L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di *digital privacy* come osservatorio privilegiato*

Angelica Bonfanti

Abstract

Il presente studio esamina l'utilizzo di *big data* da parte di forze dell'ordine nello svolgimento delle funzioni di protezione della sicurezza pubblica e prevenzione e repressione del crimine. In particolare ci si focalizza sulle tecniche di polizia predittiva, ossia l'incrocio, mediante algoritmi, di dati immagazzinati attraverso fonti diverse, al fine di prevedere il compimento di reati e la loro localizzazione o elaborare profili criminali individuali. Lo studio intende verificare la compatibilità di simili tecniche con la tutela del diritto alla privacy e la protezione dei dati personali, nella prospettiva del diritto internazionale ed europeo. A questo fine, dopo avere analizzato la nozione di "*big data*" ed esaminato se essi possano essere considerati realmente anonimi, lo studio si focalizza, nella prospettiva descritta, sulla profilazione, la raccolta generalizzata e il trattamento automatizzato dei dati, pratiche alla base delle tecniche di polizia predittiva.

This essay examines the exploitation of big data by law enforcement agencies as a tool for accomplishing to their public security and crime prevention and repression functions. More specifically, it focuses on predictive policing - i.e. a technique that combines, through algorithms, data obtained from different sources in order to elaborate crime hotspots and composite. The essay aims at assessing the consistency of predictive policing with the right to privacy and data protection, as ruled at international and EU level. From this perspective, after analyzing the meaning of "big data" and whether it is really anonymous, it focuses on the techniques employed within predictive policing, such as profiling, automated processing, data retention and storage.

Sommario

* Il presente testo rappresenta una versione ampliata e con l'aggiunta delle note della relazione presentata dall'Autore alla Tavola rotonda su "Big data: prospettive di diritto internazionale e dell'Unione europea" svoltasi nel Dipartimento di giurisprudenza dell'Università di Ferrara il 6 giugno 2018 in occasione del Convegno nazionale della Società italiana di diritto internazionale e dell'Unione europea (SIDI). Su determinazione della direzione, l'articolo è stato pertanto sottoposto a referaggio anonimo.

Keywords

Polizia predittiva, Privacy, Big data, Protezione dei dati, Diritto internazionale

1. L'utilizzo di *big data* per fini di polizia predittiva

I rischi che l'utilizzo di *big data* comporta per la tutela della privacy e la protezione dei dati personali sono noti. Accanto alle criticità legate alla profilazione per fini commerciali, l'utilizzo di *big data* da parte di forze dell'ordine nello svolgimento delle funzioni di protezione della sicurezza pubblica e prevenzione e repressione del crimine merita certamente un'analisi, cui le riflessioni del presente studio si indirizzano. Più in particolare, in questa sede si intendono esaminare le potenziali ingerenze nella protezione del diritto alla privacy e dei dati personali derivanti dall'utilizzo di tecniche che comportano la collezione massiccia di dati, il loro immagazzinamento, la lettura incrociata delle banche dati e, più specificamente, la profilazione per fini di polizia predittiva.

Quest'ultima tecnica consiste nell'incrocio, mediante algoritmi, di dati immagazzinati attraverso fonti diverse, al fine di prevedere il compimento di reati e la loro localizzazione ("*crime hotspot*") o elaborare profili criminali individuali ("*predictive composite*").[1] Tra le fonti rientrano le banche dati elaborate dalle forze dell'ordine o acquisite da *databrokers*, i social networks, internet e gli impianti a circuito chiuso. Gli effetti negativi sulla tutela dei diritti umani connessi all'utilizzo di tecniche di polizia predittiva sono notevoli: in primo luogo, l'individuazione di classi di soggetti a diverso grado di pericolosità ("*social sorting*") implica evidenti rischi di stigmatizzazione e discriminazione. In secondo luogo, come rilevato dal Parlamento Europeo nel 2017, non si può trascurare il rischio di falsi positivi dovuti all'inaccuratezza dei dati processati, con l'effetto che «*low-quality data and/or low-quality procedures behind decision-making processes and analytical tools could result in biased algorithms, spurious correlations, errors, an underestimation of the legal, social and ethical implications*».[2]

Le tecniche in esame sono ampiamente utilizzate. La polizia statunitense si avvale di strategie di prevenzione del crimine fondate sull'utilizzo di algoritmi, con cui perviene a identificare celle geografiche di probabile attività criminale, potendo così incidere significativamente sulla riduzione del crimine. Anche la Danimarca ha recentemente adottato una normativa che potenzia le capacità di intrusione della polizia e dei servizi segreti nei dati personali, attraverso una piattaforma (POL-INTEL) che incrocia le banche dati della polizia e i dati provenienti da investigazioni con quelli acquisiti tramite videocamere, internet, social networks o ottenuti mediante *databrokers* ("*open source collection, hotspot analysis* e *social network analysis*"), realizzando in questo modo una colle-

[1] Si vedano: A. Babuta, *Big Data and Policing. An Assessment of Law Enforcement Requirements, Expectations and Priorities*, in *Royal United Services Institute for Defence and Security Studies*, 2017; M. Mendola, *One Step Further in the 'Surveilance Society': The Case of Predictive Policing*, Tech and Law Center, 17 ottobre 2016.

[2] European Parliament, *Report on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement*, 2016/2225(INI), Committee on Civil Liberties, Justice and Home Affairs, 20 febbraio 2017, par. M.

zione generalizzata di dati e informazioni senza limitazione di scopo.[3] L'elaborazione e la gestione della piattaforma sono affidate a una società privata, la Palantir Technologies, specializzata nell'analisi di dati per operatori privati, agenzie militari, sevizi segreti e forze dell'ordine. Il ricorso a società di analisi private da parte di governi, d'altronde, è frequente. Si pensi ad esempio al governo statunitense che ricorre all'esame di dati provenienti da Facebook, Twitter e altri social networks mediante i servizi offerti da società ICT come Geofeedia, Snaptrends, Dataminr, Madia Sonar, Babel Street, Digital Stakeout, Pathar, Beware, Betwater,[4] e, da ultimo, Cambridge Analytica, come emerso nella vicenda che ha recentemente coinvolto Facebook.[5]

In questo scenario la Cina merita una specifica attenzione: il suo Police Cloud System consente infatti alle forze dell'ordine una sorveglianza capillare e continuativa sui cittadini cinesi. Secondo uno studio condotto da Human Rights Watch, il programma consente di incrociare numerose fonti di informazione, tra cui «*data routinely gathered by China's police, such as residential addresses, family relations, birth control methods, and religious affiliations*» con «*hotel, flight and train records, biometrics, CCTV footage, and information from other government departments and even private companies*».[6] La piattaforma identifica sette categorie di profili potenzialmente pericolosi per il mantenimento di sicurezza e ordine pubblico: «*petitioners, those who 'undermine stability', those who are involved in terrorism, major criminals, those involved with drugs, wanted persons, and those with mental health problems who 'tend to cause disturbances*».[7] Ad esempio il contratto di gestione del Police Cloud di Jinan specifica che la piattaforma analizza profili rintracciati sulla base dell'incrocio di informazioni che concernono «*ethnicity, criminal offense records, and others*», al fine di informarne le forze dell'ordine su base giornaliera o settimanale. Il governo cinese dispone poi di una seconda piattaforma di sorveglianza, la Integrated Joint Operations Platform, specificamente indirizzata a individuare comportamenti 'anomali' da parte degli uiguri, la minoranza musulmana residente nella regione dello Xinjiang.[8]

Infine, anche l'Italia a partire dal 2014 si avvale del programma software Key-Crime, che utilizza algoritmi per individuare potenziali profili criminali. Il sito della Polizia di Stato spiega che «le informazioni – raccolte da interrogatori – sommate all'analisi effettuata fotogramma per fotogramma dei filmati recuperati dagli impianti a circuito chiuso vengono inseriti nell'interfaccia grafica di Key-Crime. L'algoritmo matematico [..] elabora e incrocia tutti i dati […] proponendo al poliziotto una serie di dati che sono potenzialmente collegabili [..] [L]a serie criminale così individuata consente di avere capacità predittive con ottime probabilità di successo».[9]

Le tecniche in esame si inquadrano nel contesto più ampio della sorveglianza statale

[3] In merito *New Legal Framework for Predictive Policing in Denmark,* in *EDRi,* 22 febbriao 2017.

[4] T. Scassa, *Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges*, in *Scripted*, 2017.

[5] V. Ng, *What Next After the Facebook and Cambridge Analytica Revelations?*, 23 luglio 2018.

[6] Human Rights Watch, *China: Police 'Big Data' Systems Violate Privacy, Target Dissent Automated Systems Track People Authorities Claim 'Threatening'*, 19 novembre 2017.

[7] *Ibid.*

[8] M. Wang, *Cambridge Analytica, Big Data and China*, 18 aprile 2018.

[9] *La chiave del crimine*, reperibile a: www.poliziadistato.it.

sugli individui per fini di sicurezza pubblica e nazionale. Al contesto di analisi sono riconducibili, ad esempio, le misure adottate da alcuni Stati per fini emergenziali e di lotta al terrorismo, e poi in maniera sempre più stabile. Esse prevedono la realizzazione di programmi di intercettazione delle comunicazioni di cittadini propri e stranieri e di raccolta generalizzata di dati personali. Tra le misure anche il programma PRISM, già ampiamente commentato in dottrina, con cui il governo statunitense, prima, e quelli inglese e francese, poi, hanno sviluppato un piano di sorveglianza elettronica di massa, duraturo e indifferenziato, per accedere e immagazzinare dati personali di cittadini statunitensi ed europei. [10]

Più recentemente nel rapporto sulla trasparenza pubblicato il 25 maggio 2018 da Apple, la società rivela che nella prima parte dell'anno ha ricevuto dal governo statunitense 16.249 richieste di accesso a dati personali di utenti per fini di sicurezza nazionale, misura doppia rispetto a quella del secondo semestre 2017. Alla medesima tendenza si allineano anche Facebook e Google.[11] Il dato è ancora più inquietante se si considera che nel febbraio 2018 Apple, per adempiere alla legge cinese sulla cyber-security entrata in vigore il 1° giugno 2017, ha trasferito a un server di costituzione locale tutti i dati degli utenti cinesi e le relative chiavi crittografiche. Il fatto è stato ampiamente criticato per la potenzialità che esso implica di comprimere il godimento non solo del diritto alla privacy ma anche di altri diritti umani fondamentali. [12]

Il presente articolo intende svolgere riflessioni sulla compatibilità delle tecniche di polizia predittiva con la tutela del diritto alla privacy e la protezione dei dati personali, nella prospettiva del diritto internazionale ed europeo. A questo fine, dopo avere esaminato la nozione di "*big data*" e verificato se essi possano essere considerati realmente anonimi (§ 2), lo studio analizza la profilazione (§ 3), la raccolta generalizzata (§ 4) e il trattamento automatizzato dei dati (§ 5), pratiche alla base delle tecniche di polizia predittiva, per valutarne le potenzialità lesive nei confronti del diritto alla privacy e della protezione dei dati personali.

2. *Big data*, anonimato e pseudo-anonimato

Prima di entrare nel dettaglio dell'analisi giuridica, è opportuno definire cosa si intenda per "*big data*" e verificarne la natura anonima o la possibile riconduzione a soggetti individuati. Citando le parole del Parlamento Europeo «*big data refers to the collection, analysis and the recurring accumulation of large amounts of data, including personal data, from a variety of*

[10] G. Della Morte, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018, 178 ss.; V. Mitsilegas, *Surveillance and Digital Privacy in the Transatlantic 'War on Terror': The Case for a Global Privacy Regime*, in *Columbia Human Rights Law Review*, 2016, 3 ss.; M. Nino, *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti umani e diritto internazionale*, 2013, 440 ss.; M. Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Oxford, 2017. In generale si veda anche L. Borlini, *Tutela della privacy e protezione dei dati personali a fronte della sicurezza pubblica e dell'integrità del sistema finanziario europeo*, in *Diritti umani e diritto internazionale*, 2017, 23.

[11] S. Nellis, *Apple sees steep increase in U.S. national security requests*, 25 maggio 2018.

[12] Amnesty International, *When Profits Threaten Privacy – 5 Things You Need to Know about Apple in China*, 27 febbraio 2018.

sources, which are subject to automatic processing by computer algorithms and advanced data-processing techniques using both stored and streamed data in order to generate certain correlations, trends and patterns (big data analytics)».[13]

Quanto alla natura anonima degli stessi, è utile, nel contesto del presente studio, riferirsi alla direttiva 2016/680.[14] Essa concerne infatti la protezione dei dati personali nell'ambito delle attività svolte dalla polizia o da altre autorità pubbliche preposte all'applicazione della legge per la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esercizio di poteri per la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. La direttiva stabilisce di applicarsi «a tutte le informazioni relative a una persona fisica identificata o identificabile»,[15] rimanendo pertanto escluse dall suo ambito di regolamentazione le informazioni anonime, ossia le «informazioni che non si riferiscono a una persona fisica identificata o identificabile»[16] o che coinvolgono «dati personali resi sufficientemente anonimi e tali da non consentire più l'identificazione dell'interessato».[17] Per stabilire l'identificabilità di una persona fisica, devono essere presi in considerazione «tutti i mezzi, […], tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici».[18]

L'art. 20 della direttiva prevede che il titolare del trattamento – ossia l'autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvaguardia contro e prevenzione di minacce alla sicurezza pubblica - metta in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte a proteggere in modo efficace i dati e a integrare le necessarie garanzie, avendo considerazione dello stato dell'arte e dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e dei rischi per i diritti e le libertà dell'interessato. L'autorità pubblica in questione deve inoltre adottare misure che garantiscano che solo i dati personali necessari, per quantità, portata del trattamento, periodo di conservazione e accessibilità, siano trattati attraverso impostazioni predefinite.

La pseudonimizzazione consiste nel trattamento dei dati personali tramite cui essi «non poss[o]no più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile».[19] Occorre tuttavia notare che la pseudonimizzazione non garantisce in modo assoluto e definitivo

[13] European Parliament, *Report on fundamental rights implications of big data,* cit., para. A). Sulla nozione di "big data" si veda G. Della Morte, *op. cit.*, 161 ss. e i riferimenti ivi richiamati.

[14] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in OJ L 119, 4 maggio 2016, 89 ss.

[15] Direttiva (UE) 2016/680, cit., considerando 21.

[16] *Ibid.*

[17] *Ibid.*

[18] *Ibid.*

[19] *Ibid.*, art. 3, par. 5.

l'anonimato dei dati personali:[20] permane infatti il rischio, rilevato anche dal Parlamento Europeo, che sia possibile procedere alla «*re-identification of individuals by correlating different types of anonymised data*»,[21] con la conseguenza, evidenziata dallo Special Rapporteur sul diritto alla privacy, che alla domanda «*do de-identification processes deliver data that does not interfere with individuals' information privacy rights?*»[22] si deve inevitabilmente, allo stato attuale, rispondere negativamente.

Con riguardo all'anonimato, occorre infine precisare se e a quali condizioni dati apparentemente non riconducibili a persone identificabili possano essere rivelati. A questo proposito è chiarificatoria la sentenza *Breyer* della Corte di giustizia dell'Unione europea[23] per i rilievi sulla qualificazione degli indirizzi IP dinamici. Secondo la Corte, pur «non rivela[ndo tali indirizzi] direttamente l'identità della persona fisica proprietaria del computer a partire dal quale avviene la consultazione di un sito Internet, né quella di un'altra persona che potrebbe utilizzare detto computer»,[24] esiste tuttavia il rischio che essi vengano incrociati con altre informazioni, divenendo così «un mezzo che può essere ragionevolmente utilizzato per identificare la persona interessata».[25] In pratica «il fornitore di servizi di media online dispon[e] di mezzi che possono essere ragionevolmente utilizzati per identificare, con l'aiuto di altri soggetti, ossia l'autorità competente e il fornitore di accesso a Internet, la persona interessata sulla base degli indirizzi IP conservati».[26] Date queste premesse, anche «un indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce [pertanto] nei confronti di tale fornitore, un dato personale […], qualora [egli] disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui […] dispone».[27] Va infine aggiunto che l'anonimato *online* è legittimo in conformità con le previsioni specifiche dei diritti nazionali e che qualora, come conclude la Corte europea dei diritti dell'uomo nella sentenza *Delfi v. Estonia*,[28] esso sia consentito, «*[t]he release of [personal] information would usually require an injunction by the investigative or judicial authorities and would be subject to restrictive conditions*».[29]

3. *Big data* e profilazione

Sulla base di queste premesse si giustificano le cautele previste dalla direttiva 2016/680

[20] Sulla distinzione tra dati anonimi e pseudo-anonimi G. Della Morte, *op. cit.*, 156 ss.

[21] European Parliament, *Report on fundamental rights implications of big data*, cit., par. 7.

[22] *Report of the Special Rapporteur on the right to privacy*, A/72/43103, 19 ottobre 2017, par. 95.

[23] CGUE, C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland* (2016). In merito: D. Marrani, *Dati personali e cybersicurezza: la decisione Breyer della Corte di giustizia*, in *SIDIBlog*, 11 aprile 2017.

[24] CGUE, *Breyer c. Bundesrepublik Deutschland*, cit., § 38.

[25] *Ibid.*, § 45.

[26] *Ibid.*, § 48.

[27] *Ibid.*, § 49.

[28] CEDU, *Delfi AS v. Estonia,* ric. 64569/09 (2015).

[29] *Ibid.*, § 148.

in materia di "profilazione", ossia il «trattamento automatizzato di dati personali consistente [nel loro] utilizzo […] per valutare determinati aspetti personali relativi a una persona fisica, in particolare […] riguardanti il [suo] rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti».[30] L'art. 11 della direttiva vieta che le decisioni assunte da forze dell'ordine si fondino «unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato». Occorrono pertanto garanzie adeguate, tra cui «almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento».[31] È invece da considerarsi del tutto illegittima la profilazione che conduce alla «discriminazione di persone fisiche sulla base di categorie particolari di dati personali».[32]

I rischi legati all'utilizzo di tecniche di profilazione sono evidenti. Secondo il Parlamento Europeo, innanzitutto, vi è «*the risk of data being used for discriminatory or fraudulent purposes and the marginalisation of the role of humans in these processes, leading to flawed decision-making procedures that have a detrimental impact on the lives and opportunities of citizens, in particular marginalised groups, as well as bringing about a negative impact on societies and businesses*».[33] Ciò ha l'effetto di rendere l'utilizzo di *big data* capace di causare non solo violazioni dei diritti individuali fondamentali, ma anche trattamenti discriminatori o discriminazioni indirette nei confronti di gruppi di persone con caratteristiche simili, e in particolare nell'ambito dell'accesso all'istruzione o al lavoro o nella valutazione delle loro preferenze in qualità di consumatori.[34]

Anche la Corte europea dei diritti dell'uomo evidenza i rischi di stigmatizzazione connessi all'immagazzinamento di dati e informazioni personali. Nella sentenza *S. and Marper v. The United Kingdom* essa perviene alla conclusione che «*the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8*».[35] Più precisamente, essa ravvisa un sensibile rischio «*stemming from the fact that persons […] who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons*».[36] E questo anche pur essenso vero che «*the retention of the applicants' private data cannot be equated with the voicing of suspicions*»[37]: infatti la «*perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed*».[38]

---

30 Direttiva (UE) 2016/680, cit., art. 3, par. 4.

31 *Ibid*., considerando 38.

32 *Ibid*., art. 11, par. 3, e considerando 38.

33 European Parliament, *Report on fundamental rights implications of big data*, cit., par. M.

34 *Ibid*., par. 19.

35 CEDU, *S. and Marper v. the United Kingdom*, ric. 30562/04 e 30566/04 (2008), § 67. In merito: I. Voina-Motoc, *La génétique et l'article 8 de la CEDH: la généalogie de Marper c Royaume Uní dans le droit international*, in J. Casadevall-G. Raimondi-E. Fribergh-P. Titiun-P. Kempees-J. Darcy (eds.), *Mélanges en l'honneur de Dean Spielmann: liber amicorum Dean Spielmann*, Oisterwijk, 2015, 399 ss.

36 CEDU, *S. and Marper v. the United Kingdom*, cit., § 122

37 *Ibid.*

38 *Ibid.*

Infine, come evidenziato nelle conclusioni dell'Avvocato Generale alla Corte di giustizia dell'Unione europea sulla domanda di parere 1/15, profilazione e trattamento automatizzato possono determinare il pericolo che «modelli comportamentali predefiniti "a rischio" o "preoccupanti", collegati ad attività terroristiche e/o di criminalità transnazionale grave» conducano a «identificare persone fino a quel momento sconosciute ai servizi di polizia o non sospette»[39] e ingenerino «la spiacevole sensazione che tutti […] siano trasformati in potenziali sospetti».[40] Se si pensa all'Accordo PNR tra UE e Canada,[41] oggetto del Parere 1/15 – su cui si tornerà a breve – l'ingerenza riguarda infatti, «in modo sistematico, tutti i passeggeri che usufruiscono dei collegamenti aerei tra il Canada e l'Unione europea, vale a dire varie decine di milioni di persone all'anno», ed è evidente che «il trasferimento di quantitativi ingenti di dati personali dei passeggeri aerei, in cui sono compresi dati delicati, che necessitano, per definizione, di un trattamento automatizzato, nonché la [loro] conservazione […] per un periodo di cinque anni, mira[no] [proprio] a consentir[n]e un confronto, eventualmente retrospettivo». [42] Avendo pertanto concluso che l'utilizzo automatizzato di dati e il ricorso alla profilazione a fini di polizia predittiva devono essere debitamente regolati, rimane da indagare se e a quali condizioni l'immagazzinamento generalizzato degli stessi e la loro consultazione ed elaborazione possano essere considerati leciti.

4. La raccolta generalizzata di dati

La direttiva 2016/680, il GDPR[43] e la Convenzione europea dei diritti dell'uomo ("CEDU") legittimano restrizioni del diritto alla privacy e della protezione dei dati personali per esigenze di sicurezza pubblica.[44] Per quanto concerne la CEDU, il suo art. 8, par. 2, stabilisce l'illegittimità dell'ingerenza delle autorità pubbliche nel diritto alla privacy salvo che essa «sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui». La direttiva

[39] CGUE, parere 1/15, Conclusioni dell'Avvocato Generale Paolo Mengozzi presentate l'8 settembre 2016, § 176.

[40] *Ibid.*

[41] Proposta di decisione del Consiglio relativa alla conclusione dell'accordo tra il Canada e l'Unione europea sul trasferimento e sul trattamento dei dati del codice di prenotazione [COM(2013) 528 final].

[42] *Ibid.*

[43] Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, in OJ L 119, 4 maggio 2016, 1 ss. ("GDPR").

[44] M. Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Era*, in *Harvard International Law Journal*, 2015, 56 ss., spec. 81; A. Terrasi, *Il rapporto tra diritto alla privacy e protezione dei dati personali tra Corte di Giustizia dell'Unione Europea e Corte Europea dei Diritti dell'Uomo*, in M. Distefano (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale. Temi scelti*, Napoli, 2017, 127; M. Weiler, *The Right to Privacy in the Digital Age: the Commitment to Human Rights Online*, in *German Yearbook of International Law*, 2014, 651 ss. In generale: J. Carrascosa González*, The Internet – Privacy and Rights Relating to Personality*, *in Collected Courses of The Hague Academy of International Law*, Leiden/Boston, v. 378, 2016; L.A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford, 2014.

2016/680 segue lo stesso orientamento e autorizza gli Stati membri ad adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato o a limitare, in tutto o in parte, il suo diritto di accesso o di rettifica o cancellazione,[45] se e per il tempo in cui ciò costituisca «una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di: a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui».[46] Analogamente l'art. 23 del GDPR legittima la compressione dei diritti riconosciuti, purché essi rispettino «l'essenza dei diritti e delle libertà fondamentali e sia[no] una misura necessaria e proporzionata in una società democratica» per garantire la sicurezza pubblica e nazionale e la prevenzione, l'indagine, l'accertamento o il perseguimento di reati.

I principi citati trovano applicazione in alcune importanti decisioni della Corte di giustizia dell'Unione europea. Particolarmente significative nel presente contesto sono le sentenze *Digital Rights*[47] e *Tele 2 Sverige*.[48] Secondo la prima, la direttiva 2006/24[49] – che obbliga i *service providers* a conservare per un certo periodo dati relativi agli utenti e prevede l'accesso ad essi da parte delle autorità nazionali, senza indicare criteri obiettivi che limitino «il numero di persone che [dispongono] dell'autorizzazione di accesso o l'uso dei dati conservati a quanto strettamente necessario alla luce dell'obiettivo perseguito»[50] – è invalida in quanto determina un'ingerenza «di vasta portata» e «particolarmente grave» nei diritti sanciti dagli artt. 7 e 8 della Carta europea dei diritti fondamentali dell'Unione europea.[51] Pur riconoscendo la legittimità dell'obiettivo della direttiva – ossia quello di contribuire alla lotta contro la criminalità grave – la Corte conclude che l'ingerenza nei diritti individuali procurata dalla direttiva non è necessaria e proporzionale. È infatti indiscutibile che «tenuto conto della crescente importanza dei mezzi di comunicazione elettronica, i dati che debbono essere conservati […] permettono alle autorità nazionali competenti in materia di perseguimento di reati di disporre di possibilità supplementari di accertamento dei reati gravi e […] costituiscono quindi uno strumento utile per le indagini penali».[52] Tuttavia, anche ammettendo che «la lotta contro la criminalità grave [è] di capitale importanza per garantire la sicurezza pubblica» e «la sua efficacia [dipende] in larga misura dall'uso delle moderne tecniche

[45] Direttiva 2016/680, cit., considerando 44.

[46] *Ibid*., art. 13.

[47] CGUE, C-293/12, *Digital Rights Ireland* (2014).

[48] CGUE, C-203/15 e C-698/15, *Tele2 Sverige AB c. Postoch telestyrelsen e Secretary of State for the Home Department c. Tom Watson, Peter Brice, Geoffrey Lewis* (2016).

[49] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

[50] CGUE, *Digital Rights Ireland*, cit., § 62.

[51] *Ibid*., § 37.

[52] *Ibid*., § 49.

di indagine»,[53] la Corte conclude che «simile obiettivo di interesse generale, per quanto fondamentale, non può di per sé giustificare il fatto che una misura di conservazione, come quella istituita dalla direttiva 2006/24, sia considerata necessaria». Pertanto occorre che siano previste regole chiare e precise che disciplinino l'applicazione delle misure e impongano garanzie sufficienti contro il rischio di abusi, accessi e usi illeciti ai danni dei titolari dei dati. È inoltre preclusa la possibilità – che la direttiva configura – di effettuare raccolte di dati che concernano «in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica, nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi» e che conseguentemente coinvolgano «anche […] persone per le quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché indiretto o lontano, con reati gravi».[54] Infine la Corte censura la direttiva perché essa non stabilisce che «l'accesso ai dati conservati da parte delle autorità nazionali competenti [sia] subordinato ad un previo controllo effettuato da un giudice o da un'entità amministrativa indipendente».[55]

Analogamente, nella sentenza *Tele 2 Sverige* del 21 dicembre 2016, la Corte di giustizia conclude che le normative svedese e inglese di recepimento della direttiva sopra citata, che obbligano i *service providers* a conservare in maniera generalizzata i dati degli abbonati, «travalica[no] i limiti dello stretto necessario e non [possono] essere considerat[e] giustificat[e], in una società democratica».[56] La Corte ritiene invece legittima l'adozione da parte di uno Stato membro di una normativa che consenta «a titolo preventivo, la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta contro la criminalità grave, a condizione che la conservazione dei dati sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario»,[57] ossia purché essa «preveda norme chiare e precise che disciplinino la portata e l'applicazione di una siffatta misura di conservazione dei dati e fissino un minimo di requisiti, di modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti tali da permettere di proteggere efficacemente i loro dati perso-

[53] *Ibid.*, § 51.

[54] *Ibid.*

[55] Sulla sentenza: F. Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, in *Harvard Human Rights Journal*, 2015, 65 ss.; G. Caggiano, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *questa Rivista*, 2, 2018, 64 ss.; L. Seminara, *Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani*, *ivi*, 141 ss.; M. P. Granger-K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, in *European Law Review*, 2014, 835 ss.; T. Konstadinides, *Mass Surveillance and Data Protection in EU Law - the Data Retention Directive Saga*, in M. Bergström, A. Jonsson Cornell, *European Police and Criminal Law Co-Operation*, Oxford, 2014, 69 ss.; M. Nino, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di 'data retention'*, in *Il diritto dell'Unione Europea*, 2014, 803 ss.

[56] CGUE, *Tele2 Sverige*, cit., § 107.

[57] *Ibid.*, § 108.

nali contro i rischi di abuso».[58]

Anche la giurisprudenza sull'art. 8 della Corte europea dei diritti dell'uomo perviene a conclusioni analoghe. Più in particolare, quanto alla potenzialità lesiva del diritto alla privacy di misure di sorveglianza generalizzata, nel caso *Roman Zakharov c. Russia* la Corte aggiunge che «*the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures*»[59] configura di per sé una violazione del diritto alla privacy se l'intercettato appartiene a un «*group of persons targeted by the contested legislation*» o se la stessa «*directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted*».[60]

5. Il trattamento automatizzato dei dati PNR

Le considerazioni svolte trovano una propria specifica applicazione con riferimento alla raccolta generalizzata di dati connessi ai cosiddetti "*Passengers Name Records*" (PNR), ossia i dati e le informazioni relative ai codici di prenotazione di biglietti aerei. L'immagazzinamento e l'accesso a questi dati da parte di autorità pubbliche, anche non europee – pratica certamente utile ai fini di polizia predittiva – sono disciplinati da alcuni strumenti giuridici che meritano di essere specificamente presi in considerazione in questo contesto. In particolare ci si riferisce alla direttiva 2016/681 ("Direttiva PNR")[61] e agli accordi conclusi tra Unione europea e Australia,[62] Stati Uniti[63] e Canada.[64]

I dati desumibili dai codici PNR sono molteplici: essi variano a seconda della compagnia aerea e possono includere informazioni sul viaggio e l'identità dei passeggeri, la data del volo, i recapiti, le modalità di pagamento, i posti assegnati, o informazioni di carattere etnico, religioso e sanitario connesse alla scelta del pasto o alla richiesta di servizi aggiuntivi.[65] Nonostante i dati siano non verificati – e dunque non necessariamente

[58] *Ibid*., § 109.

[59] CEDU, *Roman Zakharov c. Russia*, ric. 47143/06 (2015). In merito E. Psychogiopoulou, *The European Court of Human Rights, Privacy and Data Protection in the Digital Era*, in M. Brkan-E. Psychogiopoulou (eds.), *Courts, Privacy and Data Protection in the Digital Environment*, Cheltenham-Northampton, 2017, 32.

[60] *Ibid*., § 171. Sul punto, V. Mitsilegas, *op. cit.*, 22.

[61] Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, in OJ L 119, 4 maggio 2016, 132 ss. In merito: F. Di Matteo, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella direttiva PNR?*, in *Diritti umani e diritto internazionale*, 2017, 213 ss.

[62] Decisione 2012/472/UE del Consiglio, del 26 aprile 2012, relativa alla conclusione dell'accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al dipartimento degli Stati Uniti per la sicurezza interna, in OJ 2012, L 215, 4. In merito, V. Mitsilegas, *op. cit.*, 25.

[63] Decisione 2012/381/UE del Consiglio, del 13 dicembre 2011, relativa alla conclusione dell'accordo tra l'Unione europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione (*Passenger Name Record* – PNR) da parte dei vettori aerei all'Agenzia australiana delle dogane e della protezione di frontiera, in OJ 2012, L 186, 3.

[64] Proposta di decisione del Consiglio relativa alla conclusione dell'accordo tra il Canada e l'Unione europea sul trasferimento e sul trattamento dei dati del codice di prenotazione, cit.

[65] F. Di Matteo, *op. cit.*, 215.

affidabili – in quanto rilasciati dal passeggero al momento dell'acquisto del biglietto o del check-in, il loro studio incrociato rappresenta una fonte di informazione utile a fini investigativi nei confronti di individui sospettati o accusati di commettere atti criminali. A seguito di un percorso legislativo lungo e complesso, iniziato nel 2007 e inframmezzato dalle commentate pronunce della Corte di giustizia, l'Unione europea il 27 aprile 2016 ha adottato la Direttiva PNR. Essa presenta indubbiamente elementi di miglioramento rispetto alle censure mosse alle prime proposte,[66] quanto meno con riferimento alla limitazione degli obblighi di raccolta e scambio dei dati PNR ai soli voli extra-europei (mentre per quelli europei le pratiche in questione rimangono facoltative),[67] all'elencazione tassativa dei "reati gravi" per il perseguimento dei quali la raccolta e lo scambio si giustificano[68] e alla limitazione temporale della loro conservazione.[69] Ciò nonostante, come già rilevato in dottrina,[70] la direttiva continua a presentare profili di rischio per la tutela dei diritti individuali, sostanzialmente dovuti alla circostanza che, sia pur con le menzionate limitazioni, il suo obiettivo e le pratiche che essa disciplina consistono proprio nella raccolta generalizzata, nell'utilizzo e nella trasmissione di dati, il cui incrocio potrebbe portare a ingiustificate ingerenze nel diritto alla privacy dei passeggeri e nella protezione dei loro dati personali o alla stigmatizzazione di determinati profili o categorie.

Simili preoccupazioni sono peraltro alla base del già citato Parere 1/15 adottato dalla Corte di giustizia il 26 luglio 2017 con riferimento alla compatibilità dell'accordo internazionale tra Unione europea e Canada sul trasferimento e l'utilizzo di dati PNR, all'epoca in corso di negoziazione, con gli articoli 7, 8 e 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16 del Trattato sul funzionamento dell'Unione europea.[71] Con specifico riferimento al trattamento automatizzato di dati PNR, il Parere sottolinea alcuni aspetti di indubbia criticità. Il primo concerne l'inaffidabilità dei dati e delle informazioni, l'analisi dei quali, condotta sulla base di modelli e criteri prestabiliti, può presentare sensibili margini di errore. Nonostante l'art. 15 dell'Accordo preveda infatti che il Canada non prenda «*decisions significantly adversely affecting a passenger solely on the basis of automated processing of PNR data*», secondo la Corte è proprio la natura e la formulazione di modelli e criteri prestabiliti a determinare il livello dell'interferenza con la tutela dei diritti di cui agli articoli 7 e 8 della Carta.[72] Pertanto è indispensabile che tali modelli e criteri siano specifici e affidabili e che si limitino a consentire l'individuazione di soggetti «*who might be under a 'reasonable suspicion' of participation*

[66] *Ibid*., 230 ss.

[67] Direttiva (UE) 2016/681, cit., considerando 10 e artt. 1 e 2.

[68] *Ibid*., art. 3, par. 9.

[69] *Ibid*., art. 12.

[70] P. De Hert-V. Papakonstantinou, *Repeating the Mistakes of the Past Will Do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and the Unsatisfactory Current Data Protection*, in *New Journal of European Criminal Law*, 2014, 160; F. Di Matteo*, op. cit*., 254 ss.

[71] CGUE*,* parere 1/15, 26 luglio 2017; Proposta di decisione del Consiglio relativa alla conclusione dell'accordo tra il Canada e l'Unione europea sul trasferimento e sul trattamento dei dati del codice di prenotazione, cit.

[72] CGUE, parere 1/15, cit., § 172.

in terrorist offences or serious transnational crime», senza implicare effetti discriminatori.[73] Come sottolineato a questo riguardo dall'Avvocato Generale Mengozzi «[l]a disciplina e la determinazione precisa degli scenari e dei criteri di valutazione prestabiliti devono poter consentire, in gran parte, di raggiungere risultati che abbiano come obiettivo individui sui quali potrebbe gravare un «sospetto ragionevole di partecipazione a reati di terrorismo o a reati gravi di natura transnazionale».[74] Considerati i margini di errore, affinché i risultati possano costituire l'oggetto di provvedimenti nei confronti dei passeggeri, è indispensabile inoltre che essi formino l'oggetto di «*individual re-examination by non-automated means*».[75] Evidenziati gli aspetti incompatibili dell'Accordo con il diritto europeo, la Corte ritiene dunque che, pur essendo di per sé legittimi il trasferimento e il trattamento automatico di dati PNR, essi debbano essere condotti nel rispetto di alcune garanzie fondamentali finalizzate a proteggere l'individuo e a evitare che i passeggeri, tutti e indistintamente, possano nella prassi essere trattati come sospetti.

6. Conclusioni

Esaminati i profili di incompatibilità delle tecniche di polizia predittiva con la tutela di privacy e dati personali, chi scrive condivide le conclusioni per cui «*pseudomysation is likely to be the only way to perform big data analytics on personal datasets while complying with data protection law*».[76] Nonostante il presunto anonimato dei dati e delle rilevazioni sui medesimi condotte, l'utilizzo di *big data*, come dimostrato, è suscettibile di causare violazioni dei diritti individuali connessi alla potenziale re-identificazione dei loro titolari. Ciò grazie a incroci di database o tecniche di re-identificazione capaci di ricondurre le informazioni a un singolo individuo o a un profilo criminale. È dunque opportuno che le tecniche di polizia predittiva siano condotte con «*greater algorithmic accountability and transparency*»,[77] ossia mediante la predisposizione di misure tecniche e operative che assicurino la trasparenza ed evitino conseguenze negative in tema di discriminazione e violazione del diritto alla privacy e presunzione di innocenza, effetti che potrebbero altrimenti discendere da decisioni automatizzate su comportamenti individuali. Solo il rispetto di simili garanzie può eliminare, o quanto meno ridurre, i profili di incompatibilità delle tecniche in esame con la tutela dei diritti fondamentali, legittimando il ricorso da parte delle forze dell'ordine a pratiche che indiscutibilmente offrono grandi potenzialità nella lotta al crimine e nel mantenimento della sicurezza pubblica.

[73] *Ibid.*

[74] CGUE, parere 1/2015, Conclusioni dell'Avvocato Generale Paolo Mengozzi, cit., § 256.

[75] CGUE, parere 1/2015, cit., § 173.

[76] A. Babuta, *op. cit.*, 35.

[77] European Parliament, *Report on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement*, cit., par. 8.