaborate dalla giurisprudenza amministrativa[54], incentivando il ricorso da parte delle Amministrazioni all'utilizzo di procedure automatizzate (con specifico riguardo all'intero "ciclo di vita" dell'appalto) in una prospettiva di efficienza e semplificazione dell'attività amministrativa.

E tuttavia, se nella lettura della sentenza si opera uno sforzo volto a identificare gli argomenti su cui il Tar Campania fonda la propria decisione distinguendoli dalle considerazioni, ormai quasi tralatizie, del giudice amministrativo sull'amministrazione per algoritmi, ci si avvede della modesta innovatività della pronuncia. A ben vedere, infatti, il provvedimento di secondo grado è dichiarato illegittimo per difetto di motivazione sussistente sia in relazione alla mancata indicazione delle ragioni giuridiche poste a fondamento della decisione, sia in riferimento alla non conoscibilità (e non spiegabilità) dell'algoritmo e del programma che ne costituisce la traduzione in linguaggio macchina.

Come si è innanzi osservato una compiuta riflessione sulla natura giuridica del programma (e dell'algoritmo sul quale esso si fonda) è indispensabile per ricostruire i tratti

[52] Cfr. art. 30, d.lgs. 36/2023, che espressamente prevede: «1. Per migliorare l'efficienza le stazioni appaltanti e gli enti concedenti provvedono, ove possibile, ad automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse l'intelligenza artificiale e le tecnologie di registri distribuiti, nel rispetto delle specifiche disposizioni in materia. 2. Nell'acquisto o sviluppo delle soluzioni di cui al comma 1 le stazioni appaltanti e gli enti concedenti: a) assicurano la disponibilità del codice sorgente, della relativa documentazione, nonché di ogni altro elemento utile a comprenderne le logiche di funzionamento; b) introducono negli atti di indizione delle gare clausole volte ad assicurare le prestazioni di assistenza e manutenzione necessarie alla correzione degli errori e degli effetti indesiderati derivanti dall'automazione. 3. Le decisioni assunte mediante automazione rispettano i principi di: a) conoscibilità e comprensibilità, per cui ogni operatore economico ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e, in tal caso, a ricevere informazioni significative sulla logica utilizzata; b) non esclusività della decisione algoritmica, per cui comunque esiste nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata; c) non discriminazione algoritmica, per cui il titolare mette in atto misure tecniche e organizzative adeguate al fine di impedire effetti discriminatori nei confronti degli operatori economici. 4. Le stazioni appaltanti e gli enti concedenti adottano ogni misura tecnica e organizzativa atta a garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, nonché a impedire effetti discriminatori nei confronti di persone fisiche sulla base della nazionalità, dell'origine etnica, delle opinioni politiche, della religione, delle convinzioni personali, dell'appartenenza sindacale, dei caratteri somatici, dello status genetico, dello stato di salute, del genere o dell'orientamento sessuale. 5. Le pubbliche amministrazioni pubblicano sul sito istituzionale, nella sezione "Amministrazione trasparente", l'elenco delle soluzioni tecnologiche di cui al comma 1 utilizzate ai fini dello svolgimento della propria attività».

[53] È il caso di ricordare che il Governo – esercitando la facoltà prevista dall'art. 14, n. 2, r.d. 26 giugno 1924, n. 1054, espressamente richiamato anche dall'art. 1, c. 4, l. 78/2022 − ha affidato al Consiglio di Stato il compito di redigere una proposta di articolato normativo del nuovo codice. Lo schema definitivo del codice è stato licenziato dal Consiglio di Stato il 7 dicembre 2022 ed è stato sostanzialmente recepito, quasi senza modifiche, attraverso il d.lgs. 36/2023.

[54] Cfr. *supra* par. 3, nota 26 e 27.

peculiari dell'atto amministrativo (in tutto o in parte) automatizzato. Ciò in relazione, per esempio, alla avvertita necessità di delineare percorsi ermeneutici che consentano la piena operatività dei principi individuati dalla giurisprudenza[55] e, prima ancora, delle regole che informano l'azione amministrativa.

Può osservarsi – come mero spunto di riflessione da approfondire in una successiva ricerca – che ove si riconoscesse al programma la natura di atto amministrativo presupposto, le garanzie procedimentali potrebbero trovare adeguata considerazione non solo (e non tanto) nel singolo procedimento che conduce all'adozione del provvedimento automatizzato, quanto piuttosto nella fase di studio che precede la elaborazione dell'algoritmo e del programma e, dunque, la traduzione in linguaggio intellegibile dalla macchina dei principi e delle regole che devono sovrintendere all'adozione dei provvedimenti (amministrativi) automatizzati[56]. In altri termini, il ricorso alla funzione amministrativa automatizzata (a mezzo di algoritmi o sistemi di intelligenza artificiale) non può di per sé considerarsi legittima, essendo necessario dimostrare, sulla base dei criteri adoperati nella procedura, il rispetto delle regole che informano l'attività amministrativa.

Con riguardo, invece, ai rapporti tra decisione algoritmica e procedimento di secondo grado, l'utilizzo di siffatti moduli decisori non dovrebbe poter condurre ad un (nuovo) allargamento delle maglie del potere di autotutela decisoria che spetta sì all'Amministrazione, ma che deve essere esercitato nel rispetto dei limiti e delle garanzie di trasparenza poste a presidio del legittimo affidamento dei privati e, con esso, della certezza dei rapporti giuridici.

Rispetto ai provvedimenti automatizzati di secondo grado si pongono problemi analoghi a quelli dei provvedimenti adottati in prima battuta quanto, ad esempio, alla tutela delle garanzie partecipative degli interessati. Con un non trascurabile differenza: attraverso il provvedimento di annullamento d'ufficio l'Amministrazione torna sui propri passi e, in nome dell'interesse pubblico in concreto e del principio di legalità, priva di effetti un proprio provvedimento con il quale aveva già deciso una determinata situazione, contribuendo a creare non solo affidamento in capo al destinatario dell'atto, ma anche certezza giuridica a beneficio dell'ordinamento. Ne deriva che particolarmente accurata dovrebbe essere la costruzione degli algoritmi posti a fondamento dei provvedimenti di secondo grado e massima, dunque, dovrebbe essere l'attenzione delle Amministrazioni nell'offrire (in termini di effettività) agli interessati (o, eventualmente, ad associazioni o enti esponenziali dei relativi interessi) la possibilità di partecipare al relativo procedimento.

In definitiva, se il ricorso a decisioni amministrative automatizzate non è più qualificabile (di fatto) come una mera opzione per le Amministrazioni candidandosi a divenirne il modulo ordinario per l'esercizio delle funzioni, non può più ritenersi derogabile l'esigenza di chiarire se ed entro quali termini le regole e i principi costruiti intorno ai

[55] Cfr. G. Avanzini, *Decisioni amministrative e algoritmi informatici*. cit., 120 ss. Cfr., altresì, C. Strainati, *Algoritmi e decisioni amministrative*, in *Foro amministrativo*, 2020, 1591 ss.; B. Marchetti, *Amministrazione digitale*, cit., 75 ss.

[56] Tanto, se si considera, altresì, che nelle ricostruzioni più recenti della giurisprudenza il rispetto dei principi dell'azione amministrativa assurge non di meno a parametro di legittimità dell'attività automatizzata. Cfr., da ultimo, Trib. Trani, sez. lavoro, 31 gennaio 2023, n. 2210.

provvedimenti espressione della decisione umana siano compatibili con una realtà nella quale la decisione è sovente affidata alla macchina[57]. Pur confidando nella saggezza del giudice amministrativo, infatti, non pare che si possa delegare ancora a lungo alla giurisprudenza il compito di governare un fenomeno che non può essere ignorato né affidato a soluzioni episodiche e disorganiche[58].

[57] Cfr. G. Gallone, *Riserva di umanità e funzioni amministrative,* cit., 16, ove afferma che «non esiste più una sfera di esclusivo appannaggio dell'umano, essendo anche quella intellettuale divenuta ormai contendibile dalla macchina».

[58] Nella proposta di Regolamento UE inerente alla armonizzazione delle regole sulla intelligenza artificiale, ad esempio, si adombra la possibilità che «ciascuno Stato membro istituisce o designa autorità nazionali di vigilanza al fine di garantire l'applicazione e l'attuazione del regolamento. Le autorità nazionali competenti sono organizzate e gestite in modo che sia salvaguardata l'obiettività e l'imparzialità dei loro compiti e attività. Ciascuno Stato membro designa un'autorità nazionale di controllo tra le autorità nazionali competenti. L'autorità nazionale di controllo agisce in qualità di autorità di notifica e di autorità di vigilanza, al fine di garantire l'applicazione uniforme delle regole inerenti all'utilizzo di sistemi di intelligenza artificiale» (cfr. art. 59, capo II). Su questi profili cfr., in dottrina, F. Costantino, *Algoritmi, intelligenza artificiale e giudice amministrativo*, in *Giurisprudenza italiana*, 2022, 1527 ss.; F. Donati, *Diritti fondamentali e algoritmi nella proposta di Regolamento sull'intelligenza artificiale*, in A. Pajno-F. Donati-A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, I, Bologna, 2022, 111 ss.

Cronache

The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations*

Elena Kaiser

Abstract

This article examines the impact of the new obligations set forth in directive (EU) 2022/2555 (NIS II) on small and medium enterprises (SMEs). SMEs represent 99% of all businesses in Europe and are crucial to the Digital Single Market. However, despite their importance, these companies still lack the necessary cybersecurity measures to resist and respond to major cyberattacks.

Summary

1.Introduction. – 2. From NIS I to NIS II. – 2.1 NIS II and the size-cap rule. - 2.2. The new role of SMEs in the directive. - 3. What are the new obligations for SMEs falling under the scope of the directive?. - 3.1. Cybersecurity risk management measures. - 3.2 Reporting obligations. – 3.3 Penalties and enforcement measures. – 4. Impact and costs of the new directive on SMEs: initial considerations. – 5. ENISA's role and SMEs. – 6. Conclusions

Keywords

NIS directive – security of network and information systems – small and medium enterprises (SMEs) – impact

1. Introduction

Small and medium enterprises (SMEs), which represent 99% of all businesses in the European Union, are the backbone of the Digital Single Market.[1]
According to the definition given by Eurostat, small enterprises are defined as entities

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

[1] Eurostat, *EU small and medium-sized enterprises: an overview*, in *ec.europa.eu*. In 2018 there were approximately 25 million SMEs in the European Union. See ENISA, *Cybersecurity for SMEs - Challenges and Recommendations*, 2021, in *enisa.europa.eu*, 2021, 9.

having fewer than 50 employees and an annual turnover of less than or equal to €10 million. In contrast, medium-sized companies are defined as having a maximum of 250 employees and a yearly turnover of less than or equal to €50 million.[2] Finally, entities with less than 10 employees and an annual turnover of less than or equal to €2 million are considered micro-enterprises.

Despite their importance in the economic market, most SMEs still need to improve their cybersecurity capacities. According to surveys conducted by the European Commission analyzing the impact of the EU directive concerning the security of network and information systems (NIS I Directive) on entities within the EU, only 27% of small enterprises had an ICT cybersecurity policy in place, compared to 51% of medium enterprises and 72% of large enterprises[3].

SMEs are often targeted by cybercriminals due to low cybersecurity awareness and inadequate incident response programs, which make them easy targets for attacks. Contrary to the common belief that cyber-attacks only occur in large organizations, SMEs may be crucial components of broader supply chains or provide services to critical entities[4]. Additionally, most SMEs process critical information, defined as «information that if it is stolen or lost, the organization would face serious legal repercussion, and the owners of the personal information could encounter significant or even irreversible consequences (...)».[5]

This article provides some initial considerations on how the new European directive concerning the security of network and information systems (NIS II Directive)[6] will affect SMEs. The NIS II was adopted by the European Council on December 14, 2022 and came into force on January 16, 2023. The new legal framework broadens its scope and introduces new compliance obligations and notification requirements, which will be discussed in the following paragraphs.

It is essential to highlight that the NIS II Directive still needs to be implemented at the national level by Member States, as required by European law. Due to the current early stages of the directive's implementation, it can be challenging to obtain a complete and precise overview of the costs and impact on the entities falling under its scope.

The impact assessment will be supported by the documents drafted by the European Commission accompanying the negotiation of the new directive, and by evidence gathered from reports and other initiatives supported by the European Union Agency for Cybersecurity (ENISA).

---

[2] European Commission, *SME*, in *single-market-economy, ec.europa.eu/smes/sme-definition_en.*

[3] G. Endrodi - G. Maridis - S. Schmitz, et. al., *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)*, 2021, 97, in *data.europa.eu.*

[4] ENISA, *Cybersecurity for SMEs - Challenges and Recommendations,* 2021, 8, in *enisa.europa.eu.*

[5] Ivi, 12.

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 /NIS 2 Directive).

2. From NIS I to NIS II

On July 6, 2016, the European Parliament approved the NIS Directive (EU) 2016/1148[7], which is the first horizontal legal instrument aimed at improving cybersecurity resilience in the European internal market. The directive imposes new obligations on Member States to adopt a national cybersecurity strategy, designate one or more national cybersecurity incident response teams (CSIRTs), establish a competent national authority to implement and supervise the directive and appoint a single point of contact for transnational cooperation. Additionally, to promote swift and effective operational cooperation among Member States, including information sharing, the directive establishes a network of national CSIRTs. Finally, it introduces new security and notification requirements.

Regarding its scope, the NIS I Directive distinguishes between "operators of essential services" and "digital service providers". Operators of essential services (OES) are those that belong to sectors and subsectors listed in Annex II, such as energy, transport, banking, financial market infrastructures, health sector, water, and digital infrastructures, and that meet the following criteria: a) providing a service that is essential for the maintenance of critical societal and economic activities; b) the provision of that service depends on network and information systems; c) an incident would have significant disruptive effects on the provision of that service.[8] On the contrary, digital service providers (DSPs) are legal entities that provide digital services listed in Annex III, such as online marketplaces, online search engines, and cloud computing services. Member States bear the responsibility of identifying OESs operating within their territories.[9] However, the NIS Directive fails to provide any precise mechanism to identify such OESs or establish standard criteria based on their size.[10] Additionally, Member States are not obligated to identify DSPs. As a result, some entities that play an essential role in the digital market and which certain OESs rely on to provide their services, such as cloud service providers, are beyond the scope of competent national authorities' supervision.

The lack of an identification procedure for OESs and DSPs reflects the minimum harmonization criterion, which the directive adopts as a general approach for all its obligations and mechanisms.

The NIS I sets only generic objectives, giving Member States the freedom to choose measures to adopt at the national level to achieve these goals. However, this broad discretion led to inconsistent and inefficient implementation of the directive among Member States.

Besides the aforementioned issues with identifying OESs and DSPs, other critical

[7] 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.

[8] Art. 5, directive (EU) 2016/1148.

[9] According to art. 5, para. 1, directive (EU) 2016/1148, by 9 November 2018, Member States shall identify the operators of essential services with an establishment on their territory for each sector and subsector referred to in Annex II.

[10] See also T. Sievers, *Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligation*, in *International Cybersecurity Law Review*, 2021, 225-226.

issues have emerged concerning the incident notification and sanction system. For instance, the lack of specific parameters for measuring "the significance or substance of an incident" that triggers the notification obligations to competent authorities or CSIRTs, has contributed to underreporting of incidents and a lack of coordinated crisis response.[11]

Additionally, non-specified security obligations have resulted in inconsistent levels of cybersecurity awareness and resilience across Member States and sectors. Finally, the penalty system has been undetermined[12]: penalties for non-compliance with the provisions of the NIS Directive have differed significantly among Member States and, in some cases, were almost non-existent.[13]

Furthermore, the digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape with increased and more sophisticated attacks originating from both within and outside the European Union. The cybersecurity directive has been incapable of addressing these new challenges.[14]

The necessity to harmonize the NIS Directive and its insufficiency in dealing with emerging cyber threats made it imperative to adopt a new legal text to enhance and ensure cybersecurity resilience within the European Union. The Council of the European Union approved the final text of the NIS II Directive in December 2022, and it came into force on 16 January 2023. This new regulatory framework, along with the Critical Entities Resilience (CER) Directive[15], is a crucial policy pillar of the so-called "European Cybersecurity Strategy for the Digital Decade".[16]

2.1 NIS II and the size-cap rule

While NIS I differentiated between operators of essential services and digital service providers, the recently approved NIS II replaces these categories with essential and important services and significantly expands the list of entities and sectors falling under its scope.

The method of supervision, kept from the previous directive, is the main distinguishing factor between essential and important entities: for the first category, the control

[11] G. Endrodi - G. Maridis - S. Schmitz, et. al., *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive*), cit., 46.

[12] Art. 21, directive (EU) 2016/1148, only indicates that penalties shall be effective, proportionate, and dissuasive.

[13] G. Endrodi - G. Maridis - S. Schmitz, et. al., *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive*), cit., 54 ss.

[14] Commission Staff working document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

[15] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[16] European Commission, *The EU's Cybersecurity Strategy for the Digital Decade*, 16 December 2020, in *digital-strategy.ec.europa.eu*.

is more rigorous and covers both *ex ante* and *ex post* aspects. In contrast, for important entities, supervisory powers intervene only when there is evidence that the organization did not comply with its risk management and notification obligations (*ex post*).[17]
Unlike the NIS I Directive, which allowed Member States to determine the entities recognized as OES, the new NIS II Directive introduces a unique criterion based on the size of the entity, known as the "size-cap" rule. According to this rule, all medium and large entities operating in sectors or providing services listed in Annex I and II of the directive fall within its scope by default.
Furthermore, companies must determine for themselves whether they are essential or important entities, "as a determination made by the national competent authority (NCA) is no longer required".[18]
As for the size threshold, the directive is clear: it applies to entities that meet or exceed the thresholds for medium-sized enterprises.[19] Consequently, micro and small enterprises are, generally, excluded from its scope.
However, there are broad exceptions to this criterion. According to art. 2, the directive always applies, regardless of the size, to providers of public electronic communications networks or publicly available electronic communications services[20], trust service providers, top-level domain name registries, or system service providers.
In addition, national authorities can identify also micro and small entities as essential or important if they are the only service provider, have a significant impact on public safety and security, perform a vital function for society, or are important at the national or regional level. Public administrations can also be identified as essential or important, regardless of their size, if they are central governments or provide significant services.
Finally, the exemption also applies to entities identified as critical according to the CER Directive and to entities providing domain name registration services.
Based on these elements of analysis, the list of entities that may be considered essential or important is much broader than in the past, and it may even include entities such as public administrations that were entirely excluded from the scope of the previous directive.
While NIS I did not explicitly mention size criteria for its applicability, certain SMEs, particularly those of medium size, were already deemed operators of essential services by the competent national authorities of Member States, primarily in smaller European countries. However, the establishment of medium size as the general criterion

[17] Artt. 32 and 33, directive (EU) 2022/2555.

[18] T. Sievers, *Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligation*, cit., 226.

[19] Art. 2, para. 1, directive (EU) 2022/2555.

[20] Providers of public electronic communications networks or publicly available communications services are already subject to regulation under the European Electronic Communication Code (directive (EU) 2018/1972) which includes high-security standards. Similarly, trust service providers would be exempt from the size cap rule as some security standards are already implemented within the eIDAS framework (regulation (EU) 910/2014). Excluding micro and small providers from the NIS scope may have a negative impact on these existing standards.

under NIS II may substantially expand the number of entities subject to new cybersecurity compliance obligations, potentially resulting in increased costs and burdens that may prove challenging to manage.

2.2 The new role of SMEs in the directive

As mentioned earlier, the size of an entity was not a criterion for applying or excluding NIS I. Therefore, even though some SMEs were playing critical roles as digital service providers in certain Member States, the previous directive did not make any explicit reference to them. The only exception is contained in Recital 40, which states that «Information about incidents is increasingly valuable to the general public and businesses, particularly small and medium-sized enterprises».

On the contrary, NIS II recognizes that strengthening the cyber resilience and cyber hygiene baseline of SMEs, especially those excluded from the directive's scope, is a key policy element that must be addressed in the national cybersecurity strategies of Member States. In particular, resilience shall be strengthened by providing «easily accessible guidance and assistance for their specific needs».[21] In order to assist small and medium-sized enterprises in tackling their cybersecurity challenges, Member States should implement a range of measures, including the establishment of a national point of contact and the provision of operational services such as website configuration and logging.[22]

As per the new directive, the European Union Agency for Cybersecurity (ENISA) is responsible for evaluating the cybersecurity awareness level among small and medium-sized enterprises at the European level. The findings of this research will be included in the biennial report on the status of cybersecurity in the Union, which is prepared in collaboration with the European Commission and the Cooperation Group and presented to the European Parliament.[23]

3. What are the new obligations for SMEs falling under the directive's scope?

Alongside the new categorization of essential and important entities and a broader area of application, the NIS II established new obligations and cooperation mechanisms.

The new principles and obligations established by NIS II are numerous and complex. Therefore, it is crucial to ensure that Member States, as well as essential and important entities falling under the new legal framework, have the necessary resources to comply with them.

NIS II introduces a new crisis management framework (art. 9), new tasks and require-

[21] Art. 7, part. 2, lett. i), directive (EU) 2022/2555.

[22] Recital 56, directive (EU) 2022/2555. See also ENISA, *Cybersecurity for SMEs, Challenges and Recommendations*, cit., 14 ss.

[23] Art. 18, para. 1, lett. c), directive (EU) 2022/2555.

ments for national CSIRTs (art. 11), a coordinated vulnerability disclosure mechanism (art. 12), and the European Cyber Crisis Liaison Organization Network (EU-CyCLONe) for the management of large-scale European cybersecurity incidents (art.16). However, these new obligations mainly impact national authorities, CSIRTs, and all entities in charge of crisis management.

On the other hand, essential and important entities, which may also include SMEs, are obligated to comply with risk management measures and reporting obligations.

While art. 14 of NIS I generally referred to «security requirements and incident notifications», the new text dedicates the entire Chapter IV to «Risk management measures and reporting obligations», which includes five articles: governance, cybersecurity risk management measures, coordinated security risk assessment of supply chains, reporting obligations, and the use of European cybersecurity certification schemes.

According to NIS I, operators of essential services and digital service providers should take appropriate and proportionate technical and organizational measures to manage risks posed to the security of network and information systems and adopt proper measures to mitigate the impact of incidents affecting the security of such systems.[24] In addition, OESs and DSPs were required to promptly notify the competent authority or the national CSIRT if they experience incidents that had a significant impact on the continuity of essential services or that substantially affect the provision of their online marketplace, online search engine, or cloud computing service within the Union. The criteria used to assess whether an incident was of significant or substantial impact could include the number of affected users, the incident's duration, and the geographical extent.[25]

However, as highlighted above, such obligations were too undetermined. As a consequence, security requirements differed significantly across Member States. Additionally, the lack of understanding regarding the time and notification process, as well as the threshold triggering it, led to many unreported incidents.[26]

[24] Art. 14, paras. 1 and 2; art. 16, paras. 1 and 2, directive (EU) 2016/1148.

[25] Art. 14, paras. 3 and 4; art. 16, paras. 3 and 4, directive (EU) 2016/1148.

[26] Although the Cooperation Group provided guidelines on the security requirements and notification mechanisms for both OESs and DSPs, Member States adopted different approaches, resulting in varying levels of security and a lack of harmonization in incident response. Reference document on security measures for Operators of Essential Services, available at *digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group*. G. Endrodi - G. Maridis - S. Schmitz, et. al., *Study to support the review of Directive (EU) 2016/1148 concerning measures foir a high common level of security of network and information systems across the Union (NIS Directive)*, cit., 15. Additional elements to determine security requirements and the substantial effect of a cybersecurity incident for digital service providers are provided by the European Commission Implementing Regulation 2018/151 of 30 January 2018 laying down rules for application of directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact. See also D. Markopoulou - V. Papakonstantinou - P. de Hert, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, in *Computer Law & Security Review*, 2019, 4.

3.1. Cybersecurity risk management measures

In line with the previous directive, art. 21, para. 1, NIS II establishes that security measures should be adopted to manage and mitigate risks posed to the security of network and information systems and to prevent and minimize the impact of incidents. «The main objective of these measures should be to ensure the continuity of such services».[27]

The novelty lies in para. 2 of art. 21, which outlines a detailed list of minimum measures that entities must adopt. This list of criteria can contribute to a more harmonized approach among Member States, which was missing in the previous directive, and promote generalized cyber resilience among all entities operating in the European Union. The required cybersecurity measures include a) conducting risk analysis and developing information system policies establishing; b) incident handling procedures; c) implementing backup and crisis management plans, ensuring disaster recovery to maintain business continuity; d) securing the supply chain; e) ensuring network and information system security during acquisition, development, and maintenance, including vulnerability handling; f) establishing policies and procedures to assess the effectiveness of cybersecurity risk-management measures; g) promoting basic cyber hygiene practices; (h) implementing policies and procedures for the use of cryptography and encryption; (i) human resources security and (j) multi-factor authentication. Failure to comply with these measures may result in the adoption of necessary, appropriate, and proportionate corrective measures by Member States.[28]

The utilization of ICT products, services, and processes that hold cybersecurity certification under the provisions of regulation (EU) 2019/881 (also known as the Cybersecurity Act) is a means to exhibit conformity with the aforementioned obligations.[29]

3.2 Reporting obligations

Art. 23 of the new directive sets out comprehensive reporting obligations for essential and important entities, which entail specific timelines, content requirements, and the involvement of CSIRTs in the reporting process. This reporting mechanism bears similarities to the one described in art. 33 of the General Data Protection Regulation (GDPR).[30]

States must promptly notify CSIRTs or the competent authorities of incidents that significantly affect the provision of their services. An incident qualifies as having a significant impact if it has resulted in or could result in severe operational disruption

[27] D. Markopoulou - V. Papakonstantinou - P. de Hert, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, cit., 3.

[28] Art. 21, para. 4, directive (EU) 2022/2555.

[29] Art. 24, paras. 1 and 2., directive (EU) 2022/2555.

[30] 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.

of the services or financial loss for the concerned entity, or if it has caused or could cause considerable material or non-material damage to other natural or legal persons.
An entity affected by a cybersecurity incident that causes a significant impact must provide the CSIRT or competent authority with the following:
a) An early warning, indicating whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact. This warning must be provided without undue delay and, in any event, within 24 hours.
b) An incident notification within 72 hours of becoming aware of the significant incident. The notification should include an initial assessment of the incident's severity and impact.
c) An intermediate report upon request of the CSIRT.
d) A final report not later than one month after the incident notification submission. The final report should include a detailed description of the incident, the type of threat or root cause likely to have triggered the incident, mitigation measures that have been applied, where applicable, and the cross-border impact of the incident.
Upon receiving the early warning, the CSIRT or competent authority shall provide, where possible, a response to the notifying entity within 24 hours, including initial feedback and, upon request, operational advice on possible mitigation measures.
Moreover, both essential and important entities, as well as entities that are not covered by this directive, can always voluntarily report any significant incidents, cyber threats, or near misses.[31]

3.3 Penalties and enforcement measures

Art. 34 of the NIS II introduces a sanction scheme that provides maximum penalties for non-compliance with the directive obligations, similar to what is already done in the GDPR. In contrast, the previous directive delegated Member States to adopt rules on infringements of national laws transposing the directive and imposed a general obligation for these measures to be effective, persuasive, and dissuasive. As noted above, penalties for non-compliance with the NIS Directive varied greatly among Member States in both characteristics and severity.
The NIS II Directive sets the threshold for administrative fines that Member States must impose on essential and important entities that fail to comply with cybersecurity measures and reporting obligations.
Non-compliance with art. 21, which concerns cybersecurity risk-management measures, and art. 23, which concerns reporting obligations, results in:
For essential entities: an administrative fine of a maximum of at least EUR 10 000 000 or a maximum of at least 2% of the total worldwide annual turnover.
For important entities: an administrative fine of a maximum of at least EUR 7.000.000 or a maximum of at least 1,4% of the total worldwide annual turnover[32].
If we compare these figures with the average financial capacity of small and medium

[31] Art. 30, para. 1, lett. a) - b), directive (EU) 2022/2555.

[32] Art. 34, paras. 4 and 5, directive (EU) 2022/2555.

size businesses, it becomes evident that these new penalties are significantly high and can have a considerable impact on their business continuity.
Besides administrative fines, essential and important entities are also subjected to supervisory and enforcement measures by competent national authorities, which can also lead to adopting corrective measures and administrative fines.
As mentioned above, for essential entities, the supervision is both *ex ante* and *ex post*, while for the important entities, it is only *ex post*. This different method of supervision is kept from the previous directive. Supervisory tasks include on-site inspections, regular and target security audits, or requests to access data[33].
If the supervisory activities described above ascertain any violation of the obligations laid down by the directive, competent authorities also exercise enforcement powers to ensure compliance with such obligations. According to arts. 32 and 33, these measures include warnings about infringements; orders of ceasing conducts infringing the directive; orders of compliance with cybersecurity risk-management measures and reporting obligations; orders of providing information to the natural or legal persons potentially affected by a cyber threat; orders of designating a monitoring officer to oversee the compliance of cybersecurity risk-management measures and of reporting obligations. Finally, competent national authorities may impose or request relevant bodies or tribunals to impose administrative fines under art. 34 NIS II Directive.

4. Impact and costs of the new directive on SMEs: initial considerations

Due to the broader scope of the new directive, which includes sectors and entities that were previously excluded from the application of NIS II, and the numerous exceptions to the size-cap rule, more companies, including micro and small, will have to comply with European obligations. At the same time, according to the general rule established by art. 2, it is expected that new medium-sized enterprises will have to comply with the obligations established by NIS II.
As a general rule, small and micro enterprises are explicitly excluded from the scope of the directive. However, Member States may choose to extend the directive's scope to include those that are deemed critical to the functioning of essential services. In such cases, the costs and impact of NIS on small and micro enterprises will need to be carefully evaluated to ensure that the benefits outweigh the costs.
While micro-enterprises rarely provide public electronic communication networks, trust services providers, or other essential and important services to a country, except for some small Member States, small and medium enterprises may provide essential services and even become suppliers of critical entities.
It is widely known that in the technological sector, the size of an organization does not necessarily reflect its importance in a particular economy or the quantity and relevance of the data it processes.
Additionally, SMEs can play a crucial role in supply chains. In this regard, essential

[33] Artt. 32 and 33, directive (EU) 2022/2555.

concerns have been raised during the negotiation process of the NIS II Directive. In particular, the European DIGITAL SME Alliance has stated that:
«While the NIS2 directive excludes small and micro enterprises from having to comply with the directive, the need for supply chain security and the requirement for entities to ensure that their supply chains and service providers are cybersecurity could lead to small and micro enterprises having to prove compliance with the directive, in order to retain business relationships. The forthcoming risk assessment should ensure that security requirements for service providers and manufacturers in the supply remain proportionate and realistic, relative to the level of threat and vulnerability (...)».[34]
It is, therefore, of utmost importance to support not only micro and small entities that will fall within the scope of the directive but also those that will be excluded from it and, as a result, are precluded from awareness campaigns, projects, and funding.
The NIS II tasks the European Commission, in cooperation with the Cooperation Group, to provide guidelines to SMEs to assess whether they fall within the directive's scope and to support them in this regard.[35] However, as the NIS II text has only recently entered into force and still needs to be implemented by Member States through national legislation, it is presumed that these guidelines will be provided in the coming months.
Various assessment reports conducted by the European Commission, which accompanied the proposal for the new directive[36], highlighted an insufficient application of cyber resilience and risk management practices by SMEs. Small companies often lacked financial and human resources, staff, and awareness to provide adequate cybersecurity. The concern with a small company arose mainly when they had access to or relate to more significant targets, thus becoming vectors for cyber-attacks on more critical targets.[37]
According to another survey carried out by ENISA, many SMEs already had some cybersecurity measures in place even before the COVID-19 crisis, which heavily impacted their business continuity and exposed them to new risks mainly due to remote working. However, such measures were mostly basic technical controls, such as antivirus software.[38] Notwithstanding the low level of cybersecurity capacity, SMEs within the European Union understood that cybersecurity was an important issue and that

[34] European DIGITAL SME Alliance, *Digital SME input to the consultation of the proposal for a revised directive on the Security of Network and Information systems (NIS 2 Directive)*, in *digitalsme.eu,* 2021.

[35] Recital 20, directive (EU) 2022/2555.

[36] Parts 1, 2, 3 of the Commission Staff working document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

[37] Supply chain attacks are increasing in terms of frequency and strength. For much information concerning the threat landscape, ENISA *Threat landscape for supply chain attacks*, in *enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks*, 2021. The level of resilience and risk management practices applied by SMEs varies across different sectors. For example, the health sector, which has been significantly affected by the COVID-19 crisis, is now covered by more specific elements under NIS II (Annex I), including entities involved in research and development of medicinal products and those manufacturing medical devices. Annex I, directive (EU) 2022/2555.

[38] ENISA, *Cybersecurity for SMEs, Challenges and Recommendations*, cit., 28.

they relied on their ICT infrastructure.[39]

The European legislator shall generally require Member States to establish frameworks for raising awareness of cyber threats among SMEs and supporting them in confronting those threats. This need is reflected in art. 7 of the new NIS II Directive, which mandates national cybersecurity strategies to adopt specific policies that strengthen cyber awareness and hygiene among SMEs. However, the question remains whether this provision alone will sufficiently address all the challenges faced by SMEs in terms of cyber resilience and costs.

At this early stage, it is ambitious to assess the concrete impact and costs of NIS II on such enterprises, given that the new text entered into force only in January. Data on the number of medium and small-sized enterprises that fall under the scope of NIS as essential or important entities are, in fact, not yet available. It is also unclear how many of these companies were previously considered OESs or DSPs under NIS I and had, therefore, sufficient cybersecurity measures already in place.

It is estimated companies falling under the scope of the directive, which certainly include medium-sized enterprises, will need to increase their current ICT security spending by a maximum of 22% over the next few years[40], with compliance costs being the most significant. These costs are primarily related to fulfilling the risk management obligations outlined in art. 21, complying with reporting obligations under art. 23, and documenting compliance with supervisory and enforcement measures imposed by competent authorities.[41]

At the same time, raising the level of security requirements for these entities would also incentivize their cybersecurity capabilities and help improve their ICT risk management. However, currently, there are no comparable data available across the EU to measure the return on security investment (ROSI) at the company level, either across sectors or per sector.[42]

5. ENISA's role and SMEs

In June 2019, the European Cybersecurity Act came into force, which established a European cybersecurity certification scheme and granted a permanent mandate to the European Union Agency for Cybersecurity (ENISA).[43]

ENISA's mandate encompasses providing support to Member States and Union institutions to enhance cybersecurity and reduce internal market fragmentation[44], which

[39] Ivi, 3. According to the survey, over 80% of the SMEs stated that cybersecurity issues would seriously impact their business within a week of the problems happening, with 57% saying that they would most likely go bankrupt or go out of business.

[40] Commission Staff working document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, cit., part. ⅓., 72.

[41] Ivi, 74.

[42] Ivi, 69.

[43] Established in 2004.

[44] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on

includes assisting with the transposition of NIS I into national legislation.

The NIS II Directive has expanded ENISA's role in the network and information security context, and it is now responsible for the following:

- Developing and maintaining a European vulnerability database[45];
- Assisting in developing CSIRTs, if requested by Member States[46];
- Provide the secretariat to the CSIRTs network[47] and the EU-CyCLONe[48];
- Carrying out a coordinated security risk assessment of supply chains in cooperation with the Cooperation Group and the Commission[49];
- Developing guidance on security requirements and reporting obligations for providers of public electronic communications networks or publicly available electronic communications services to facilitate harmonization and transition[50];
- Creating and maintaining a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms[51];
- Supporting the establishment of cybersecurity information-sharing arrangements exchanging best practices and providing guidance[52].

Moreover, as part of its duties under NIS II, the European Cybersecurity Agency is responsible for producing a biennial report on the state of cybersecurity in the European Union, which includes an evaluation of the level of cybersecurity awareness and hygiene among small and medium enterprises.

Since 2006, even before the permanent mandate given by the Cybersecurity Act, the European Agency has been promoting initiatives to support SMEs and Member States in elevating their level of understanding of cybersecurity risks and threats (such as phishing and ransomware), raising awareness, and promoting best cybersecurity practices.[53]

More recently, in 2021, ENISA published a report called "Cybersecurity for SMEs -

ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

45 Art. 12, para. 2, directive (EU) 2022/2555; recital 60, directive (EU) 2022/2555.

46 Art. 10, para. 10, directive (EU) 2022/2555.

47 Art. 15, para. 2, directive (EU) 2022/2555.

48 Art. 16, para. 2, directive (EU) 2022/2555.

49 Art. 22, directive (EU) 2022/2555 ; recital 90, directive (EU) 2022/2555.

50 Recital 95, directive (EU) 2022/2555.

51 Art. 27, directive (EU) 2022/2555; recital 117, directive (EU) 2022/2555.

52 Art. 29, para. 5, directive (EU) 2022/2555.

53 Between 2006 and 2015, the Agency published several reports aimed at supporting SMEs in managing cybersecurity risks, including two Information Package for SMEs reports providing risk assessment and management methodologies, a Business Continuity for SMEs report facilitating IT knowledge transfer, and a Cloud Security Guide for SMEs report addressing security risks and opportunities related to cloud services. These reports can be accessed at *enisa.europa.eu.*

Challenges and Recommendations"[54], which advises SMEs on measures to improve their cybersecurity resilience and suggests concrete actions for Member States to support them in this process. The report highlights how the COVID-19 crisis exacerbated existing challenges and provides guidelines for mitigating them. ENISA has identified the main challenges for SMEs as low cybersecurity awareness and management support, inadequate protection for critical and sensitive information, budgetary issues, lack of ICT cybersecurity expertise and personnel, lack of appropriate guidelines.[55] The most frequent incidents experienced by SMEs include ransomware attacks on their service providers or PCs, theft of laptops, and CEO fraud[56]. The report provides recommendations addressing three main areas and levels: people, processes, and technology.

A short practical guide called "Cybersecurity Guide for SMEs" accompanies the report, providing 12 high-level steps to better secure SMEs' systems and their business.[57] In the same year, ENISA also promoted the "SecureSME-cyber tips," which provide short and practical suggestions to protect employees, enhance processes, strengthen technical measures, and overcome all issues companies had to deal with during the COVID-19 pandemic.[58] The portal includes practical videos to aid in this endeavor.

In March 2023, ENISA developed a new "Cybersecurity Maturity Assessment" tool to diagnose SMEs' cybersecurity maturity level.[59] The tool includes essential features, such as a cybersecurity evaluation based on several questions and a personalized action plan that aligns with best cybersecurity practices. Similar to the "Cybersecurity for SMEs" report, the tool focuses on the three key areas: people, technology, and processes.

6. Conclusions

In summary, the NIS II Directive imposes new obligations on a larger number of entities, including SMEs. The directive expands its scope to cover additional sectors and entities and introduces a "size-cap" rule, that sets the minimum threshold for medium and large organizations. As a result, medium-sized enterprises are now included by default in the new legal framework, while micro and small enterprises are generally excluded from its scope.

Art. 2 NIS II Directive lists exceptions where the regulatory framework applies "regardless of the size", such as when entities provide public electronic communications network services, trust services, top-level domain name registries, services with sig-

[54] ENISA, *Cybersecurity for SMEs, Challenges and Recommendations*, 2021, cit.

[55] Ivi, 14 ss.

[56] Ivi, 24 ss.

[57] ENISA, *Cybersecurity guide for SMEs, 12 steps to securing your business*, 2021, in *enisa.europa.eu.*

[58] ENISA, *Secure SME*, 2021, in *enisa.europa.eu.*

[59] ENISA, *Diagnose your SMEs Cybersecurity and Scan for Recommendations*, in *enisa.europa.eu.* See also ENISA, *Cybersecurity Maturity Assessment for Small and Medium Enterprises,* in *enisa.europa.eu.*

nificant impact on public safety and security, or perform vital functions for society. As a result, even micro and small enterprises, which are generally excluded from the directive's scope, may fall under these exceptions. Although micro-enterprises rarely provide essential services, small and medium-sized enterprises can become suppliers of critical entities, making them vulnerable to cyberattacks.

Notwithstanding their importance in the digital market, the general level of cyber awareness and incident management of SMEs is still relatively low. Based on some surveys carried out by the European Commission, only 27% of small enterprises have an ICT cybersecurity policy in place, compared to 51% of medium enterprises.

As for the impact of NIS II on micro and small-sized enterprises, there is no concrete estimation done so far. Additionally, no data is available yet on how many medium and small-sized enterprises that were considered OESs or DSPs according to the previous directive will become essential or important entities. On the contrary, for medium-sized enterprises, it can be expected that there would be an increase in their ICT security spending in the first years following the introduction of the new NIS II framework.

Several initiatives targeting and improving the cybersecurity resilience of SMEs have been promoted at the European level by ENISA. The cybersecurity agency was established in 2004 and received a permanent mandate in 2021 to support Member States and Union institutions in improving cybersecurity and reducing internal market fragmentation, including the implementation of NIS Directive obligations. New functions have been assigned to the Agency by the new directive, including carrying out security assessments of supply chains and developing guidance on security requirements and reporting obligations.

According to NIS II, cybersecurity awareness and hygiene of SMEs have also become vital policy elements that need to be addressed and implemented by Member States through their national cybersecurity strategies.

La tutela dei minori nel cyberspazio. *Parental Control* di Stato e libera circolazione dei contenuti: un delicato equilibrio*

Nicolò Biligotti

Abstract

L'art. 7-*bis*, d.l. 28/2020, rubricata "sistemi di protezione dei minori dai rischi del cyberspazio" impone agli *Internet service providers* l'obbligo di strutturare e pre-attivare gratuitamente un sistema di filtro e blocco dei contenuti ritenuti inappropriati per un pubblico minorenne. Il precetto normativo – ad oggi rimasto lettera pressoché morta, poiché non recepito (o solo parzialmente recepito, a seconda dei casi) dagli operatori di rete – è in procinto di acquisire nuovo momento in virtù delle Linee Guida emanate dall'Autorità per le Garanzie nelle Comunicazioni (AGCOM). Ai fini di una compiuta analisi dello strumento di tutela – si badi: disegnato dal legislatore alla stregua di un parental control di Stato – pare opportuno collocare il medesimo all'interno del più ampio contesto normativo dedicato alla disciplina del cyberspazio, così da valutare le potenzialità della soluzione proposta nel panorama dei principi generali che regolano la materia

Art. 7-*bis,* Law Decree no. 28/2020, on "systems to protect minors from the risks of cyberspace", imposes an obligation on Internet service providers to structure and pre-activate, free of charge, a system for filtering and blocking content deemed inappropriate for a minor audience. The regulatory provision – which to date has remained an almost dead letter, as it has not been implemented (or only partially implemented, as the case may be) by network operators – is about to gain new momentum by virtue of the Guidelines issued by the Italian Authority for Communications (AGCOM). For the purposes of a full analysis of the protection instrument – note: designed by the legislator in the manner of a State parental control – it seems appropriate to place the same within the broader regulatory context dedicated to the regulation of cyberspace, so as to assess the potential of the proposed solution in the scenario of the general principles governing the matter.

*Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Nicolò Biligotti

Sommario

Premessa e sintesi dei contenuti. – 1. La libertà di espressione nel cyberspazio: una libertà fondamentale – 2. La libertà di espressione nel cyberspazio: una libertà fondamentale messa a dura prova dall'evoluzione del *web* – 3. *Parental control* di Stato: art. 7-*bis,* d.l. 28/2020 e delibera AGCOM n. 9/23.

Keywords

AGCOM - Tutela minori - Libertà di espressione - Cyberspazio - Parental Control.

Premessa e sintesi dei contenuti

Qualora si adotti una definizione ampia di cyberspazio – lo spazio concettuale in cui si svolgono interazioni mediate da dispositivi informatici – la presenza di molteplici pericoli per lo sviluppo psico-sociale dei minori si impone ad oggi come evidenza empirica: *fake news*, cyberbullismo, *hate speech*, incitamento ad atti autolesionisti (specie in forma di *challenges*), pornografia e promozione di droghe forniscono soltanto una prima approssimazione delle minacce esplicite rivolte dal *web* al benessere psico-fisico dei minorenni, e a queste deve essere aggiunta l'incognita rappresentata dalla esposizione ai contenuti tipici dei *social network* (rapidi ed immediati, spesso di impronta narcisista, scientificamente programmati per indurre assuefazione e autoalimentarsi in casse di risonanza algoritmiche, non da ultimo a fini commerciali).

Le insidie del *web 2.0* non sono certo rivolte in via esclusiva ai soggetti di minore età: i primi decenni di vita del fenomeno hanno ben evidenziato la necessità (e la materiale possibilità) di strutturare – a beneficio di tutti gli utenti, seppur adulti – un quadro normativo volto a promuovere il libero sviluppo del cyberspazio nella repressione giuridica dei contenuti di natura illecita. Ciò che, tuttavia, contraddistingue la posizione dei minorenni è la loro intrinseca vulnerabilità: una caratteristica di categoria che impone una riflessione circa l'opportunità di conferire loro uno strato di protezione ulteriore; protezione necessariamente peculiare, sia in ragione di contenuti resi patologici dalla minore età e invece fisiologici per adulti, sia in ragione dei significativi danni individuali riportabili da soggetti ontologicamente fragili.

L'opportunità – acuita dal più stretto contatto tra minori e cyberspazio indotto dallo scenario pandemico – è stata colta dal legislatore italiano nell'aprile 2020 con l'introduzione dell'art. 7-*bis* d.l. 28/2020: rubricata «sistemi di protezione dei minori dai rischi del cyberspazio», la disposizione normativa impone agli *Internet service providers* l'obbligo di strutturare e pre-attivare gratuitamente un sistema di filtro e blocco dei contenuti ritenuti inappropriati per un pubblico minorenne. Il precetto normativo – ad oggi rimasto lettera pressoché morta, poiché non recepito (o solo parzialmente recepito, a seconda dei casi) dagli operatori di rete – è in procinto di acquisire nuovo momento in virtù delle Linee Guida emanate dall'Autorità per le Garanzie nelle Comunicazioni (AGCOM).

Ai fini di una compiuta analisi dello strumento di tutela – si badi: disegnato dal legislatore alla stregua di un *parental control* di Stato – pare opportuno collocare il medesimo all'interno del più ampio contesto normativo dedicato alla disciplina del cyberspazio, così da valutare le potenzialità della soluzione proposta nel contesto dei principi generali che regolano la materia. La conclusione è quella per cui l'indeterminatezza dei contenuti oggetto di blocco e le ridotte possibilità di personalizzazione del filtro contenutistico da parte dell'utenza inducono plurime preoccupazioni sul versante della tutela del generale principio di *Internet free speech* e legittimano più di una riflessione sull'opportunità di invertire la gerarchia Stato-famiglia prevista dalla Carta costituzionale nell'espletamento della funzione educativa del soggetto minorenne.

1. La libertà di espressione nel cyberspazio: una libertà fondamentale

La libertà di espressione e informazione è più di una libertà fondamentale: essa è la pietra angolare su cui si regge l'ordinamento democratico; si colloca in posizione preminente nella scala assiologica di valori imposta dalla concezione liberale e trova solido ancoraggio nel nucleo duro dell'assetto costituzionale.
Interviene in questo senso il *First Amendment* della Costituzione degli Stati Uniti d'America, nonché, per quanto attiene all'ordinamento europeo, l'art. 10 della Convenzione Europea dei Diritti dell'Uomo, il quale declina la libertà fondamentale in termini di «libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche», postulando, quale limite tassativo al suo esercizio, la sola norma di legge strettamente necessaria a salvaguardare un proporzionato equilibrio con altri valori essenziali all'*humus* democratico, tra cui viene fatta espressa menzione della salute degli individui e della pubblica morale.
Per quanto di stretta pertinenza in questa sede, è inoltre doveroso evidenziare come la tutela del *free speech* – della libertà fondamentale che esso sottende – rappresenti il cardine attorno a cui gli ordinamenti democratici risultano aver imperniato *ab origine* la disciplina giuridica del cyberspazio.
È così per gli Stati Uniti d'America, ove la *Section 230 - Communications Decency Act* garantisce piena immunità da responsabilità editoriale all'*interactive computer service provider*, tanto in relazione alla trasmissione in rete di contenuti generati da terzi, quanto in relazione alla restrizione o all'eliminazione di tali contenuti. E con le dovute proporzioni, in direzione analoga si inserisce l'ordinamento dell'Unione Europea, ove gli artt. 12-15 *E-Commerce Directive* – nell'escludere expressis verbis la legittimità di un monitoraggio generale e preventivo posto in capo agli operatori di piattaforma – postulano, relativamente ai contenuti generati da terzi, un catalogo di esenzioni da responsabilità civile modulate sulla diversa natura dell'*Internet service provider* considerato (*mere conduit, caching* o *hosting service provider*).
Si impone una prima, essenziale, considerazione: la libertà di espressione, proprio poiché costituzionalmente protetta a titolo fondamentale, pone un limite invalicabile all'interpretazione della normativa in materia di cyberspazio, in particolar modo delle

norme la cui finalità (o ad ogni modo effetto) è quella di porre argini alla libera circolazione dei contenuti in rete.

Qualsiasi norma volta a precludere l'accesso a contenuti digitali (il *parental control* di Stato non fa eccezione) si rivela ontologicamente lesiva della fondamentale libertà di espressione e, come tale, la sua conformità con l'assetto costituzionale deve essere vagliata ai sensi del principio di proporzionalità di cui all'art. 52 par. 1 della Carta dei Diritti Fondamentali dell'Unione Europea: conforme è soltanto quella compressione della libertà fondamentale che si riveli – non solo strettamente necessaria a garantire la tutela di un ulteriore substrato giuridico parimenti fondamentale (libertà, diritto, o interesse generale dell'Unione) – ma altresì assistita da una serie di presidi di misura che assicurino il raggiungimento della finalità perseguita per via della minor compressione possibile della libertà di espressione.

Se è indubbio, sul piano generale, che la salute psico-fisica dei soggetti minorenni sia un diritto fondamentale titolato ad operare in bilanciamento con altri valori fondamentali (quale, nel caso di specie, la libertà di espressione), è tuttavia necessario prestare particolare attenzione al versante della proporzionalità per quanto attiene alla massima estensione della compressione della libertà fondamentale ritenuta tollerabile, al fine, dall'ordinamento giuridico. Oltrepassato tale stringente confine, ciò che si prospetta è invero il conflitto della norma con i principi fondanti dell'ordinamento e, dunque, la sua invalidità costituzionale.

La miglior approssimazione del vaglio di proporzionalità operato dalla Corte di giustizia dell'Unione europea a tutela della libertà di espressione nel cyberspazio può essere colta tramite l'analisi della *case-law* relativa alla normativa sui diritti di proprietà intellettuale.

La *case-law* prodotta dall'ordinamento giuridico statunitense – nel cui assetto costituzionale il *free speech* occupa posizione preminente e, come tale, resistente al bilanciamento con altri diritti fondamentali, specie non enumerati – offre poi esempi paradigmatici della sfera di incostituzionalità riservata a mal calibrate restrizioni di contenuti *web* fondate sulla tutela dei minori. In *Reno v. American Liberties Union*, la Corte Suprema ha rigettato la conformità a Costituzione di una normativa – peraltro contenuta nel *Communications Decency Act* (per quanto più sopra detto, nucleo fondante dell'*Internet free speech made in USA*) – volta a reprimere, tramite criminalizzazione, la consapevole diffusione in rete di materiale "osceno", "indecente" o "manifestatamente offensivo" a minori di anni diciotto, con contestuale esenzione di responsabilità per quei soli operatori che si fossero attivati per evitare il contatto tra minori e contenuti proibiti per il tramite di efficaci filtri basati sulla *proof of age* degli utenti. Si noti: l'intrinseca vaghezza delle locuzioni "osceno", "indecente" e "manifestatamente offensivo" ha indotto la censura costituzionale della normativa – non tanto sul piano del principio di determinatezza della fattispecie criminosa, sancito in seno all'ordinamento USA dal *Fifth Amendment* e dalla correlata *Void for Vagueness Doctrine* – bensì, ancor più a monte, sul piano dell'indebita compressione della libertà di informazione tutelata dal *First Amendment*, la quale, nel caso di specie non opportunamente calibrata stante la sua genericità terminologica, avrebbe indotto il rischio di privare i minorenni di contenuti espliciti ancorché di natura artistica o educativa, nonché di allontanare gli adulti da contenuti

che, ancorché osceni o indecenti, costituiscono parte integrante del loro fondamentale diritto di libera informazione. Per dirla con le parole della Corte Suprema, incostituzionale è quel filtro interposto tra informazione e utente che, seppur finalizzato alla tutela del minore, finisce col confinare l'adulto al perimetro contenutistico adatto al soggetto vulnerabile («*it is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials, but that interest does not justify an unnecessarily broad suppression of speech addressed to adults; as we have explained the Government may not reduce the adult population to only what is fit for children*[1]»).

2. La libertà di espressione nel cyberspazio: una libertà fondamentale messa a dura prova dall'evoluzione del *web*

L'impianto normativo di cui alla *E-Commerce Directive*, imperniato sulla tutela della libertà di espressione per via della de-responsabilizzazione dell'*Internet service provider*, è stato calato, nell'anno 2000, in un cyberspazio dalla fisionomia drasticamente differente da quella assunta in tempi più recenti. In allora, era lecito supporre che la libertà di informazione avrebbe trovato terreno fertile in un *world wide web* a trazione pluralista, in cui i contenuti generati dagli utenti avrebbero potuto fluire liberamente in rete, trasmessi e ospitati da una moltitudine piattaforme digitali opportunamente de-responsabilizzate al fine: *blog*, *forum*, portali; il *web 1.0*: Internet come libero mercato di idee e contenuti.

La transizione al *web 2.0* ha tuttavia profondamente inciso sulla fisionomia originaria del cyberspazio; oggi, più che da plurimi attori, occupato (anzi, oligopolizzato) da singole piattaforme globali emerse vincitrici dall'effetto *winner takes it all* indotto dalle peculiarità strutturali del mercato digitale: simultanea economia di scala dal lato della offerta e della domanda, con conseguente aggregazione di utenti attorno a singoli servizi il cui valore viene alimentato dall'ampiezza della *customer base*, infine monetizzata per il tramite di strategie commerciali tarate sui profili digitali dei consumatori.

In siffatta concentrazione di mercato, gli *Internet service providers* – quegli stessi soggetti de-responsabilizzati dalla normativa europea relativamente alla veicolazione dei contenuti prodotti dagli utenti – assumono le vesti di veri e propri *gatekeepers* del traffico digitale; ruolo, quest'ultimo, che li pone in posizione privilegiata per eseguire operazioni di filtro e monitoraggio del flusso informativo: nella prospettiva tipica dell'analisi economica del diritto, destinatari ideali di obblighi di *compliance* normativamente imposti dall'autorità pubblica, poiché in grado di strutturare e implementare le soluzioni tecnologiche più idonee al fine e di sopportarne i rispettivi costi in virtù della monetizzazione del mercato che essi presidiano.

La considerazione è pregnante al punto da aver indotto il legislatore europeo a porsi in progressiva controtendenza rispetto all'originario paradigma normativo di cui alla *E-Commerce Directive*; numerosi, infatti, sono gli obblighi normativi calati dal legislatore

[1] Janet Reno, Attorney General of the United States, et al. v. American Civil Liberties Union et al., 521 U.S. 844 (1997).

in capo ai *gatekeepers* relativamente ai contenuti originati da terzi e da loro veicolati in rete: la normativa italiana in materia di *parental control* di Stato, dunque, non si configura come eccentrica compressione dell'*Internet free speech*, ma si colloca nel solco di distinti provvedimenti UE – *Digital Services Act* e *Audiovisual and Media Service Directive* tra tutti – emanati al dichiarato fine di coinvolgere i *players* della rete nella regolamentazione volta ad incrementare la sicurezza e la qualità contenutistica del cyberspazio.

Il *Digital Services Act* è paradigmatico del moderno approccio regolamentare: nonostante gli *Internet service providers* mantengano discreti margini di manovra nell'implementazione dei presidi necessari ad assicurare la *compliance* normativa, ad essere calata dall'alto in una logica *top-down*, da regolatore a regolato, è la categorizzazione degli operatori in quattro distinte classi di rischio, individuate alla luce della stimata influenza dell'attività svolta con i diritti fondamentali degli utenti; classi di rischio, quest'ultime, a cui si ricollegano ventagli di obblighi normativi progressivi nella loro estensione, sempre individuati in via unilaterale dal legislatore.

Per quanto attiene alla tutela dei minori in rete, è ad ogni modo l'*Audiovisual and Media Service Directive* ad applicare l'approccio normativo in analisi al tema: previa individuazione della categoria *video sharing platforms*, la Direttiva impone agli Stati Membri di vincolare quest'ultima ad assicurare la protezione dei minorenni da contenuti digitali qualificati come dannosi per il loro sviluppo fisico, mentale e morale; ciò attraverso una serie di soluzioni tecniche – implementabili dalle piattaforme, anche in ottica di *self-regulation* o *co-regulation* con l'Autorità – che postulano l'applicazione di filtri basati sulla *age verification* e su meccanismi di *flagging* dediti alla segnalazione di contenuti ritenuti nocivi, nonché su sistemi di *parental control* la cui attivazione e modulazione è, tuttavia, interamente rimessa alla disponibilità dell'utente.

È stato, acutamente, osservato come ci si trovi dinnanzi ad un nuovo paradigma di regolamentazione del cyberspazio a struttura, per così dire, "triangolare", poiché tarato sui tre vertici rispettivamente rappresentati dalla autorità pubblica, dagli utenti di rete e – non da ultimo, anzi in posizione preminente – dagli *Internet service providers*, progressivamente responsabilizzati del monitoraggio della rete tramite imposizione normativa e, dunque, in buona misura, delegati allo svolgimento di compiti di stretta pertinenza dei pubblici poteri, ivi incluso il delicato bilanciamento tra i diritti fondamentali degli utenti[2].

Se l'efficienza economica e tecnologica costituisce il punto di forza del rinnovato paradigma normativo, numerose sono le sue controindicazioni giuridiche, in particolar modo avuto riguardo alla necessaria, per tutto quanto più sopra visto, salvaguardia della libertà di espressione nel cyberspazio.

Assegnare agli *Internet service providers* il bilanciamento di diritti fondamentali – nel caso che ci occupa, il bilanciamento tra libertà di espressione e tutela dei minori – significa delegare, quantomeno in prima istanza, l'equilibrio dell'assetto costituzionale del cyberspazio a soggetti privati, di certo non altrettanto sensibili alle istanze del diritto pubblico quanto lo sono alle esigenze economiche imposte dal proprio *business model*.

Profonda, dunque, deve essere la consapevolezza che l'assegnazione di obblighi di monitoraggio in capo all'*Internet service provider* porta con sé, quale effetto collaterale,

[2] () J.M. Balkin, *Free speech is a triangle*, in *Columbia Law Review*, 118(7), 2018, 2011 ss.

la tendenza verso il fenomeno di *collateral censorship*: trattasi della censura di contenuti, ancorché potenzialmente leciti, operata da soggetti indifferenti alla salvaguardia di tali contenuti poiché estranei alla loro produzione e meramente dediti alla loro diffusione a scopo di lucro. Stante la concentrazione di mercato, d'altronde, ogni singolo *Internet service provider* trasmette (o ospita) per il tramite della propria piattaforma una mole di contenuti tale da rendere irrilevante il peso specifico di singoli pezzi di informazione; ne consegue che l'*Internet service provider*, per cui la rimozione di contenuti è operazione economicamente neutra, risulta finanziariamente incentivato ad elidere ogni contributo potenzialmente (e non necessariamente) illecito, così da evitare in radice il rischio di violazione della normativa ad esso destinata e i conseguenti costi connessi a possibili responsabilità vicarie o sanzioni amministrative.

Il rischio di *collateral censorship* viene inoltre catalizzato nel *web* dalla possibile opacità con cui le operazioni di blocco dei contenuti possono essere compiute: filtraggi automatizzati – specie se affidati all'intelligenza artificiale, alla sua nota opacità algoritmica, svolti in assenza di *human oversight* e svincolati dalla possibilità di opposizione per gli utenti – conducono a soppressioni intrinsecamente indebite della libera informazione, poiché non trasparenti e, pertanto, non giustificabili in un'ottica di *due process*.

Il legislatore europeo dimostra costante consapevolezza del fenomeno di *collateral censorship* e, invero, numerose sono le cautele poste a tutela della libertà di espressione che affiancano l'introduzione di ogni obbligo di monitoraggio dei contenuti calato in capo all'*Internet service provider*. Per restare al tema della tutela dei minori, è dirimente notare come le operazioni di filtro dei contenuti nocivi postulate dalla *Audiovisual and Media Service Directive* si collochino innanzitutto nel contesto di esenzione da responsabilità imposto dagli artt. 12-15 *E-Commerce Directive* già più sopra esaminato e, pertanto, come esse non possano in alcun caso risolversi nell'imposizione, in capo agli *Internet service providers,* di un obbligo di monitoraggio generale e preventivo dei contenuti diffusi in rete dagli utenti. Di più: se, da un lato, ai sensi della Direttiva appare legittimo applicare le più rigide misure di controllo dei contenuti a tutela dei minori, queste, dall'altro lato, sono nondimeno tenute ad ispirarsi ad un principio di proporzionalità parametrato, non solo in base alle dimensioni della piattaforma *on-line*, al servizio offerto e alla natura del contenuto tramesso, ma altresì in base al fondamentale diritto di libera espressione riconosciuto dall'ordinamento in capo al creatore del contenuto passibile di blocco, nonché al generale interesse del pubblico alla libera fruizione del medesimo. E ancora: le decisioni assunte dalla piattaforma in merito al blocco dei contenuti, anche all'esito di segnalazione da parte degli utenti tramite il meccanismo di *flagging*, lungi dall'essere unilaterali, devono poter essere contestate per il tramite di trasparenti procedure di *complaints redressal* strutturate dalla piattaforma stessa, e ogni disputa ad esse relativa deve poter essere giudicata imparzialmente nel corso di procedure stragiudiziali messe a disposizione degli utenti da parte degli Stati Membri.

Trattasi, quelle ora elencate, di una serie di garanzie poste a salvaguardia dei diritti fondamentali degli utenti: non solo di coloro i quali vantano il legittimo interesse a vedere implementati i sistemi di filtraggio dei contenuti a tutela dei minori, ma altresì dei *content creators*, a cui è riconosciuto il diritto di libera espressione in merito alle informazioni veicolate sul *web*, nonché del pubblico nel suo complesso.

3. *Parental control* di Stato: art. 7-*bis*, d.l. 28/2020 e delibera AGCOM n. 9/23

Esaurita l'analisi del contesto tecnologico e giuridico in cui si inserisce la normativa italiana in materia di *parental control* di Stato, è ora possibile passare in rassegna i suoi contenuti specifici, così come recentemente esplicitati dalle Linee Guida emanante dall'AGCOM; ciò al fine di vagliare le potenzialità dello strumento posto a tutela dei minori e i relativi attriti con il generale principio di libera espressione nel *web*. A sintesi di quanto finora detto, si impone invero un punto fermo: è necessario vagliare la costituzionalità della normativa italiana in materia di *parental control* di Stato alla luce dei presidi di proporzionalità in essa insiti, a partire dalla circostanziata individuazione dei contenuti suscettibili di blocco e dall'indirizzamento di tale filtro nei confronti dei soli soggetti resi vulnerabili dalla minore età.

Ai sensi del primo comma dell'art. 7-*bis,* d.l. 28/2020, «i contratti di fornitura nei servizi di comunicazione elettronica disciplinati dal codice di cui al decreto legislativo 1° agosto 2003, n. 259, devono prevedere tra i servizi pre-attivati sistemi di controllo parentale ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto».

Quanto all'ambito oggettivo di applicazione della disposizione normativa – ricavabile dalle utenze coinvolte nella pre-attivazione del meccanismo di blocco – esso è opportunamente limitato alle sole offerte dedicate ai minori, nella misura in cui è in relazione a queste che opera l'obbligo di pre-attivazione del *parental control*, mentre per le restanti utenze il filtro contenutistico sarà soltanto reso disponibile ed attivabile (anziché disattivabile) a discrezione del titolare del contratto. Se – come evidenziato da alcune associazioni a tutela dei minori – ciò rende possibile l'aggiramento del filtro da parte dei minori tramite utilizzo dei dispositivi elettronici dei genitori o di altri soggetti maggiorenni, reagire a siffatto rischio tramite pre-attivazione del meccanismo di *parental control* sulla generalità delle utenze avrebbe postulato una frontale violazione alla libera circolazione dei contenuti digitali, stante l'impossibilità costituzionale di proteggere i minorenni tramite una re-disegnazione complessiva del cyberspazio a prova di soggetto vulnerabile che finisca col confinare la totalità degli utenti al medesimo, ridotto, perimetro contenutistico. Le critiche mosse alle Linee Guida sotto il profilo in analisi si rivelano dunque non condivisibili e prive di fondamento, poiché tarate in via esclusiva sulla esigenza di fornire ai minorenni il più ampio perimetro di tutela possibile, senza considerare le interferenze che un siffatto (ampio) perimetro di tutela genera con altri diritti fondamentali e interessi generali di pari rango quali quelli attinenti alla sfera dell'*Internet free speech*.

Quanto all'ambito soggettivo di applicazione della disposizione normativa, esso si palesa ben più ampio di quello fatto proprio dalla *Audiovisual and Media Service Directive*: se quest'ultima prevede sistemi di *parental control* liberamente attivabili dall'utenza e strutturati dalla sola categoria delle *online video sharing platforms*, la normativa italiana coinvolge nell'implementazione – e pre-attivazione – di siffatti sistemi di blocco contenutistico gli operatori di rete, ossia, quegli *Internet service providers* che, offrendo tramite i propri servizi l'accesso ad *Internet*, si qualificano alla stregua di *mere conduit*

service providers ai sensi della *E-Commerce Directive* e, pertanto, godono di esenzione da responsabilità nei confronti di tutti i contenuti da loro trasmessi *(i)* senza dare origine alla trasmissione, *(ii)* senza selezionare il destinatario della trasmissione e *(iii)* senza selezionare o modificare le informazioni trasmesse.

Trattasi dei destinatari ideali dell'esenzione di responsabilità prevista dalla *E-Commerce Directive*, poiché rientranti, ancor più di altri *Internet service providers*, nell'archetipo di operatori di rete neutrali rispetto ai contenuti veicolati nel *web*. Per dirla con le parole della giurisprudenza della Corte di giustizia dell'Unione europea che si è occupata di perimetrare i confini soggettivi dell'esenzione di responsabilità prevista dalla *E-Commerce Directive*: operatori di rete che agiscono per via della mera elaborazione tecnica ed automatizzata delle informazioni apportate dagli utenti («*by a merely technical and automatic processing of the information provided by the recipient of the service*[3]»). Trattasi, pertanto, di soggetti particolarmente esposti al fenomeno di *collateral censorship* di cui si è poc'anzi detto, invero insito nell'indifferenza, soprattutto economica, nutrita dagli operatori rispetto ai contenuti veicolati in rete e alla loro possibile censura.

Il rischio di *collateral censorship* risulta nel caso di specie enfatizzato dalla vaga indicazione dei contenuti oggetto di blocco o filtro a tutela dei minori. A tal riguardo, la disposizione normativa italiana si rivela quantomai generica, limitandosi ad indicare, quali contenuti rispettivamente passibili di filtraggio e blocco, le vaghe categorie dei «contenuti inappropriati per i minori» e dei «contenuti riservati ad un pubblico di età superiore agli anni diciotto». L'apoditticità di siffatte indicazioni si configura come deleteria per la tutela dell'*Internet free speech*, palesando il profilo di incostituzionalità già più sopra sviscerato con l'ausilio della giurisprudenza della Corte Suprema USA, nel contesto che ci occupa peraltro esasperato dalla dinamica di *collateral censorship* indotta dalla concentrazione di mercato e dalla neutralità degli operatori di rete coinvolti nel paradigma normativo. Seppur esenti da responsabilità civile per omesso controllo dei contenuti di terze parti ai sensi della *E-Commerce Directive*, gli *Internet service providers* si troverebbero invero incentivati a formulare una interpretazione estensiva delle categorie contenutistiche suscettibili di blocco o filtraggio, così da minimizzare il rischio dell'esercizio del potere sanzionatorio conferito all'AGCOM in caso di omessa o parziale implementazione del *parental control* imposto *ex lege*.

Pregevole, dunque, è l'impostazione offerta dalle Linee Guida dell'AGCOM, nella misura in cui – tramite una lettura sistematica delle disposizioni di cui alla *Audiovisual and Media Service Directive* e del Codice Europeo delle Comunicazioni Elettroniche – priva gli operatori di rete del potere di riempire di significato le categorie di contenuti "inappropriati" o "riservati" postulate dalla normativa e riserva la competenza di tale classificazione in capo alla stessa Autorità amministrativa indipendente, seppur all'esito di procedure di co-regolamentazione svolte in sinergia con gli *Internet service providers*.

Ciò nonostante, la soluzione proposta dall'AGCOM è destinata a trovare applicazione nel solo lungo periodo: nelle more della procedura di consultazione che sarà necessario implementare al fine di determinare i contenuti "inappropriati" per i minori o "riservati" agli adulti, infatti, la categorizzazione dei medesimi viene temporaneamente rimessa dalle Linee Guida in capo ai medesimi operatori di rete, i quali, al fine, posso-

[3] () CGUE C-236/08, *Google France* (2008); CGUE, C-324/09, *L'Oréal* (2009).

no utilizzare le liste di domini/sottodomini e contenuti determinate secondo proprie specifiche di servizio e/o fornite da soggetti terzi individuati sulla base della serietà e capacità professionale avuto riguardo alla idoneità degli stessi a perseguire gli scopi della legge e alle migliori prassi.

Preme dunque evidenziare, quantomeno nel breve periodo, un significativo incentivo di *collateral censorship* posto dalla normativa italiana in commento, che è necessario minimizzare quanto prima tramite instaurazione e finalizzazione del procedimento volto alla precisa classificazione ed individuazione dei contenuti a visione non libera. E, sul punto, è senz'altro necessario raggiungere un maggior grado di precisione rispetto a quanto anticipato in via interlocutoria dall'AGCOM tramite le Linee Guida in commento: categorie contenutistiche ambigue e suscettibili di interpretazione quali quelle proposte– *e.g.* «contenuti per adulti: nudità totale o parziale in un contesto sessuale pornografico» – rendono ardua la distinzione algoritmica, per stare nell'esempio, tra una *clip* di *Pornhub* e un estratto di "Ultimo Tango a Parigi", sollevando dunque più di un dubbio circa l'opportunità di sottoporre al medesimo meccanismo di blocco contenuti ontologicamente distinti sul piano artistico-culturale, e così sulla piano della loro attitudine ad impattare lo sviluppo psico-sociale del soggetto minorenne. Tanto più che il filtraggio – in ottemperanza ad un pregevole presidio di proporzionalità previsto dalle Linee Guida – deve avvenire in linea di massima su singoli contenuti e, soltanto ove ciò si riveli non tecnicamente possibile, il blocco può coinvolgere l'intero dominio su cui il contenuto è ospitato, seguendo il criterio più ristrettivo sulla base dei contenuti presenti. Ove non si concretizzi un filtro tarato su singoli contenuti, invero, ciò che si prospetta all'orizzonte è l'espulsione coatta dei minorenni dalle piattaforme che accentrano l'utenza del *web*: di fatto, la frontale negazione del loro diritto di informazione e espressione in rete.

La necessità di una oculata categorizzazione dei contenuti passibili di blocco deve essere stressata altresì alla luce della ridotta possibilità di personalizzazione del *parental control* da parte dell'utenza. Ferma la sua pre-installazione, il potere di disattivazione, riattivazione e configurazione è rimesso all'esercente la potestà genitoriale sul minorenne titolare del contratto con l'*Internet service provider*, il quale – previa identificazione digitale – lo esercita tramite l'interfaccia *web* o *app* che l'operatore di rete è tenuto a disegnare in maniera semplice ed intuitiva. Tuttavia, l'unica funzionalità che l'*Internet service provider* è tenuto a garantire all'utenza è quella volta alla attivazione-disattivazione delle categorie oggetto di blocco (*e.g.* «contenuti per adulti» – «armi» – «odio e discriminazione»), mentre resta una mera facoltà dell'operatore di rete l'implementazione di una soluzione tecnologica che consenta all'utente (maggiorenne) la personalizzazione dello specifico contenuto di siffatte categorie tramite liste di domini consentiti e vietati (*block list* e *allow list*). Una facoltà che – stante il principio di gratuità nell'offerta del servizio a cui sono vincolati gli operatori di rete – risulta assistita da incentivi finanziari al suo omesso esercizio e che dunque raramente, si crede, sarà implementata. Si configura, pertanto, lo scenario che vede l'esercente la potestà genitoriale essere vincolato alla scelta di consentire la visione da parte del minorenne di tutti (o nessuno) i contenuti appartenenti ad una data categoria, senza possibilità di ulteriore distinzione: per riprendere l'esempio, il video pornografico e la scena sessualmente esplicita di

un'opera cinematografica. In questo senso, è possibile argomentare l'inversione del rapporto gerarchico famiglia-Stato imposto dagli artt. 29-31 della Carta costituzionale nell'esercizio della funzione educativa del minore: è l'autorità pubblica, con l'aiuto degli *Internet service providers*, a predisporre e pre-attivare gli strumenti dediti alla selezione del patrimonio informativo del minorenne e i contenuti da questi filtrati o bloccati, lasciando residuare in capo alla funzione genitoriale la sola scelta della loro totale rimozione o della loro parziale modulazione, ma negli angusti limiti in cui questa è concessa dall'architettura tecnologica degli applicativi.

Nella medesima ottica di esautorazione genitoriale, rileva, da ultimo, l'assenza di procedure di *complaints redressal* finalizzate alla gestione delle contestazioni formulate dall'utenza circa le modalità di selezione dei contenuti rispettivamente ammessi o bloccati alla stregua delle categorie contenutistiche previste dalla autorità pubblica (ad oggi, dagli operatori di rete). Pare invero aprirsi un vuoto di tutela: tanto per l'esercente la potestà genitoriale che veda il minore accedere a contenuti riservati agli adulti o non accedere a contenuti idonei alla minore età nonostante (o a causa de) il *parental control*; quanto per il *content creator* i cui contenuti vengano vietati al pubblico minorenne, che di tale circostanza potrebbe addirittura restare ignaro, nell'assenza di obblighi informativi previsti nei suoi confronti.

Pubblicità tradizionale e *digital advertising*: profili di valutazione economica

Roberto Moro-Visconti

Abstract

La pubblicità è, da oltre un secolo, l'anima del commercio. Accanto ai tradizionali canali (televisione, radio, carta stampata), il digital advertising sta assumendo una dimensione preponderante, sfruttando la rete Internet per indirizzare i consumi e utilizzando sofisticati algoritmi che segmentano la clientela. In questo ambito evolutivo, oggetto di profonde mutazioni, si inseriscono le metriche di valutazione per le società che fruiscono dei servizi pubblicitari, nell'ottica di incrementare le vendite e la conoscibilità del marchio (*brand awareness*). Le stime sono utilizzate in ambito stragiudiziale ovvero contenzioso, in caso di pubblicità ingannevole o altre fattispecie.

Advertising has been the soul of commerce for over a century. Alongside traditional channels (television, radio, printed paper), digital advertising is assuming a preponderant dimension, exploiting the Internet to direct consumption, and using sophisticated algorithms to segment customers. In this evolutionary field, subject to profound changes, the evaluation metrics for the companies that use advertising services are considered, to increase sales and brand awareness. The estimates are used in out-of-court or litigation matters, in the case of misleading advertising or other matters.

Sommario

1. Pubblicità tradizionale e *digital advertising*. – 2. Rappresentazione in bilancio. – 3. Aspetti fiscali e crediti d'imposta per investimenti pubblicitari. – 4. Modelli di business. – 5. *Marketing* personalizzato, *social network* e valore della clientela. – 6. Andamento e prospettive del mercato pubblicitario. – 7. Ricavi pubblicitari incrementali. – 8. Pubblicità ingannevole, concorrenza sleale e stima dei danni.

Keywords

pubblicità online - *brand awareness* - *marketing*; *social networks* - internet.

1. Pubblicità tradizionale e *digital advertising*

La pubblicità è definibile come «l'insieme di tutti i mezzi e modi usati allo scopo di

segnalare l'esistenza e far conoscere le caratteristiche di prodotti, servizi, prestazioni di vario genere predisponendo i messaggi ritenuti più idonei per il tipo di mercato verso cui sono indirizzati»[1].

La pubblicità commerciale[2] è ogni forma di comunicazione volta a promuovere la vendita di beni o la prestazione di servizi da parte di un operatore economico (art. 2, lett. *a)*, d.lgs. 145/2007).

Il Codice del consumo (d.lgs. 206/2005) fa rientrare la pubblicità nella più ampia nozione di "pratica commerciale", aggiungendo che tale pratica è ingannevole se contiene informazioni non rispondenti al vero o idonee a indurre in errore, ed è scorretta se contraria alla diligenza professionale.

La *digital advertising* (pubblicità online) corrisponde al valore della raccolta pubblicitaria effettuata sulla Rete, all'interno di siti web e *mobile app*, fruiti da qualsiasi dispositivo che disponga di una connessione internet[3].

La pubblicità su internet si declina sui principali canali che costituiscono l'esperienza online degli utenti: *social media*, motori di ricerca, siti web, *newsletter*, video, etc., è per questo è diventata ormai una leva prioritaria negli investimenti in *marketing* e comunicazione delle aziende[4]. In prospettiva, la *digital advertising* sfrutterà la realtà virtuale ed aumentata (sconfinando nel metaverso) e algoritmi di intelligenza artificiale (per la profilazione proattiva dei consumatori, l'elaborazione di modelli auto-predittivi, le *chatbot*, etc.).

In ambito pubblicitario, il *barter* o *bartering* è un sistema di cambio merci che consiste nel pagamento, parziale o totale, di uno spazio pubblicitario sui mezzi di comunicazione (tipicamente, format televisivi) effettuato da un'azienda attraverso prodotti e servizi dell'azienda medesima.

Rispetto all'*advertising* tradizionale, veicolato su televisione[5], radio, stampa e cartellonistica *out-of -home* (OOH), la pubblicità online si presta meglio a un tipo di comunicazione mirata, personalizzata e misurabile[6].

Sui *media* tradizionali, inoltre, l'investimento richiesto è piuttosto elevato e spesso non sostenibile dalle aziende minori. I formati pubblicitari online richiedono invece investimenti più contenuti e aprono perciò opportunità di visibilità, anche per le realtà imprenditoriali minori.

Le principali tipologie di *digital advertising* sono sintetizzate nella Tabella 1.[7]:

---

1 *Pubblicità* (voce), in *Treccani, Enciclopedia on line,* in *treccani.it.*

2 M. Fusi – P. Testa, *Diritto e pubblicità*, Bologna, 2006.

3 F. Oldani, *La digital advertising oltre il tradizionale*, in *Mark up*, 281, 2019, 36 ss.

4 J. Chen – J. Stallaert, *An economic analysis of online advertising using behavioral targeting*, in *MIS Quarterly*, 2, 2014, 429 ss.

5 Per i dati di ascolto, che rilevano ai fini dei canoni pubblicitari, si utilizza l'Auditel, che dal 1984 raccoglie e pubblica dati sull'ascolto televisivo italiano.

6 A. Mandelli – M. Massi – C. Piancatelli, *Nuove logiche e traiettorie di crescita dell'advertising*", in *Economia & Management*, 1, 2022, 85 ss.

7 A. Lamperti, *Guida al Digital Advertising: formati e strategie di misurazione della pubblicità online*, in *blog.osservatori.net*, 1 luglio 2022.

Tabella 1. – Tipologie di pubblicità digitale

Fattispecie	Descrizione
Display advertising	Banner, *rich media* (contenuti multimediali), *video in/out stream* (formato pubblicitario all'interno di un altro contenuto video o a parte), *social media advertising*, *in-image* (immagini editoriali)
Native advertising	Contenuti sponsorizzati all'interno del contenuto principale (*reccomendation widget* e *content feed*), che non distraggono l'utente durante la navigazione
Search advertising	Intercetta l'utente durante le fasi inziali del processo d'acquisto (come la ricerca di un'informazione o di un prodotto su un motore di ricerca) e indirizza il traffico quanto più qualificato e interessato verso un sito *ad hoc*
Classified / eCommerce advertising	Acquisto di visibilità per annunci su siti di compravendita o *directory online* da parte di aziende e l'acquisto di visibilità all'interno di cataloghi e motori di ricerca presenti nei portali e nei siti di *eCommerce*
E-mail advertising	Include qualsiasi forma pubblicitaria all'interno di *newsletter* ed email inviate a un database di utenti che abbiano espresso esplicitamente consenso in conformità con la normativa GDPR
Audio advertising	Acquisto di spazi pubblicitari all'interno di flussi audio, come *web radio*, *podcast* e musica in *streaming on-demand*
Addressable Tv advertising	L'insieme di tecnologie che permettono agli investitori pubblicitari di selezionare una determinata *audience* televisiva, basata su dati di prima/seconda/terza parte, a cui offrire spot personalizzati, per quanto riguarda i contenuti e i formati, internamente a un programma o a uno schermo di navigazione comune (*smart tv*)
Digital Out-of-Home (cartellonistica digitale)	Tecnologie e servizi relativi a insegne digitali e contenuti promozionali posizionati in aree pubbliche ad alto traffico, come aree urbane pedonali, stazioni e aeroporti, strade, centri commerciali, mezzi in movimento ed in generale in luoghi di aggregazione

Le tendenze evolutive ricomprendono anche applicazioni futuribili come il metaverso[8].

2. Rappresentazione in bilancio

La contabilizzazione delle spese di pubblicità sostenute rappresenta un presupposto

[8] C. Pappalardo, *La pubblicità nel metaverso*, in G. Cassano – G. Scorza (a cura di), *Metaverso,* Pisa, 2023.

per la loro valorizzazione, contrapponendo costi operativi monetari (raramente capitalizzati) a maggiori ricavi attesi.
Il d.lgs. 139/2015 ha eliminato, dall'art. 2424 c.c., il riferimento ai costi di ricerca e di pubblicità fra le immobilizzazioni immateriali dello stato patrimoniale (voce B.I.2), mantenendo la possibilità di capitalizzare i soli costi di sviluppo.
Pertanto, i costi di pubblicità devono essere spesati in conto economico nell'esercizio in cui sono sostenuti.
Un'eccezione a quanto sopra è illustrata dal principio contabile OIC 24 ("Immobilizzazioni immateriali")[9], secondo cui possono essere iscritti nella voce dell'attivo "costi di impianto e ampliamento" (B.I.1) i costi di "startup" sostenuti «da una società di nuova costituzione per progettare e rendere operativa la struttura aziendale iniziale, o i costi sostenuti da una società preesistente prima dell'inizio di una nuova attività, quali ad esempio un nuovo ramo d'azienda, un nuovo centro commerciale per una società che opera nella grande distribuzione, un nuovo processo produttivo, ecc. Tra questi costi sono compresi, ad esempio, i costi del personale operativo che avvia le nuove attività, i costi di pubblicità sostenuti in tale ambito, (…)» (§ 25.).
Sempre secondo l'OIC 24, tuttavia, i costi di startup possono essere capitalizzati quando sono rispettate tutte le seguenti condizioni (§ 43.): «(i) i costi sono direttamente attribuibili alla nuova attività e sono limitati a quelli sostenuti nel periodo antecedente il momento del possibile avvio (i costi generali e amministrativi e quelli derivanti da inefficienze sostenute durante il periodo di start-up non possono essere capitalizzati); (ii) il principio della recuperabilità dei costi è rispettato, in quanto è ragionevole una prospettiva di reddito».

3. Aspetti fiscali e crediti d'imposta per investimenti pubblicitari

Fiscalmente, i costi di pubblicità seguono il principio generale indicato nel 1° comma del T.U.I.R. (Testo Unico delle Imposte sui Redditi, D.P.R. 917/1986), secondo cui «le spese relative a più esercizi sono deducibili nel limite della quota imputabile a ciascun esercizio». Per le spese di rappresentanza è invece previsto un regime diverso (con alcuni limiti).
Secondo la Cassazione, sentenza n. 34166, del 20 dicembre 2019[10], le spese di pubblicità o propaganda sono quelle sostenute per ottenere un incremento, più o meno immediato, della vendita di quanto realizzato nei vari cicli produttivi e in certi contesti, anche temporali, mentre le spese di rappresentanza sono quelle effettuate senza che vi sia una diretta aspettativa di ritorno commerciale.
Il "Decreto Energia" (D.L. 17/2022, convertito in legge) ha modificato la disciplina del c.d. "bonus pubblicità", ritornando a quanto precedentemente previsto sull'approccio incrementale delle spese, con esclusione dall'agevolazione degli investimenti

[9] Organismo Italiano di Contabilità, *Principi contabili - Immobilizzazioni immateriali,* in *fondazioneoic.eu.*

[10] Cass. civ., sez. tributaria, 20 dicembre 2019, n. 34166.

pubblicitari sulle emittenti televisive e radiofoniche locali, sia analogiche che digitali (come invece previsto per il triennio 2020-2022).
A partire dal 1° gennaio 2023[11], il credito d'imposta è dunque pari al 75% del valore incrementale degli investimenti in campagne pubblicitarie effettuati esclusivamente sulla stampa quotidiana e periodica, anche online.

4. Modelli di *business*

Una campagna pubblicitaria relativa a un bene di consumo e a un marchio ha inizio con lo sviluppo del piano di *marketing*, che consiste nello studio del loro posizionamento (*brand position* e *brand image*), cioè nell'analisi delle caratteristiche del prodotto e della marca, in modo da individuare una fascia di probabili consumatori (*target group*), decidere la strategia creativa (*copy strategy*), da cui dipende la possibilità di imporre il prodotto su vasta scala, i criteri di distribuzione (*trade*) e i canali pubblicitari, e le eventuali attività di sostegno, come la promozione, sponsorizzazione, il *direct marketing*, i rapporti con la stampa specializzata (ufficio stampa)[12].
La pubblicità è oggetto di fruizione prioritaria da parte di imprese che si posizionano sul segmento B2C della catena del valore, interagendo direttamente con i consumatori finali.
I ricavi pubblicitari (P) assumono rilievo ai fini della stima del presumibile valore di mercato delle testate giornalistiche; la formula (empirica) basata sui moltiplicatori proposta dalla dottrina valutativa[13] è la seguente:

W = aF + bP – cR
ove:
W = valore di mercato della testata;
F = fatturato (abbonamenti e vendite);
a = moltiplicatore da applicare al fatturato (di norma pari a 1);
P = ricavi da pubblicità;
b = moltiplicatore da applicare ai ricavi da pubblicità (di norma ricompreso nell'intervallo da 1 a 2);
R = perdite operative;
c = moltiplicatore da applicare alle perdite operative (di norma ricompreso nell'intervallo da 3 a 5).

[11] Agenzia delle Entrate, *Investimenti pubblicitari incrementali - Che cos'è*.

[12] V. Persiani, *Le nuove frontiere della pubblicità*, in *Largo consumo*, 7/8, 2022, 84 ss.

[13] L. Guatri – M. Bini, *Nuovo trattato sulla valutazione delle aziende*, Milano, 2009, 188-189; R. Moro-Visconti, *La valutazione delle testate editoriali cartacee e online*, in *Il diritto industriale*, 6, 2014, 549 ss.

5. *Marketing* personalizzato, *social network* e valore della clientela

Il *marketing* personalizzato rappresenta un'innovazione delle esperienze di *mass market* uniformato e indifferenziato, fondandosi su una segmentazione sempre più mirata delle preferenze dei consumatori, anche attraverso un utilizzo dei loro dati personali, per creare nuove opportunità di business derivanti dall'incrocio di offerte di beni e servizi sempre più personalizzati con una domanda sempre più sofisticata[14].
Basandosi sulla cronologia e sulla geolocalizzazione (non sempre consapevole) delle attività dell'utente, delle sue preferenze e delle sue interazioni con i vari *brand*, si ha la possibilità di proporre dei messaggi promozionali coerenti e personalizzati, ritagliati su misura per ogni consumatore[15].
I *social network* consentono di trarre guadagno principalmente dalla fornitura a terzi delle informazioni degli utenti, che alimentano gratuitamente la base di conoscenza, in secondo luogo dalla pubblicità mirata che le aziende indirizzano agli utenti in base ai siti visitati, *link* aperti, permanenza media, alle informazioni da loro stessi inserite.
I modelli di *business* seguono nuovi paradigmi che hanno un impatto sempre più profondo sulla catena del valore (per produttori, erogatori di servizi, intermediari e consumatori), con rilevanti conseguenze anche di natura giuridica[16].
In tale prospettiva, gli strumenti digitali acquistano sempre più rilevanza non solo come "luoghi" di espressione e condivisione in rete, ma anche in quanto efficaci veicoli di informazione, sviluppo del *brand*, *marketing* e business[17].
I fornitori di servizi di comunicazione possono fidelizzare i consumatori focalizzandosi, principalmente, sull'esperienza generale degli stessi.

6. Andamento e prospettive del mercato pubblicitario

Secondo le ricerche dell'Osservatorio Internet Media[18], nel 2021, nonostante l'emergenza sanitaria, gli investimenti delle aziende italiane in *digital advertising* sono cresciuti del 24% rispetto all'anno precedente, a sua volta in crescita rispetto al 2019. Il valore di 4,28 miliardi di euro ha raggiunto quasi la metà dell'intero comparto pubblicitario italiano, pari a 9,3 miliardi di euro.
La pubblicità online rappresenta il 46% del totale, confermando la sua *leadership* per il secondo anno consecutivo, anche nei confronti dell'advertising televisivo (40%), su stampa (7%), radio (4%) e *out-of-home* (3%).

[14] M. Preti, *Monitorare i cambiamenti nel portafoglio clienti: quali vantaggi per l'azienda?* in *Amministrazione & Finanza*, 5, 2014, 41 ss.

[15] S. Erevelles - N. Fukawa - L. Swayne, *Big Data consumer analytics and the transformation of marketing*, in *Journal of Business Research*, 2, 2015, 897 ss.

[16] M. Sciarelli - M. Tani, *La social network analysis per lo studio dell'innovazione nelle reti di imprese*, in *Sinergie*, 93, 2014, 87 ss.

[17] Per maggiori approfondimenti, si rimanda a F. Oldani, *Brand Managing e social network*, in *Mark Up*, 24, 2017, 90 ss.

[18] Osservatori.net digital innovation, *Internet Media*.

Nonostante la congiuntura economica, il conflitto ucraino e la spirale inflattiva, anche nel 2022 si è registrata un'ulteriore crescita del mercato pubblicitario, seppur minima rispetto all'anno precedente[19].
Per il 2023, le stime prevedono invece per l'Italia una riduzione degli investimenti pubblicitari (che dovrebbero tornare positivi nel 2024), mentre la *digital advertising* dovrebbe superare il 50% delle spese[20].
Nel mercato operano le concessionarie di pubblicità, che fanno da intermediario tra editori e agenzie. L'intermediazione riguarda l'acquisto di spazi pubblicitari dai proprietari dei mezzi di comunicazione con rivendita ai centri media oppure, direttamente agli inserzionisti.

7. Ricavi pubblicitari incrementali

La valutazione economica può essere effettuata attraverso diversi profili, tra cui:
Costo per *impression* (CPM): si tratta del costo per ogni visualizzazione della pubblicità. Nel caso della pubblicità tradizionale, il CPM può essere calcolato dividendo il costo totale della campagna pubblicitaria per il numero di persone raggiunte. Nel *digital advertising*, il CPM si riferisce al costo per ogni migliaia di visualizzazioni dell'annuncio.
Costo per click (CPC): questo profilo di valutazione si riferisce al costo per ogni *click* effettuato sulla pubblicità. Nel caso della pubblicità tradizionale, il CPC può essere calcolato dividendo il costo totale della campagna pubblicitaria per il numero di persone che hanno interagito con l'annuncio. Nel *digital advertising*, il CPC si riferisce al costo per ogni *click* sul *banner* pubblicitario.
Return on investment (ROI): redditività operativa della campagna pubblicitaria rispetto al costo totale della stessa[21]. Il ROI può essere calcolato sia per la pubblicità tradizionale che per il *digital advertising*.
L'azienda che acquista spazi pubblicitari (su canali tradizionali e/o digitali) persegue legittimi obiettivi di incremento dei ricavi di vendita.
Il reddito differenziale/incrementale incide sulla marginalità economico/finanziaria, anche per effetto della scalabilità del modello di business.
Attraverso la pubblicità digitale molti elementi "fisici", legati a business tradizionali, acquisiscono una dimensione immateriale, incorporando fattori di scalabilità che consentono un incremento più che proporzionale dei ricavi di vendita.
A fronte di costi fissi per definizione costanti e di costi variabili incrementali tendenzialmente contenuti, l'incremento esponenziale delle vendite si riverbera sull'aumento dei margini economici-finanziari (a cominciare dal MOL/EBITDA) che misurano la creazione di liquidità nel conto economico. Ciò si verifica, in particolare, in modelli di

[19] M. Mancinelli, *L'inflazione non frena l'advertising*, in *Largo consumo*, 11, 2022, 23 ss.

[20] *Dentsu stima una crescita del 3,8% per gli investimenti nel 2023, più per l'inflazione che per la crescita dei volumi*, 16 dicembre 2022, in *brand-news.it*.

[21] Data dal rapporto tra reddito operativo (assimilabile alla "differenza tra valore e costi della produzione A-B" ex art. 2425 c.c.) e capitale raccolto (o investito), corrispondente al totale delle passività (patrimonio netto + debiti finanziari).

business scalabili, anche per effetto di piattaforme digitali che interagiscono in rete.
L'avviamento dipende anche dalla predetta scalabilità, che consente di incrementare, anche esponenzialmente, i volumi di vendita, grazie a nodi digitali (ad esempio, i siti di ecommerce), che fungono da intermediari tra l'azienda e nuovi clienti.
Il processo può essere spiegato attraverso la teoria dei *network*, suscettibile di applicazioni anche in ambito giuridico[22] ed estendibile, per quanto qui rileva, anche all'interpretazione del plusvalore indotto all'avviamento dalla pubblicità digitale.
In un *network*, ciascun nodo è collegato ad altri nodi da lati. Il valore della rete dipende dal numero di nodi, dai loro collegamenti e dall'intensità degli stessi. Attraverso ciascun collegamento, si intermediano flussi informativi (*big data*) e transazioni; la crescita esponenziale indotta dalla pubblicità digitale aumenta sia il numero di nodi, sia l'intensità dei collegamenti, generando un plusvalore che si accumula nell'extra-avviamento.
L'impatto della pubblicità digitale sull'avviamento incrementale coinvolge l'intero sistema patrimoniale – economico – finanziario. Rileva, in particolare, il nesso causale nei confronti dei parametri più sensibili alla stima dell'avviamento incrementale, come riassunto nella Tabella 2.

Parametri tradizionali	**Impatto della pubblicità digitale**	**Avviamento incrementale**
Conto economico		
Ricavi di vendita (A)	La scalabilità dei ricavi aumenta i volumi di vendita	Ai maggiori ricavi (incrementali / differenziali) si associa un maggior avviamento implicito
Costi Operativi Monetari (OPEX) (B)	La pubblicità digitale può accorciare la *supply chain* e riduce i costi di transazione / intermediazione	I minori costi incrementano il Risultato Netto e il differenziale (R-iK)
Margine Operativo Lordo (EBITDA) (C)=(A)-(B)	L'aumento dei ricavi associato ad una contrazione dei costi fa incrementare il MOL	Il MOL più elevato fa crescere i moltiplicatori di mercato e impatta positivamente sui flussi di cassa (operativi e netti)
Ammortamenti e accantonamenti (D)	I minori investimenti in immobilizzazioni (CAPEX) riducono i costi operativi non monetari	I minori ammortamenti generano avviamento incrementale comprimendo i costi e aumentando il margine (risultato) operativo e netto
Risultato Operativo (EBIT) (E)=(C)-(D)	Il Risultato Operativo aumenta	L'avviamento incrementale migliora la marginalità economica
Risultato Netto	Il Risultato Netto aumenta	

[22] R. Moro-Visconti, *Il danno da contraffazione tra nesso giuridico causale e teoria dei network*, in *Il diritto industriale*, 4, 2022.

Stato patrimoniale		
Avviamento (contabilizzato e internamente generato)	La pubblicità digitale aumenta l'avviamento implicito (internamente generato), per effetto dei più elevati margini economici e finanziari e dei plusvalori patrimoniali	L'avviamento incrementale (differenziale) cresce
Immobilizzazioni nette (CAPital EXpenditure – CAPEX)	La pubblicità digitale comporta maggiori investimenti immateriali, a fronte di potenziali risparmi negli investimenti fissi	L'ottimizzazione tra dati di *input* (capitale investito, corrispondente all'attivo e ricomprendente la CAPEX) e dati di *output* (marginalità economica e finanziaria) fa crescere l'avviamento
Valore contabile del patrimonio netto (*book value of equity*)	Il saldo della CAPEX influenza il patrimonio netto contabile	Se il patrimonio netto contabile K si riduce, aumenta il differenziale (R-iK) che stima l'avviamento con un metodo misto patrimoniale-reddituale
Impatto sulle garanzie collaterali, *ratios* patrimoniali, merito creditizio e *rating* per gli affidamenti bancari	L'aumento del risultato netto incrementa il valore del patrimonio netto e la solidità patrimoniale dell'impresa affidata	Garanzie più estese o meno onerose impattano positivamente sull'avviamento
Valore di mercato del patrimonio netto (*market value of equity*)	L'incremento dei risultati reddituali e finanziari crea un extra-valore reddituale (maggiori margini economici), finanziario (maggiore liquidità creata) e, da ultimo, patrimoniale	L'avviamento incrementale aumenta il differenziale tra valore di mercato e valore contabile del patrimonio netto
Rendiconto finanziario		
Flussi di cassa in entrata (creazione di liquidità)	L'aumento dei ricavi monetari e del MOL fa incrementare i flussi di cassa in entrata	La liquidità incrementale impatta positivamente sull'avviamento
Flussi di cassa operativi (*Operating Cash Flows – Free Cash Flow to the Firm*)[1]	I flussi di cassa operativi aumentano grazie all'incremento del MOL	
Flussi di cassa netti (*Net Cash Flow – Free Cash Flow to Equity*)[2]	Anche i flussi di cassa netti sono positivamente influenzati dall'aumento del MOL	

Tabella 2. – *Impatto della pubblicità digitale e avviamento incrementale*

[1] Corrispondono ai flussi di cassa determinati prima del servizio del debito finanziario.

[2] Corrispondono ai flussi di cassa netti (residuali) per i soci, dopo il servizio del debito finanziario.

L'impatto della pubblicità sull'avviamento incrementale si ripercuote anche sulla valorizzazione dei marchi e sulla loro conoscibilità e consapevolezza (*brand awareness*) da parte dei consumatori, soprattutto in un ambito *retail*, connesso a catene distributive (*supply chain*) e del valore (*value chain*) operanti nel *mass market* Business to Consumer (B2C).

La valorizzazione del marchio (con investimenti cumulati per alimentare la c.d. "*brand equity*"[23]), alimentata dai *battages* pubblicitari, trova un riscontro contabile nel suo incremento di valore (contabilizzato nell'attivo) soltanto in seguito all'adozione di provvedimenti di rivalutazione *ex lege* ovvero in caso di acquisizione a titolo oneroso (o di conferimento in natura) di marchi che incorporano un plusvalore riflesso nel (maggior) valore di acquisto.

8. Pubblicità ingannevole, concorrenza e stima dei danni

Secondo l'art. 2 del già menzionato d.lgs. 145/2007, è da intendersi come ingannevole «qualsiasi pubblicità che in qualunque modo, compresa la sua presentazione è idonea ad indurre in errore le persone fisiche o giuridiche alle quali è rivolta o che essa raggiunge e che, a causa del suo carattere ingannevole, possa pregiudicare il loro comportamento economico ovvero che, per questo motivo, sia idonea a ledere un concorrente».

Secondo il citato Codice del consumo (artt. 21-23), la pubblicità ingannevole riguarda le pratiche commerciali scorrette, idonee a indurre in errore il consumatore medio, falsandone il processo decisionale[24]. L'induzione in errore, anche attraverso metodiche subliminali, può riguardare il prezzo, la disponibilità sul mercato del prodotto, le sue caratteristiche, i rischi connessi al suo impiego.

In tale ambito, ha assunto rilievo, in tempi recenti, il c.d. "*greenwashing*", che rappresenta una pratica ingannevole, usata come strategia di *marketing* da alcune aziende per dimostrare un finto impegno nei confronti dell'ambiente, con l'obiettivo di catturare l'attenzione dei consumatori attenti alla sostenibilità[25].

La pubblicità ingannevole e le pratiche commerciali scorrette possono assumere il connotato della concorrenza sleale, con gravi ripercussioni economiche per il danneggiato.

In genere, oltre ai danni patrimoniali (perdite subite), assume altresì rilevanza il pregiudizio derivante dalla perdita (devalorizzazione) dell'avviamento, che ricomprende sia il concetto di danno emergente (perdita di *goodwill* – avviamento – storico) che quello di lucro cessante (influendo negativamente sulla capacità futura del soggetto danneggia-

[23] S.Z.S. Shah – S. Akbar, *Value relevance of advertising expenditure: A review of the literature*, in *British Academy of Management*, 2008.

[24] G. Visconti, *Pratiche commerciali. La tutela delle imprese contro la pubblicità ingannevole e comparativa scorretta effettuata dai concorrenti*, in *PMI*, 8/9, 2017, 47 ss.

[25] A. Pistilli, *Il 'green-washing' tra pubblicità ingannevole e pratica commerciale scorretta: quando può dirsi atto di concorrenza sleale*, in *Il Diritto Industriale*, 4, 2022, 381 ss.

to di generare un'extra-utilità, anche in termini di maggiore marginalità).
In senso lato e considerando molteplici e interconnesse sfaccettature (da adattare – di volta in volta – al caso di specie), il danno da perdita di avviamento può essere, tra l'altro, causato dalle fattispecie riportate nella seguente Tabella 3.:

Tabella 3. – *Danno da perdita di avviamento*

Fattispecie	Descrizione
Storno, sviamento e accaparramento del portafoglio clientela (concorrenza sleale), a seguito di pratiche commerciali scorrette	Il portafoglio clienti incorpora molti elementi che rappresentano l'essenza e la sintesi delle strategie di *marketing* sempre più profilate *ad personam* e la prerogativa più rilevante dello stesso avviamento. Lo sviamento di clientela, il danno d'immagine e altre fattispecie annesse e connesse comportano un affievolimento o perdita del rapporto personale con i clienti, riducendo il valore del portafoglio clientela e, con esso, l'avviamento.
Contraffazione di beni immateriali	La violazione di diritti immateriali comporta naturalmente un indebito sviamento dell'avviamento ad essi associato, causando danni diretti, ma anche indiretti.
Calo di prestigio e danno (svilimento) d'immagine	L'avviamento è, tra l'altro, anche prestigio, immagine, rinomanza, notorietà, a volte celebrità; il danno d'immagine comporta, in definitiva, uno svilimento anche dell'avviamento.
Perdita di *chances* e delle legittime aspettative economiche	L'avviamento, concetto intrinsecamente prospettico (ancorché fondato su eventi storicamente stratificatisi) e sempre in divenire, è intimamente legato alle *chances* future, intese come opzioni razionalmente percorribili per intraprendere nuovi investimenti, conquistare nuovi mercati e clienti (…). Le aspettative economiche si basano anche sulla proiezione dell'avviamento e delle strategie.
Impossibilità ad operare in settori proficui e con elevate potenzialità di crescita	La perdita di avviamento spesso costringe la società a riposizionarsi su obiettivi strategici meno ambiziosi, con una reazione a catena che genera un'erosione anche del nuovo avviamento potenziale, inibendo anche finanziariamente l'accesso a settori a maggiore marginalità ed ostacolando le strategie di differenziazione.
Perdita di quote di mercato, spesso difficilmente recuperabili	L'avviamento è basato anche su quote di mercato, che incidono sui volumi di vendita e indicano il posizionamento strategico dell'impresa nel settore, in chiave comparativa con la concorrenza.
Difficoltà finanziarie derivanti dal mancato incasso dei ricavi addizionali venuti meno	Il danno da perdita di avviamento sottrae indebitamente alla società ricavi e conseguenti flussi di cassa, talora fino al punto da ingenerare crisi finanziarie.
Danno economico derivante dal mancato ammortamento degli investimenti pubblicitari e dei costi fissi comunque sostenuti, riferiti a extra-ricavi venuti meno	Con la perdita di avviamento, i costi fissi (fra cui le spese pubblicitarie e l'ammortamento degli investimenti pubblicitari già effettuati) - per definizione, comunque sostenuti - si ripartiscono su più esigui ricavi, con un'incidenza proporzionalmente più elevata.

Con riferimento alla quantificazione del danno, l'art. 1223 c.c. dispone che «il risarcimento del danno per l'inadempimento o per il ritardo deve comprendere così la perdita subita dal creditore come il mancato guadagno, in quanto ne siano conseguenza immediata».

Il lucro cessante (mancato guadagno) indica una forma di danno patrimoniale, che impedisce al danneggiato di percepire una o più utilità economiche che avrebbero incrementato il suo patrimonio ove il danno non si fosse verificato. Il lucro cessante è formalmente distinto rispetto al danno emergente, che consiste nella diminuzione riscontrabile del patrimonio del danneggiato (perdita subita che sarebbe stata evitata), anche se i due concetti sono tipicamente associati.

Secondo l'art. 125 CPI, «il risarcimento dovuto al danneggiato è liquidato secondo le disposizioni degli articoli 1223, 1226 e 1227 del Codice civile, tenuto conto di tutti gli aspetti pertinenti, quali le conseguenze economiche negative, compreso il mancato guadagno del titolare del diritto leso, i benefici realizzati dall'autore della violazione e, nei casi appropriati, elementi diversi da quelli economici, come il danno morale arrecato al titolare del diritto dalla violazione. La sentenza che provvede sul risarcimento dei danni può farne la liquidazione in una somma globale stabilita in base agli atti della causa e alle presunzioni che ne derivano. In questo caso il lucro cessante è comunque determinato in un importo non inferiore a quello dei canoni che l'autore della violazione avrebbe dovuto pagare, qualora avesse ottenuto una licenza dal titolare del diritto leso. In ogni caso il titolare del diritto leso può chiedere la restituzione degli utili realizzati dall'autore della violazione, in alternativa al risarcimento del lucro cessante o nella misura in cui essi eccedono tale risarcimento».

La stima del danno si basa su diversi criteri e può essere determinata anche in via equitativa dal giudice; la giurisprudenza ha individuato, tra i criteri di stima del danno da contraffazione, anche il volume delle vendite dei prodotti ottenuti mediante la violazione di un bene immateriale, cui va applicato il margine di redditività dell'azienda che ha subito l'illecito.

Secondo Trib. Milano, 24 settembre 2014[26], il MOL (Margine Operativo Lordo / EBITDA) costituisce un elemento primario per la determinazione del danno risarcibile nel caso di abusiva utilizzazione di un brevetto di procedimento. La massima giurisprudenziale si rifà ad un parametro essenziale nella valutazione delle aziende, in quanto il MOL è un flusso sia economico che finanziario, tradizionalmente collegato a metodi di valutazione di mercato (che stimano il valore dell'intera azienda, comprensivo dell'indebitamento finanziario - *enterprise value* - moltiplicando il MOL per multipli di mercato di transazioni di aziende comparabili) ovvero ai flussi di cassa scontati[27].

Accanto alla pubblicità ingannevole, rileva anche la pubblicità indiretta o occulta[28], che consiste nella promozione di un prodotto o di un servizio fatta in maniera subdola, cioè non segnalata.

---

[26] *Contraffazione di brevetto e criteri di determinazione del danno,* in *giurisprudenzadelleimprese.it.*

[27] Il MOL/EBITDA è il punto di partenza per la derivazione contabile dei flussi di cassa operativi e poi netti, da scontare al costo del capitale (rispettivamente, medio ponderato o dell'*equity*).

[28] A. Mendola, *Considerazioni sul divieto di pubblicità occulta nell'influencer marketing*, in questa *Rivista,* 2, 2022, 145 ss.

Elenco autori

Nicolò Biligotti
LL.M. candidate, LL.M. in Law of Internet Technology, Università Bocconi; avvocato in Milano
Giovanna Capilli
professoressa associata di diritto privato, Università San Raffaele
Martina Cazzaniga
laureanda in Giurisprudenza, Università degli Studi di Milano-Bicocca
Ginevra Cerrina Feroni
vicepresidente, Autorità garante per la protezione dei dati personali; professoressa ordinaria di diritto pubblico comparato, Università degli Studi di Firenze
Luca Di Majo
ricercatore di istituzioni di diritto pubblico, Università degli Studi della Campania "Luigi Vanvitelli"
Pietro Dunn
dottorando di ricerca in Law, Science and Technology, Università di Bologna
Marina Federico
dottoranda di ricerca in diritto, mercato e persona, Università Ca' Foscari di Venezia
Davide Galliani
professore associato di istituzioni di diritto pubblico, Università degli Studi di Milano
Elena Kaiser
legal advisor, Luxembourg House of Cybersecurity
Marco Ladu
assegnista di ricerca in diritto costituzionale, Università degli Studi di Brescia
Armando Lorusso
assegnista di ricerca in diritto amministrativo, Politecnico di Bari
Roberto Moro-Visconti
professore associato di corporate finance, Università Cattolica del Sacro Cuore di Milano
Giulia Napoli
dottoressa in Giurisprudenza, Università degli Studi della Tuscia
Marco Orofino
professore ordinario di diritto costituzionale, Università degli Studi di Milano
Maria Teresa Paracampo
professoressa associata, Università degli Studi di Bari "Aldo Moro"
Sabrina Peron
avvocato in Milano
Raffaele Torino
professore ordinario di diritto privato comparato, Università degli Studi Roma Tre
Enrico Toti
professore incaricato di diritto cinese, Università degli Studi Roma Tre
Andrea Vigorito
research fellow, Università degli Studi Roma Tre
Lavinia Vizzoni
ricercatrice di diritto privato, Università degli Studi di Pisa
Vincenzo Zeno-Zencovich
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.

mediaLAWS

ANNO 2023 - CODICE ISSN 2532-9146