PRIVACY, DIRITTI DELLA PERSONA E PROCESSO PENALE [1]

1. – I rapporti tra «*diritto alla privacy*» e sistema processuale penale hanno assunto consistenza e richiamato l'attenzione degli interpreti solo a partire dagli ultimi decenni [2]. Ancora i compilatori del codice di rito del 1988, quando ponevano lo sguardo (per trarne ispirazione) verso i grandi princìpi della procedura anglo-americana, individuavano come essenziali – per richiamarne solo alcuni – i canoni dello *ius tacendi*, del contraddittorio, dell'oralità. Per contro, le prerogative in materia di *privacy* rimanevano ancora sullo sfondo dell'impianto riformato, al più riecheggiando nella disciplina delle intercettazioni o in pochi altri istituti.

Del resto, un discorso analogo – e a maggior ragione – può essere svolto con riferimento all'idea di giustizia penale racchiusa nella Carta fondamentale. Il processo criminale disegnato dai costituenti non poteva non risentire dell'assenza del diritto in questione nella trama della nostra *Grundgesetz*. Se è vero, infatti, che diverse previsioni (tra cui *in primis* l'art. 2 Cost.) possono fungere da ombrello di tutela anche per la «riservatezza», è altrettanto indiscutibile che la Costituzione disciplini in modo espresso soltanto le «tradizionali libertà «negative» (libertà personale, di domicilio e di corrispondenza)» [3].

Dagli anni Novanta dello scorso secolo, la situazione ha iniziato a cambiare radicalmente in virtù della intensa dilatazione interpretativa – che peraltro non accenna a diminuire – della nozione di *privacy* e del suo

---

[1] Testo della relazione svolta al XXXII Convegno della «Associazione tra gli studiosi del processo penale G.D. Pisapia» dedicato a «Diritti della persona e nuove sfide del processo penale» (Università degli Studi di Salerno, 25-27 Ottobre 2018).

[2] Per un approccio generale sul rapporto tra riservatezza/*privacy* e processo penale: M. Bonetti, *Riservatezza e processo penale*, Milano 2003. Di recente, nell'universo di *common law*, D. Marshall, T. Thomas, *Privacy and Criminal Justice*, Basingstoke 2017.

[3] Sul punto cfr. G. Silvestri, *L'individuazione dei diritti della persona*, in *Dir. pen. cont.* 29 ottobre 2018, 1.

perimetro applicativo (4). Un fenomeno che ha finito per estendere i suoi effetti anche all'interno del giardino, sino ad allora quasi proibito, del processo penale italiano: la *privacy* appare oggi una garanzia in profonda (e continua) espansione, in un moto «controcorrente» rispetto a salvaguardie più «classiche» del rito penale (si pensi solo al diritto al confronto con l'accusatore e all'assistenza tecnica di un difensore) che, invece, attraversano una fase, per così dire, recessiva, testimoniata dalla più recente giurisprudenza di Strasburgo (5).

Invero, è in particolare la repentina avanzata tecnologica ad aver condotto il diritto alla privatezza a fare i conti *vis-à-vis* con sfide inedite e con la necessità di adattarsi al passare dei tempi, venendo a gemmare sempre nuovi corollari. Un esempio per tutti, su cui si avrà modo di ritornare: la *privacy* rappresenta oggi (sorprendentemente?) il baluardo in grado di proteggere l'individuo contro l'avanzata incontrollata di alcune forme «aggressive» di intelligenza artificiale, in grado di travolgere i pilastri di garanzia in vari campi del diritto, tra cui anche la procedura penale.

A livello più generale, per avere una precisa riprova di quanto il diritto in esame abbia assunto un ruolo chiave nella protezione del singolo di fronte al progresso tecnologico, basti pensare alle molteplici fondamentali pronunce in cui la Corte di giustizia di Lussemburgo si è occupata della tematica *de qua* negli ultimi anni, talune anche aventi diretta rilevanza processuale penale (6).

---

(4) Il quadro europeo in materia viene ricostruito, ad esempio, in P. Beckerhoff, *Reform des europäischen Datenschutzrechts. Ein Überblick unter besonderer Berücksichtigung des Datenaustausches zwischen Polizei-, Strafjustiz – und Geheimdienstbehörden*, in *EUCRIM* 2017, 88 ss.; European Union Agency for Fundamental Rights, *Handbook on European data protecton law*, Lussemburgo 2018; Aa. Vv. *Privacy, Data Protection and Cybersecurity in Europe*, a cura di W.J. Schünemann, M.O. Baumann, Cham 2017.

(5) Cfr. C. dir. uomo, Grande Camera, 9 novembre 2018, Beuze c. Beglio; C. dir. uomo, Grande Camera, 13 settembre 2016, Ibrahim c. Regno Unito; C. dir. uomo, Grande Camera, 15 dicembre 2015, Schatschaschwili c. Germania; C. dir. uomo, Grande Camera, 15 dicembre 2011, Al-Khawaja e Tahery c. Regno Unito. In tema, da ultimo, rispettivamente, R. Casiraghi, *I nuovi approdi «europei» del diritto al confronto*, in *Cass. pen*. 2019, 1363 ss. e P. Maggio, *La Corte europea dei diritti dell'uomo promuove una versione «debole» del diritto di accesso al difensore?*, *ivi*, 1271 ss. Più in generale, sul progressivo arretramento della giurisprudenza di Strasburgo con riguardo a plurime garanzie procedurali, cfr. M. Caianiello, *You Can't Always Counterbalance What You Want*, in *European Journal of Crime, Criminal Law and Criminal Justice* 2017, 283 ss.

(6) Cfr. M. Bassini, O. Pollicino, *Commento all'art. 8 della Carta*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini, *Carta dei diritti fondamentali dell'Unione europea*, Milano 2017, 141 ss.; G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in G. Resta, V. Zeno-Zencovich, *La protezione transnazionale dei dati personali. Dai* «Safe Harbour Principles»

Si ricordi, solo per offrire qualche esempio, la sentenza della Grande Sezione dell'8 aprile 2014 *Digital Rights Ireland* (7), con la quale è stata invalidata la direttiva sulla *data retention* n. 2006/24/CE per contrasto con gli articoli 7, 8 e 52, par. 1 della Carta di Nizza; la sentenza *Google Spain SL* (8), in materia di diritto all'oblio; e, non meno importante, la pronuncia del 6 ottobre 2015, *Schrems* contro *Data Protection Commissioner* (9), con cui la decisione della Commissione 2005/520 è stata a sua volta dichiarata invalida, sulla base della considerazione per cui l'ordinamento giuridico degli Stati Uniti non garantiva un livello di tutela del diritto alla protezione dei dati personali adeguato agli *standards* UE.

Rimanendo sempre nell'orbita dell'Unione, dal punto di vista normativo viene altresì in rilievo il pacchetto di misure per la protezione dei dati, adottato nel 2016, di cui fanno parte il ben noto «GDPR» (*General Data*

---

al «Privacy Schield», Roma 2016, 113 ss.; J. Kokott, C. Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law* 2013, 222 ss.

(7) Si veda C. Giust. UE, Grande Sezione, 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, sulla quale cfr. L. Trucco, Data retention: *la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it*. 2014, 8-9, 1850 ss.; R. Flor, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont. – Riv. trim.* 2/2014, 178 ss.; 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 U.S.*, in *Harvard Human Rights Journal* 2015, 65 ss.

(8) Cfr. C. Giust. UE, 13 maggio 2014, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos e Mario Costeja Gonzàlez*. Sul punto: M. Bassini, *Google davanti alla Corte di giustizia: il diritto all'oblio*, in *Quad. cost*. 2014, 730 ss.; M. Álvarez Caro, *Reflexiones sobre la sentencia del TJUE en el asunto «Mario Costeja» (C-131/12) sobre derecho al olvido*, in *Revista española de derecho europeo* 2014, 165 ss.; G. Finocchiaro, *La giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems*, in *Il diritto dell'informazione e dell'informatica* 2015, 779 ss.; C. Kuner, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines*, in *LSE Legal Studies Working Paper* 2015, n. 3, 1 ss.; A. L. Valvo, *Il diritto all'oblio nell'epoca dell'informazione «digitale»*, in *Studi sull'integrazione europea* 2015, 355 ss. F. Viglianisi, *La sentenza Google Spain e il diritto all'oblio nello spazio giuridico europeo*, in *Contratto e impresa* 2015, 159 ss.

(9) C. Giust. UE, 6 ottobre 2015, C-362/14, *Schrems* c. *Data Protection Commissionner*, sulla quale cfr. R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giur. cost*. 2016, 289 ss.; R. Kurt, M. Roland, *Nach der Aufhebung der Safe-Harbor-Entscheidung – was jetzt?*, in *Österreichisches Recht der Wirtschaft* 2015, 691 ss.; M. Nino, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE*, in *Il diritto dell'Unione europea* 2016, 755 ss.; Y. Padova, *Le Safe Harbor est invalide. Et après? Analyse des fondements de l'arrêt de la CJUE et de ses conséquences*, in *Droit de l'immatériel: informatique, médias, communication* 2015, 50 ss.

Protection Regulation – Regolamento europeo 2016/679 (10)), e, soprattutto, per quanto qui interessa, la Direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia (Direttiva 2016/680) (11). Nel 2018 è stato poi finalmente approvato anche il Regolamento 2018/1725, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati (12). Infine, risulta tutt'ora in fase di negoziazione il cosiddetto Regolamento *ePrivacy*, ossia l'atto con cui l'Unione si prefigge di abrogare la Direttiva 2002/58/CE e adottare una disciplina specifica – coerente con il GDPR – volta a «fornire un elevato livello di tutela della vita privata per gli utenti dei servizi di comunicazione elettronica e condizioni di parità per tutti gli operatori del mercato» (13).

Sul fronte CEDU, non si può invece non porre mente alla sentenza *Big Brother Watch* v. *Regno Unito* (14), relativa al caso «*Datagate*», generato dalle rilevazioni di Snowden concernenti l'esistenza di programmi di sorveglianza di massa condotti da alcuni Stati europei e dagli U.S.A. In tale occasione, la Corte Edu, rifacendosi espressamente a quanto affermato dalla Corte di giustizia nel caso *Digital Rights Ireland*, è arrivata a ritenere la normativa inglese contrastante con l'art. 8, posto che la legislazione nazionale non è stata considerata in grado di assicurare una protezione

---

(10) In *G.U.U.E.* 4 maggio 2016, L 119/1. Per i dovuti riferimenti dottrinali sul punto: Aa. Vv., *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. Finocchiaro, Bologna 2017; Aa. Vv., *GDPR e normativa* privacy. *Commentario*, a cura di G.M. Riccio, G. Scorza, E. Belisario, Milano 2018.

(11) In *G.U.U.E.* 4 maggio 2016, L 119/89, sulla quale cfr. C.C. Cocq, *Eu Data Protection Rules Applying to Law Enforcement Activities. Towards an Harmonised Legal Framework?*, in *New Journal of European Criminal Law* 2016, 263 ss.; C. Di Francesco Maesa, *Balance Between Security and Fundamental Rights Protection: an Analysis of the Directive 2016/680 for Data Protection in the Police and Justice Sectors and the Directive 2016/681 of the Use of Passenger Name Record (PNR)*, in *www.eurojus.it*; P. de Hert, V. Papakonstantinou, *The New Police and Criminal Justice Data Protection Directive. A First Analysis*, in *New Journal of European Criminal Law* 2016, 7 ss.

(12) In *G.U.U.E.* 21 novembre 2018, L 295/39.

(13) Così, espressamente, la *relazione introduttiva* alla proposta di regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la Direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM (2017) 10 final.

(14) Cfr. C. dir. uomo, Sez. I, 13 settembre 2018, *Big Brother Watch e altri* v. *Regno Unito*. Tra i vari commenti si vedano T. Christakis, *A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on The Big Brother Watch Judgment*, in *www.europeanlawblog.eu* 20 settembre 2018; M. Tzanou, *Big Brother Watch and others v. the United Kingdom: A Victory of Human Rights over Modern Digital Surveillance?*, in *www.verfassungsblog.de* 18 settembre 2018.

efficace contro il rischio di abusi, eccedendosi quindi i limiti imposti dal principio di proporzionalità (15).

Ma v'è di più. Nel 2018 si è assistito ad una vera e propria rivoluzione sul punto anche oltreoceano. Ci si riferisce all'approvazione negli Stati Uniti del cosiddetto *Cloud Act* (16) (*Clarifying Lawful Overseas Use of Data Act*), che ha reso molto più agevole alle autorità nordamericane l'acquisizione di dati direttamente dai *service provider* (17). Come noto, tale novella ha incontrato l'opposizione di molteplici organizzazioni statunitensi, come l'*American Civil Liberties Union* (ACLU), autrice della «*Coalition Letter on Cloud Act*», in cui si affermava che la stessa «*would place too much authority in the hands of the executive branch with few mechanisms to prevent abuse*» (18).

Insomma, già il veloce affresco di fonti pare abbia consentito di mettere a fuoco quello che costituirà il *file rouge* della presente analisi, ossia la considerazione che la tematica della *privacy* non costituisce più un argomento di nicchia, destinato a rimanere ai margini delle riflessioni sul processo penale, ma, anzi, possiede profonde radici e interconnessioni nella nostra materia, di cui non si può più non tenere debito conto.

2. – Questa breve rappresentazione di scenario, accompagnata da un (necessariamente) disorganico catalogo di fonti e arresti giurisprudenziali, corre tuttavia il rischio di generare confusione se non opportunamente corredata da un'analisi dell'attuale portata teorica del concetto di *privacy*, operazione che deve essere svolta attraverso, per così dire, un ritorno alle origini.

Il termine «*privacy*» possiede radici risalenti, come tutti sanno. Ben più di un secolo fa Samuel Warren e Louis Brandeis scrivevano il celeberrimo saggio «*The right to privacy*» (19), in cui compariva la primigenia idea di un

---

(15) Va, peraltro, ricordato che il ricorso in questione è stato di recente rimesso alla Grande camera, la quale – al momento di licenziare il presente scritto – deve ancora pronunciarsi.

(16) Cfr. J. Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, in *Stanford Law Review Online* 2018, 9 ss.; Ead., *Unpacking the CLOUD ACT*, in *EUCRIM* 2018, 4, 220; J. Garland, A. Berengaut, K. Goodloe, *CLOUD Act Creates New Framework for Cross-Border Data Access*, in *www.insideprivacy.com* 26 marzo 2018; S.P. Mulligan, *Cross-Border Data Sharing Under the CLOUD Act*, *Congressional Research Service* 23 aprile 2018.

(17) Sulle implicazioni di tale complessa tematica, si rinvia a Aa. Vv., Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, a cura di L. Lupária, Milano 2012.

(18) Cfr. ACLU, *Coalition letter on Cloud Act*, in *www.aclu.org*.

(19) S. Warren, L. Brandeis, *The Right to Privacy*, in *Harvard Law Review* 1890, 193 ss.

«diritto alla sfera privata che non deve essere toccata dall'Autorità pubblica» (*right to be let alone*). Tale prospettiva è stata sviluppata in tutto il Novecento da filosofi e sociologi come Foucault, il quale – volendo qui terribilmente semplificare il ben più complesso approccio del pensatore francese – ha ripreso la celebre immagine del *Panopticon* benthamiano proprio per raffigurare l'idea del controllo della società moderna sugli individui (20).

In seguito, però, l'avvento delle nuove tecnologie ha portato a comprendere come esista una dimensione della sfera soggettiva dell'io che non soltanto merita protezione dalle incursioni dell'autorità, ma che genera al contempo un diritto fondamentale al controllo, da parte della stessa persona, dei dati che la riguardano. In sostanza, con il passare del tempo, la *privacy* ha smesso di essere mero «*right to be let alone*», ma ha assunto una parallela «dimensione esterna», legata al controllo delle proprie informazioni.

Tale dimensione della riservatezza non è peraltro esplicitata nella nostra Carta costituzionale – come già accennato *supra* –, né nell'art. 8 della CEDU, che cristallizza il solo diritto al rispetto della vita privata e familiare (anche se la Corte europea ha espresso una giurisprudenza piuttosto cospicua in materia di *data protection* (21), spesso definita «*informational privacy*») (22).

È invero il diritto eurounitario a mettere correttamente a fuoco questi due differenti volti del diritto in esame. Sul punto viene infatti in rilievo non solo il dettato dell'art. 16 TFUE (ove si cristallizza il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano (23)), ma principalmente la Carta dei diritti fondamentali dell'Unione europea, la quale proclama simultaneamente, con uno limpido *pendent*, il

---

(20) Cfr., tra gli altri, M. Foucault, *Sorvegliare e punire. Nascita della prigione*, Torino 1975, 218 ss. Per un recente affresco del pensiero dell'autore nel prisma della giustizia penale: Aa. Vv., *Confessione, liturgie della verità e macchine sanzionatorie. Scritti raccolti in occasione del Seminario di studio sulle «Lezioni di Lovanio» di Michel Foucault*, a cura di L. Lupária, L. Marafioti, Torino 2015.

(21) Per un quadro aggiornato: Council of Europe, *Guide on Article 8 of the European Convention on Human Rights*, 31 dicembre 2018, 34 ss.; K. De Vries, *Right to Respect for Private and Family Life*, in *Theory and Practice of the European Convention on Human Rights*, a cura di P. Van Dijk, F. Van Hoof, A. V. Rijn, L. Zwaak, 5ª ed., Cambridge – Antwerp – Portland 2018, 672 ss.

(22) A testimonianza di come la Convenzione sia uno strumento flessibile, in grado di adattarsi al mutare dei tempi, grazie al giudice deputato ad applicarla concretamente.

(23) Per uno studio analitico di tale disposizione: H. Hijmans, *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Cham 2016.

diritto al rispetto della vita privata e della vita familiare (art. 7) e il diritto alla «protezione dei dati di carattere personale» (art. 8) [24].

Ebbene, nell'ottica di chi scrive, questa «gemmazione» di diritti, cristallizzata nella CDFUE – frutto, inevitabilmente, anche del fatto che la Carta di Nizza trova le sue radici in un contesto culturale e sociale profondamente mutato rispetto a quello in cui era nata la CEDU – risulta particolarmente feconda. La Carta rende, infatti, immediatamente percepibile il fatto che i singoli non sono più titolari soltanto della «classica» libertà negativa di non subire interferenze nella propria sfera personale (il cuore del vecchio diritto alla *privacy*), ma anche di una libertà positiva di esercitare un controllo effettivo sul flusso dei propri dati personali, ovvero su quelle informazioni, che identificano o rendono identificabile, direttamente o in modo indiretto, una persona fisica e che possono fornire notizie sulle sue caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute, situazione economica, etc.

In definitiva, dunque, con la codificazione dell'art. 8 della CDFUE si è raggiunta «la sublimazione dell'approdo del diritto alla *privacy* da una dimensione eminentemente negativa (…) a una di carattere positivo, che si traduce nella tutela dei dati personali mediante la predisposizione di un corpo di regole e principi» [25].

Come detto, alcune pronunce dalla Corte EDU in questa materia sono antecedenti rispetto all'elaborazione dell'art. 8 CDFUE e sono andate poi a influenzare la giurisprudenza della Corte di giustizia, quando la stessa ancora non poteva fondare le proprie decisioni su un parametro autonomo. Al contrario, va segnalato che il *case law* della CEDU, pur facendo frequenti richiami [26] alle previsioni della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale [27], «*shows little evidence of being influenced by EU data protection law*» [28].

---

[24] Sull'emergere della *data protection* come diritto fondamentale in Europa, v., per tutti, G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham 2014.

[25] Così, efficacemente, M. Bassini, O. Pollicino, *Commento all'art. 8 della Carta*, cit., 136. Per una compiuta analisi del rapporto tra la nozione «classica» di *privacy* e il diritto alla «*data protection*», cfr. M. Tzanou, *Data protection as a fundamental right next to privacy? «Reconstructing» a not so new right*, in *International Data Privacy Law* 2013, 88 ss.

[26] V., ad esempio, C. dir. uomo, Grande Camera, 16 febbraio 2000, *Amann* c. *Svizzera*, § 65.

[27] Ci si riferisce alla Convenzione sulla protezione della persona rispetto al trattamento automatizzato di dati a carattere personale, CETS No. 108 del 28 gennaio 1981.

[28] Così, K. De Vries, *Right to Respect for Private and Family Life*, cit., 673.

È appena il caso di aggiungere che il consolidamento nella Carta di Nizza del diritto alla tutela dei dati personali dischiude «prospettive più ampie rispetto a quelle racchiuse nella felice formula della *Informationelle Selbstbestimmung*», creata dal *Bundesverfassungsgericht*, già negli anni Ottanta, quale «diritto all'autodeterminazione informativa». Come si è condivisibilmente affermato, il patrimonio di cui all'art. 8 guarda, infatti, oltre al «concetto di consenso e mira alla [c]reazione di un sistema di pesi e contrappesi, uno statuto dei dati personali che ne permetta il trattamento in forma lecita prescindendo, talvolta, dal consenso da parte dell'interessato» (29).

Non va peraltro tralasciato che sull'altra sponda dell'Atlantico vi è chi attribuisce al diritto alla *privacy* molte altre sfaccettature eterogenee. A tale riguardo basti pensare come un recente articolo, pubblicato dalla rivista *University of Pennsylvania Journal of International Law* (30), classifichi ben otto tipi di privacy (*bodily, intellectual, spatial, decisional, communicational, associational, proprietary* e *behavioral*), a cui ne andrebbe aggiunto un nono, ossia l'«*informational privacy*» «*that overlaps, but does not coincide, with the eight basic types*» (31) (una sorta di diritto trasversale, non derivato da altri). La possibilità di individuare così tante fisionomie del macrodiritto alla *privacy* offre un'ulteriore riprova della profonda complessità e attualità del tema in esame, tanto che viene da chiedersi quanti articoli verrebbero ad esso dedicati in una futura nuova Carta europea (o universale) dei diritti dell'uomo.

3. – Alla luce di questo contesto, tratteggiato in maniera sintetica, può allora non risultare operazione inutile ipotizzare alcune ripartizioni atte a mostrare come il processo penale si possa «atteggiare» nei confronti dei dati personali, così da esplorare future soluzioni ermeneutiche per allineare il nostro rito criminale alle nuove esigenze che lo sviluppo del diritto alla *privacy* determina.

In primis, il processo è, banalmente, un recettore di dati (32): questi ultimi arrivano dal circuito esterno alla dimensione giudiziale e fanno

---

(29) Le citazioni riportate sono sempre di M. Bassini, O. Pollicino, *Commento all'art. 8 della Carta*, cit., 136.

(30) Ci si riferisce a B.-J. Koops, B.C. Newell, T. Timan, I. Škorvánek, T. Chokrevski, M. Galiè, *A Typology of Privacy*, in *University of Pennsylvania Journal of International Law* 2017, 483 ss.

(31) B.-J. Koops, B.C. Newell, T. Timan, I. Škorvánek, T. Chokrevski, M. Galiè, *A Typology of Privacy*, cit., 486.

(32) V., al riguardo, R. Orlandi, *Il processo nell'era di internet*, in *Dir. pen. proc.* 1998,

ingresso al suo interno. Si pensi alle generalità del prevenuto o della vittima, le quali costituiscono informazioni attorno a cui ruota l'intera meccanica della verifica dell'ipotesi d'accusa.

Il processo costituisce poi, inevitabilmente, una macchina volta a cercare dati: vengono qui in rilievo i vari mezzi di ricerca della prova, anche digitale. Come si è correttamente osservato, se vista da una certa prospettiva, l'inchiesta penale (o il relativo giudizio) può essere qualificata «come una continua violazione [legalizzata] del diritto alla riservatezza»: «l'evento criminoso, da cui sorge l'obbligo di accertamento delle responsabilità, fa scivolare in secondo piano l'esigenza soggettiva di impedire intrusioni della vita privata, così come quella di non veder compromessi l'immagine e l'onorabilità, o fraintesa la personalità» (33).

Il processo è, poi, un creatore di *personal data*: non si accontenta di acquisire i dati sul prevenuto, ma di questi ricostruisce e proietta un «profilo inedito» (34). Si tratta del profilo che si staglia nella cornice del processo penale, rispetto al quale il soggetto ha il diritto di interagire: «il ritratto giudiziale (…) può avere effetti negativi, anche a prescindere dall'alternativa fra assolto e condannato» (35). Del resto, il singolo ha tutto il diritto a che il dispositivo giudiziario non costruisca di lui un'indelebile immagine distorta, che aggravi ancora di più lo stigma sociale dell'essere sottoposti a un vaglio penale (secondo la classica immagine carneluttiana del processo come pena (36)). Tale prospettiva riguarda addirittura la semplice (ma delicata) disciplina dei nomi degli imputati, utilizzati per riferirsi alle sentenze, nonché l'istituto del casellario giudiziale, oggetto di una cospicua giurisprudenza da parte della Corte EDU (37).

I dati personali nel processo devono essere ottenuti e vanno trattati in modo lecito. Sul punto l'art. 160-*bis* del codice della *privacy* stabilisce che «la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento dei dati personali non

---

140, nonché S. Carnevale, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, a cura di D. Negri, Roma 2007, 3 ss.

(33) Questa e la citazione immediatamente precedente sono di S. Carnevale, *Autodeterminazione informativa*, cit., 5 ss.

(34) Così, efficacemente, S. Allegrezza, *Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione Europa*, in *Protezione dei dati personali*, a cura di D. Negri, cit., 61.

(35) Cfr. ancora, S. Allegrezza, *Giustizia penale e diritto all'autodeterminazione*, cit., 61.

(36) Vedi F. Carnelutti, *Pena e processo*, in *Riv. dir. proc.* 1953, 161 ss.

(37) Un cenno sul punto in M. Bonetti, A. Galluccio, *Profili specifici sull'art. 8*, in *Corte di Strasburgo e giustizia penale*, a cura di G. Ubertis, F. Viganò, Torino 2016, 276 ss.

conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali». La norma appena citata non può essere letta nel senso che non risulta lecito trarre la sanzione della inutilizzabilità dal mancato rispetto delle previsioni in questione (38), ma, al contrario, come un doveroso rinvio alla singola disciplina processuale e ai valori a essa retrostanti, lasciando dunque aperta la strada ad interpretazioni che si profilano di estremo interesse in punto di possibili – e inedite – regole di esclusione.

Sotto altro profilo, è ovvio che il rito criminale chiede fisiologicamente di conservare dati. Possono essere elencati due facili esempi. Il primo concerne la normativa sulla *data retention*, cristallizzata nell'art. 132 del codice della *privacy*, disposizione di «pura» procedura penale che, per motivazioni tutto sommato casuali, risulta situata al di fuori del codice (39). Il secondo può, invece, essere individuato nella banca dati del DNA (40), il cui fine istituzionale è proprio quello di immagazzinare dati genetici (41) da immettere poi nella complessa meccanica della giustizia penale (42).

In ultima analisi, il processo penale riceve, raccoglie, elabora dati e li divulga alla collettività, ponendosi così in potenziale contrasto con quella «presunzione d'innocenza» (43), quale regola di trattamento extraprocessuale, frutto di un'intensa attività pretoria della Corte europea dei diritti dell'uomo e recentemente cristallizzata all'art. 4 della Direttiva 2016/343/

---

(38) Uno studio comparato del rapporto tra violazione delle regole sulla *privacy* e regole di esclusione è costituito dalla recente monografia di D. Giannoulopoulos, *Improperly Obtained Evidence in Anglo-american and Continental Law*, Oxford – Portland 2019, 53 ss., 120 ss.

(39) Cfr. S. Signorato, *Novità in tema di* data retention*. La riformulazione dell'art. 132 codice* privacy *da parte del D.Lgs. 10 agosto 2018 n. 101*, in *Dir. pen. contemp.* 28 novembre 2018.

(40) Sul punto si consenta il rinvio a L. Marafioti, L. Lupária, *Banca dati del DNA e accertamento penale. Commento alla legge di ratifica del Trattato di Prüm, istitutiva del* database *genetico nazionale e recente modifiche al codice di procedura penale (l. 30 giugno 2009, n. 85)*, Milano 2010. Si veda, più di recente, anche C. Fanuele, *La prova del DNA*, in *Prova scientifica e processo penale*, a cura di G. Canzio, L. Lupária, Milano 2017, 615 ss.

(41) Cfr. C. Fanuele, *Conservazione di dati genetici e privacy: modelli stranieri e peculiarità italiane*, in *Dir. pen. proc.* 2011, 117.

(42) Potrebbe qui essere ricordato anche il c.d. «braccialetto elettronico» che, non a caso, può essere applicato a un prevenuto soltanto con il suo consenso. Siffatto strumento tecnologico registra, infatti, tutti i movimenti della persona, provocando un'ingerenza profonda nella vita della persona. Sul punto, si veda già M. Bonetti, *Riservatezza e processo penale*, cit., 172.

(43) Cfr. L. Lupária, *La presunción de inocencia en la Carta de los derechos fundamentales de la Unión Europea*, in *Revista Vasca de Derecho Procesal y Arbitraje* 2017, 2, 199.

UE (44), di cui non si può che auspicare una rapida attuazione anche da parte del nostro Paese (45).

4. – Proprio il riferimento alla Direttiva 2016/343/UE fornisce l'occasione per un ulteriore spunto di riflessione. L'Unione europea non si è occupata del rapporto tra *privacy* e processo penale solo nel contesto del citato *data protection package* del 2016, ma anche in numerose altre fonti di diritto derivato, tra cui il pacchetto di Direttive approvate nel corso degli ultimi anni al fine di rafforzare le prerogative di imputati (46) e vittime (47).

---

(44) Tra i molti commenti alla direttiva: N. Canestrini, *La direttiva sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali. Un'introduzione*, in *Cass. pen*. 2016, 2224; S. Cras, A. Erbežnik, *The Directive on the Presumption of Innocence and the Right to Be Present at Trial. Genesis and Description of the New EU-Measure*, in *Eucrim* 2016, 1, 25 ss.; J. Della Torre, *Il paradosso della direttiva sul rafforzamento della presunzione di innocenza e del diritto di presenziare al processo: un passo indietro rispetto alle garanzie convenzionali?*, in *Riv. it. dir. proc. pen*. 2016, 1835 ss.; C. Valentini, *La presunzione d'innocenza nella Direttiva n. 2016/343/UE:* per aspera ad astra, in *Proc. pen. giust*. 2016, 6, 193 ss.

(45) Pare utile ricordare, infatti, che la Direttiva 2016/343/UE è scaduta il 1° aprile 2018.

(46) Ci si riferisce alle sei Direttive approvate dall'Unione in attuazione della tabella di marcia del Consiglio UE per il rafforzamento dei diritti procedurali di indagati o imputati in procedimenti penali (2009/C 295/01) e del programma di Stoccolma (2010/C 115/01). Il pacchetto ricomprende, più precisamente, le Direttive: 2016/1919/UE, del 26 ottobre 2016, sull'ammissione al patrocinio a spese dello Stato per indagati e imputati nell'ambito di procedimenti penali e per le persone ricercate nell'ambito di procedimenti di esecuzione del mandato d'arresto europeo, in *G.U.U.E.*, 4 novembre 2016, L 297/1; 2016/800/UE, dell'11 maggio 2016, sulle garanzie procedurali per i minori indagati o imputati nei procedimenti penali, in *G.U.U.E.*, 21 maggio 2016, L 132/1; 2016/343/UE, sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali, in *G.U.U.E.*, 11 marzo 2016, L 65/1; 2013/48/UE, del 22 ottobre 2013, sul diritto di avvalersi di un difensore nel procedimento penale e nel procedimento di esecuzione del mandato d'arresto europeo, sul diritto di informare un terzo al momento della privazione della libertà personale e sul diritto delle persone private della libertà personale di comunicare con terzi e con le autorità consolari, in *G.U.U.E.*, 6 novembre 2013, L. 294/1; 2012/13/UE, del 22 maggio 2012, sul diritto all'informazione nei procedimenti penali, in *G.U.U.E.*, 1 giugno 2012, L 142/1; 2010/64/UE, del 20 ottobre 2010, sul diritto all'interpretazione e alla traduzione nei procedimenti penali, in *G.U.U.E.*, 26 ottobre 2010, L 280/1. In argomento cfr. J. Della Torre, *Le direttive UE sui diritti fondamentali degli accusati: pregi e difetti nel primo embrione di un sistema europeo di garanzie difensive*, in *Cass. pen*. 2018, 1396 ss.; R.E. Kostoris, *La tutela dei diritti fondamentali*, in Aa.Vv., *Manuale di procedura penale europea*, a cura di R.E. Kostoris, 3ª ed., Milano 2017, 94 ss.

(47) Il rinvio va, in questo caso, ad alcune delle Direttive adottate per implementare la tabella di marcia del Consiglio relativa al rafforzamento dei diritti e della tutela delle vittime, in particolare nei procedimenti penali (2011/C 187/01) e, più precisamente, alla Direttiva 2017/541/UE, del 15 marzo 2017, sulla lotta contro il terrorismo, in *G.U.U.E.*, 31 marzo

A tal proposito, pare utile ricordare che la garanzia in esame viene in gioco in modi piuttosto diversi in tali provvedimenti, e analizzarli compiutamente consente di avere una mappatura degli elementi che aiutano a comprendere l'attuale peso che l'Unione attribuisce al diritto alla privatezza nel processo penale.

In primo luogo, alcune delle Direttive di Stoccolma dedicano alla *privacy* uno specifico spazio nei *considerando*. Si pensi, ad esempio, sul versante della vittima, al considerando n. 33 della Direttiva 2011/36/UE (48), sulla tratta di esseri umani, laddove il legislatore dell'Unione ha precisato, da un lato, che tale atto rispetta e osserva tutta una serie di diritti cristallizzati nella CDFUE, tra cui quello alla *data protection*, e, da un altro lato, che «la presente Direttiva è volta a garantire il pieno rispetto di tali diritti e principi e deve essere attuata di conseguenza».

Per quanto concerne l'imputato, si può ricordare, invece, il considerando n. 29 della Direttiva 2016/1919/UE (49), il quale, in modo speculare, stabilisce che tale atto va applicato tenendo in particolare conto anche del diritto al rispetto della vita privata e familiare. Si tratta, all'evidenza, di disposizioni (50) che assumono una specifica importanza non solo per l'interprete, ma soprattutto per gli Stati membri: questi ultimi sono avvisati

---

2017, L 88/6; Direttiva 2012/29/UE, che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato, in *G.U.U.E.*, 14 novembre 2012, L 315/17; Direttiva 2011/93/UE, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, in *G.U.U.E.*, 17 dicembre 2011, L 335/1; Direttiva 2011/36/UE, concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime, in *G.U.U.E.*, 15 aprile 2011, L 101/1. Per un'analisi di sintesi di tali atti: L. Lupária, J. Della Torre, *Victims of crime in the area of freedom, security and justice*, in *Fundamental Rights in the EU area of freedom, security and justice*, a cura di S. Iglesias, M. González, Cambridge, in corso di pubblicazione.

(48) Sulla quale cfr. C. Villacampa Estiarte, *The European Directive on Preventing and Combating Trafficking in Human Beings and the Victim-Centric Treatment of this Criminal Phenomenon*, in *Eur. Cr. L. R.* 2012, 291.

(49) In merito a tale atto cfr. N. Canestrini, *La direttiva sull'ammissione al patrocinio a spese dello Stato per indagati e imputati nell'ambito di procedimenti di esecuzione del mandato d'arresto europeo*, in *Cass. pen.* 2017, 839 ss.; S. Cras, *The Directive on the Right to Legal Aid in Criminal and EAW Proceedings. Genesis and Description of the Sixth Instrument of the 2009 Roadmap*, in *EUCRIM* 2017, 1, 35 ss.; C. Peloso, *L'approvazione della direttiva 2016/1919 sul patrocinio a spese dello Stato: la battuta finale nel cammino verso la mappatura dei diritti procedurali fondamentali*, in *www.legislazionepenale.eu* 4 maggio 2017; M. Postiglione, *Verso un effettivo diritto al patrocinio a spese dello Stato*, in *www.eurojus.it* 20 febbraio 2017.

(50) Oltre alle previsioni citate nel testo, si vedano anche il considerando n. 47 della Direttiva 2016/343/UE, il considerando n. 35 della Direttiva 2017/541/UE e il considerando n. 50 della Direttiva 2011/93/UE.

della necessità di prendere in considerazione anche il rispetto delle garanzie in tema di *privacy* nella fase di attuazione delle norme minime UE.

In seconda battuta, va ricordato che tanto la Direttiva 2013/48/UE (51), sul diritto al difensore, quanto la 2016/800/UE (52), sulle garanzie procedurali per i minori indagati o imputati nei procedimenti penali, dettano una nutrita serie di norme volte a tutelare la riservatezza delle comunicazioni (in qualsiasi forma le stesse si svolgano) tra avvocato e soggetti accusati di un reato (53). Orbene, se è indubbiamente vero che in tali norme la *privacy* viene ad assumere la tradizionale accezione di libertà negativa, volontariamente non approfondita nel presente scritto, pare degno di nota il fatto che l'Unione europea abbia voluto cristallizzare a chiare lettere il principio di civiltà giuridica per cui il rispetto della riservatezza delle comunicazioni fra gli indagati o imputati (minorenni o meno) e il loro legale «è fondamentale per garantire l'effettivo esercizio dei diritti della difesa ed è parte essenziale del diritto a un processo equo» (54). Per converso, è assai criticabile che una norma minima analoga non sia ancora stata dettata dal legislatore eurounitario per quanto concerne le vittime di reato (55).

Le norme di maggiore interesse risultano, però, sicuramente quelle contenute negli artt. 14 della Direttiva 2016/800/UE e 21 della Direttiva 2012/29/UE (56), entrambi interamente dedicati al «*right to protection of*

---

(51) Sulla quale cfr., tra i moltissimi, C. Amalfitano, *La terza tappa della tabella di marcia per il rafforzamento dei diritti processuali di indagati o imputati in procedimenti penali: la direttiva 2013/48/UE sul diritto di accesso al difensore*, in *Leg. pen*. 2014, 21; I. Anagnostopoulos, *The Right of Access to a Lawyer in Europe: A Long Road Ahead?*, in *Eur. Cr. L. R.* 2014, 3; M. Bontempelli, *Le garanzie processuali e il diritto dell'Unione europea, fra legge e giudice*, in *Proc. pen. giust.* 2014, 3, 800; F.A. Bubula, *La direttiva 2013/48/UE sul diritto al difensore e a comunicare con terzi e autorità consolari in caso di privazione della libertà personale*, in *Dir. pen. cont*. 29 novembre 2013; S. Cras, *The Directive on the Right of Access to a Lawyer in Criminal Proceedings and in European Arrest Warrant Proceedings*, in *EUCRIM* 2014, 1, 32.

(52) Cfr. S. Civello Conigliaro, *All'origine del giusto processo minorile europeo. Una prima lettura della Direttiva 2016/800/UE sulle garanzie procedurali dei minori indagati o imputati nei procedimenti penali*, in *Dir. pen. cont*. 13 giugno 2016; S. Cras, *The Directive on Procedural Safeguards for Children who Are Suspects or Accused Persons in Criminal Proceedings. Genesis and Descriptive Comments Relating to Selected Articles*, in *EUCRIM* 2016, 2, 109.

(53) Ci si riferisce all'art. 4 e ai considerando 33 e 34 della Direttiva 2013/48/UE e all'art. 6, da leggere assieme ai considerando 33 e 34 della Direttiva 2016/800/UE.

(54) In tal senso si esprimono, significativamente, in modo analogo, i considerando n. 33 delle Direttive 2013/48/UE e 2016/800/UE.

(55) Ciò, ovviamente, si deve allo stato del tutto embrionale della disciplina sul diritto a un difensore della vittima nelle fonti eurounitarie.

(56) Per un quadro di sintesi cfr., *ex plurimis*, S. Allegrezza, *Victim's Statute within*

privacy». Si tratta di previsioni con cui il legislatore dell'Unione ha voluto dettare uno *standard* di tutela particolarmente elevato del diritto alla riservatezza dei minori indagati o imputati e delle vittime di reato. È chiaro che questo *surplus* di garanzie è stato cristallizzato perché tali soggetti sono stati considerati «vulnerabili» (57) e, dunque, meritevoli di una particolare protezione, anche in punto di riservatezza. Merita peraltro ricordare che tali previsioni non rafforzano la *privacy* solo in ambito endoprocessuale, stabilendo, ad esempio, che le udienze nei confronti degli imputati minorenni vanno (di norma) svolte a porte chiuse (58), oppure, che «proteggere la vita privata della vittima può essere un mezzo importante per evitare la vittimizzazione secondaria o ripetuta» (59), ma anche dal punto di vista extraprocessuale. In entrambe le norme il legislatore europeo ha, infatti, condivisibilmente incoraggiato i media ad adottare misure di autoregolamentazione finalizzate a meglio salvaguardare la vita privata, l'integrità e i dati personali di tali categorie di soggetti (60), cercando così di fornire una

---

Directive 2012/29/EU, in *Victims and Criminal Justice. European standards and national good practices*, a cura di L. Lupária, Milano 2015, 3; P. Beauvais, *Nouvelle directive sur les droits de la victime*, in *Rev. trim. dir. eur.* 2013, 807; S. Bock, *Das europäische Opferrechtspaket: zwischen substantiellem Fortschritt und blindem Aktionismus*, in *ZIS* 2013, 203; A. Klip, *European Criminal Law. An Integrative Approach*, Cambridge 2016, 323-334; M.Á. Pérez Marín, *La regulaciòn de los derechos de las vìctimas: naturaleza y contenido*, in *Cooperación judicial penal en la Unión Europea*, a cura di I. González Cano, Valencia 2015, 381-395; F.F. Morillo, I. Bellander Todino, *The victims'rights directive: origins and expectations*, in *Vittime di reato e sistema penale. La ricerca di nuovi equilibri*, a cura di M. Bargis, H. Belluta, Torino 2017, 3; R. Müller-Piepenkötter, *Die EU-Opferschutz-Richtlinie 2012/29/EU: Handlungsbedarf bei Unterstützungsdiensten in Deutschland*, in *NK* 2016, 9-14; E. Vergès, *Un* corpus iuris *des droits des victimes: le droit européen entre synthèse et innovations*, in *RSC* 2013, 121.

(57) Non va dimenticato che anche la Raccomandazione della Commissione europea, del 27 novembre 2013, sulle garanzie procedurali per le persone vulnerabili indagate o imputate in procedimenti penali (2013/C 378/02), dedica una specifica previsione alla protezione della *privacy* di tutti i prevenuti vulnerabili (minorenni e non). Il § 15 di quest'atto stabilisce, infatti, che «le autorità competenti dovrebbero prendere opportune misure per proteggere la vita privata, l'integrità fisica e i dati personali compresi quelli medici, delle persone vulnerabili nel corso del procedimento penale».

(58) In tal senso cfr. art. 14, par. 2, della Direttiva 2016/800/UE.

(59) Così si esprime, testualmente, il considerando n. 54 della Direttiva 2012/29/UE.

(60) A tal proposito, pare utile ricordare che, anche nel corso dei lavori preparatori della Direttiva sulla presunzione d'innocenza, il Parlamento europeo aveva proposto di introdurre un emendamento che avrebbe portato gli Stati membri a promuovere l'adozione di codici deontologici, al fine di meglio tutelare la divulgazione da parte della stampa delle notizie (e quindi dei dati) connesse a procedimenti penali. Una norma di tal tipo non è stata però approvata, di modo che gli imputati maggiorenni ricevono una tutela meno avanzata del loro diritto alla *privacy* rispetto ai minorenni.

tutela a tutto tondo della garanzia in esame che, per l'appunto, fuoriesce dal ristretto ambito del rito penale.

5. – Il frastagliato quadro così descritto è stato di recente ancor più arricchito dal Regolamento (UE) 2017/1939, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea (cd. EPPO) (61).

Com'è noto, il Consiglio, in modo analogo a quanto già avvenuto in passato con riguardo ad altri organi dell'Unione creati nel quadro della cooperazione giudiziaria in materia penale (62), anche in questa occasione ha preferito adottare per l'EPPO un regime autosufficiente e *ad hoc* di norme in materia di protezione dei dati personali (63), non accontentandosi di effettuare un mero rinvio alle disposizioni generali in materia previste dal diritto dell'Unione (64).

Si tratta di un approccio – giova precisarlo – del tutto coerente con quanto già affermato nella Dichiarazione n. 21, allegata al Trattato di Lisbona, laddove si stabiliva che si sarebbe potuto rivelare necessario adottare norme specifiche relative alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia.

Senza dilungarsi sul punto in questa sede (65), è importante comunque ricordare che le norme sulla *data protection* costituiscono il più cospicuo

---

(61) In *G.U.U.E.*, 31 ottobre 2017, L 283/1. Per un commento organico cfr. i numeri speciali della rivista EUCRIM n. 2 del 2018 (intitolato *Focus*: *The European Public Prosecutor's Office – From the Drawing Board to Implementation*) e n. 3 del 2017 (intitolato *Focus: The European Public Prosecutor's Office*), nonché la curatela di L. Bachmaier Winter, *The European Public Prosecutor's Office. The Challenges Ahead*, Cham 2018. In lingua italiana, si vedano S. Ruggeri, *Indagini e azione penale nei procedimenti di competenza della nuova procura europea*, in *Proc. pen. giust*. 2018, 602; L. Salazar, Habemus EPPO*! La lunga marcia della Procura europea*, in *Arch. pen.* 2017, 3.

(62) Ci si riferisce, ad esempio, a Eurojust e a Frontex.

(63) In argomento cfr., in particolare, il recente saggio di P. De Hert, V. Papakonstantinou, *Data Protection and the EPPO*, in *NJECL* 2019, 34 ss.

(64) È bene comunque precisare che il considerando n. 93 del Regolamento ha cura di coordinare tale ordito speciale di disposizioni sulla *privacy* con quanto stabilito dalla Direttiva 2016/680/UE, stabilendo che le norme del regolamento sulla protezione dei dati personali devono essere interpretate e applicate conformemente a tale atto di diritto derivato.

(65) Pare utile ricordare che il regime di protezione dei dati al fine approvato dal Consiglio non ha convinto pienamente la Commissione europea, la quale, tramite una dichiarazione *ad hoc* (cfr. Doc. Consiglio UE, 10081/17), si è riservata di valutare l'opportunità di presentare nei prossimi anni una proposta normativa per novellare o abrogare le disposizioni in questione del regolamento. Non è, quindi, detto che il legislatore eurounitario non ritorni in futuro sui propri passi, facendo tesoro delle accese critiche che una parte

gruppo di articoli dell'intero regolamento sull'EPPO: alla tematica *de qua* viene dedicato il capo VIII, formato da più di quaranta articoli (artt. 47-89), a cui vanno aggiunte altre disposizioni sparse nel corpo dell'atto (tra cui ben 17 definizioni generali, contenute nell'art. 2) e un folto gruppo di considerando.

Orbene, già questo dato puramente quantitativo fornisce una precisa riprova di quanto sopra asserito: la *privacy* – tanto nella sua accezione negativa di *right to be let alone*, quanto (e in misura maggiore) in quella positiva di diritto del singolo al controllo sui propri dati personali – rappresenta ormai una garanzia talmente pivotale anche nel contesto del processo penale, da far sì che quando l'UE si è trovata a creare un proprio pubblico ministero ha (paradossalmente) dedicato molte più disposizioni a tale diritto, rispetto a quante ne ha dettate per disciplinare i compiti strettamente istituzionali e processuali dell'EPPO.

Per non parlare poi dell'impressionante sproporzione tra il capo dedicato alle garanzie procedurali di cui sono titolari i soggetti che si trovano a subire un'indagine da parte del Procuratore europeo, formato da solo due articoli (66), e, per l'appunto, quello sulla *data protection*. Questa differenza così marcata si deve al fatto che, con riguardo ai diritti processuali fondamentali dei prevenuti, l'Unione ha tenuto un approccio del tutto opposto a quello adottato in materia di *privacy*: il Consiglio, infatti, non ha considerato opportuno dettare una serie di norme *ad hoc*, tarate sulle peculiarità dell'EPPO, ma si è per lo più limitato a compiere generici rinvii alle previsioni generali contenute nelle Direttive di Stoccolma (67).

Orbene, l'auspicio non può che essere quello che nel prossimo futuro vi sia, sul punto, un secco *revirement* da parte delle istituzioni UE: se è pur vero che la *privacy*, in quanto principio basilare assicurato dalla Carta di Nizza e nella CEDU, merita una tutela particolarmente avanzata, lo stesso non può che valere anche per tutta un'altra pletora di diritti fondamentali degli accusati di un reato, che finora ricevono una tutela del tutto minimale nell'ambito del regolamento *de quo* (68) (una circostanza che sembra

---

della dottrina sta già iniziando a sollevare nei confronti delle assai complesse regole in vigore.

(66) Ci si riferisce al Capo VI del Regolamento, composto dai soli artt. 41 e 42.

(67) Cfr. articolo 41 del Regolamento sull'EPPO.

(68) Anche secondo P. Gorkič, *Strengthening Procedural Safeguards: Three Recapitulations*, in *European criminal procedure law in service of the protection of European Union financial interests: state of play ad challenges*, a cura di Z. Đurdević, K. Ivičević, Zagabria 2015, 91, dalla creazione della figura del Procuratore europeo si desume la necessità di dettare un *corpus* ben più ampio di garanzie processuali di cui possono avvalersi i prevenuti.

inserirsi nel solco di quella «recessione» o declino di alcune guarentigie di cui si parlava *supra*).

6. – Sempre al fine di stimolare una maggiore intensità di riflessioni dottrinali sulle relazioni (pericolose?) tra rito penale, *privacy* e protezione dei dati, si vuole proporre qui un minimo spunto su una tematica che potrebbe forse risultare centrale nell'evoluzione della procedura penale «contemporanea». La nuova sensibilità intorno al diritto della persona a governare i dati che intimamente la riguardano, costituenti una proiezione esterna della sua identità, della sua personalità e del suo «sapere» – tutti elementi idealmente soggetti alla autodeterminazione del singolo – potrebbe infatti chiamare l'interprete a rileggere con occhi diversi talune tradizionali garanzie processuali o privilegi difensivi, classicamente accordati all'indagato come protezione nei confronti dell'Autorità statale.

Un esempio consentirà di apprezzare tale non facile argomento. Nella prospettiva del diritto a non prestare collaborazione agli organi inquirenti nel quadro di un accertamento penale, la visione tralatizia della garanzia collega il diritto alla autodeterminazione dell'accusato ai suoi movimenti fisici e, in massima parte, alla sua parola, contro la cui coercizione si stagliano i baluardi del *nemo tenetur se detegere* e del *right to silence*. Oggi, però, viene in rilievo una situazione per certi versi inedita: senza richiedere il «consenso» del prevenuto, durante il processo penale l'autorità può essere in grado di «apprendere» dati (peraltro capaci, in ipotesi, di valere quali ammissioni di responsabilità) che sono parte della sfera individuale del singolo e la cui acquisizione si potrebbe sostenere dover essere subordinata all'esercizio della libertà morale della persona.

Del resto, volendo fare un parallelismo non irrilevante per la presente trattazione, se ormai si opera un diretto riferimento al concetto di «*habeas data*, ossia di una protezione integrale della persona nella dimensione elettronica che adempie la stessa funzione di garanzia delle libertà che ha storicamente svolto l'*habeas corpus*: l'impegno a rispettare il corpo e la libertà» ([69]), non possiamo oggi non interrogarci sui riflessi connessi alle garanzie processuali di una nuova concezione «integrale» della persona, alla cui proiezione nel mondo corrisponde il diritto al pieno rispetto di un corpo che, ormai, è al contempo «fisico» ed «elettronico».

([69]) In questo senso S. Rodotà, *Comunicato Stampa del Garante per la protezione dei dati personali*, in *www.privacy.it*, 16 settembre 2004.

Se dunque è la *data protection* ad adempiere «alla funzione di assicurare quell'*habeas data* che i tempi mutati esigono, diventando così, com'è avvenuto con l'*habeas corpus*, un elemento inscindibile dalla civiltà» (70), potrebbero intravedersi strette connessioni tra dati personali, informazioni, proiezioni del sé che si situano fuori dalla dimensione tradizionale del corpo (e della mente) dell'accusato e le «parole» che i sistemi processuali normalmente proteggono da forme lesive del diritto ad una «offerta volontaria» agli organi inquirenti.

Il diritto a fornire solo consapevolmente le informazioni racchiuse nel proprio «io», insomma, potrebbe dover essere rimodulato in rapporto ad un «io» che possiede una dimensione diversa e più estesa nell'attuale stagione tecnologica (71). Tradizionalmente si afferma che il diritto al silenzio si basa sul rifiuto di fondare l'accertamento sulla estrazione delle prove dall'imputato stesso (72), prescegliendo invece la via di una prova di responsabilità costruita fuori e intorno a lui (73). Ebbene, questa «sfera» intangibile di autodeterminazione del singolo, che l'Autorità deve «religiosamente» rispettare, va forse ritracciata sul terreno del processo e ripensata nella sua liturgia, certamente senza eccessi pseudo-garantisti ma allo stesso tempo senza ignorare i nuovi scenari testé delineati (74).

Questa prospettiva è stata intuita, seppur embrionalmente, già più di vent'anni fa, anche da Claus Roxin. Il grande Maestro, alla fine degli anni Novanta, aveva toccato incidentalmente, in un suo scritto minore, il rapporto tra privilegio contro l'autoincriminazione e diritto alla *privacy* (75). Non si può allora che condividere il richiamo compiuto alla conclusione del saggio dallo studioso, il quale invitava la comunità scientifica dei vari

---

(70) Così, testualmente, ancora S. Rodotà, *Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, in *www.privacy.it* 16 settembre 2004.

(71) Cfr. A. Monti, R. Wacks, *Protecting personal information. The right to privacy reconsidered*, Oxford 2019.

(72) V, per tutti, L. Marafioti, *Scelte autodifensive dell'indagato e alternative al silenzio*, Torino 2000; P. Marchetti, Testis contra se. *L'imputato come fonte di prova nel processo penale dell'età moderna*, Milano 1994, nonché L. Lupária, *La confessione dell'imputato nel sistema processuale penale*, Milano 2006.

(73) Cfr. B. Petrocelli, *Ritorno alla tortura* (1950), in *Saggi di diritto penale*, Padova 1952, 624.

(74) Spunti interessanti in S. Easton, *Silence and Confessions. The Suspect as the Source of Evidence*, New York 2014, *passim*; R.S. Gerstein, *Privacy and Self-Incrimination*, in *Ethics* 1970, 87 ss.; S. Lamberigts, *The Privilege Against Self-Incrimination*, in *New Journal of European Criminal Law* 2016, 42; R. McKay, *Self-incrimination and the new privacy*, in *The Supreme Court Review* 1967, 193.

(75) C. Roxin, *Involuntary Self-Incrimination and the Right to Privacy in Criminal Proceedings*, in *Israel Law Review* 1997, 74 ss.

Paesi a effettuare «*a critical comparison of the solutions developed in the various legal systems to cover the problems that exist in this field*» (76).

7. – Al termine delle presenti osservazioni – a dire il vero più vicine a suggestioni volte a gettare luce su inedite direttrici della nostra giustizia penale e quindi degne di maggior approfondimento – appare di qualche interesse soffermarsi specificamente su alcune norme del già richiamato GDPR e del d.lgs. 10 agosto 2018, n. 101 (77) di adeguamento alla normativa nazionale, nonché della Direttiva 2016/680/UE, implementata con il d.lgs. 18 maggio 2018, n. 51 (78), ovvero sul cuore dell'impianto legislativo ideato dall'Unione europea in materia di *data protection* e giustizia criminale. Si tratta di norme che possono far ben comprendere quanti risvolti ancora inesplorati risiedano nei rapporti tra *privacy* e rito penale.

La prima disposizione da richiamarsi – anche per i suoi forti profili di criticità – è l'art. 14 del d.lgs. n. 51 del 2018, dedicato alle limitazioni dell'esercizio dei diritti dell'interessato nell'ambito dell'attività giudiziaria. Tale precetto, benché sia apparentemente finalizzato a cristallizzare (al comma 1°) il diritto di chiedere, durante il procedimento penale o anche dopo la sua definizione (con le modalità di cui all'art. 116 c.p.p.), la rettifica, la cancellazione o la limitazione di dati personali, stabilisce (al comma 2°) le modalità attraverso cui è possibile ritardare o limitare o escludere i diritti stabiliti negli articoli immediatamente precedenti (79).

Si afferma che suddette garanzie possono essere ritardate, limitate o escluse «nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di: *a)* non compromettere il buon esito dell'attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, nonché l'applicazione delle misure di prevenzione personali e patrimoniali e delle misure di sicurezza; *b)* tutelare la sicurezza pubblica; *c)* tutelare la sicurezza nazionale; *d)* tutelare i diritti e le libertà altrui».

---

(76) Così appunto C. Roxin, *Involuntary Self-Incrimination*, cit., 93.

(77) Per un commento cfr. V. Cuffaro, *Quel che resta di un codice: il d.lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della* privacy *al regolamento sulla protezione dei dati*, in *Corriere giur*. 2018, 1181 ss.

(78) Sul punto cfr. C. Pansini, *Novità legislative interne*, in *Proc. pen. giust*. 2018, 690 ss.

(79) Ad esempio il diritto di accesso ai dati personali; di rettifica o cancellazione degli stessi; o di ricevere determinate informazioni.

Orbene, se è vero che con siffatta disposizione si è attuato – seppur con un maldestro copia e incolla – l'art. 15 della Direttiva 2016/680/UE, non si può che criticare il fatto che il legislatore italiano, così come quello europeo, abbiano cristallizzato ipotesi di possibile restrizione radicale dei diritti alla *data protection* eccessivamente ampie. È, del resto, difficile non notare come i motivi che possono giustificare persino l'esclusione totale di garanzie-chiave come il diritto di accesso appaiano talmente generici da lasciare un'enorme discrezionalità alla singola autorità, il che pare – se non altro – creare un dubbio di conformità di siffatta previsione con il combinato disposto di cui agli artt. 8 e 52, par. 3 CDFUE. A questo proposito, va ricordato che secondo la Corte di giustizia «la tutela del diritto fondamentale al rispetto della vita privata a livello dell'Unione esige che le deroghe e le restrizioni alla tutela dei dati personali intervengano entro i limiti dello stretto necessario» ([80]); test che difficilmente può dirsi rispettato ove l'Autorità possa persino escludere *in toto* tutta una serie di diritti, anche solo per perseguire il fine generico di «tutelare la sicurezza pubblica».

La seconda norma rappresenta, invece, un fondamentale baluardo contro la progressiva erosione del valore dell'individualità. Il riferimento è all'art. 22 del GDPR ([81]) (e, analogamente, all'art.11 della Direttiva 2016/680/UE attuata dall'art. 8 del d.lgs. 18 maggio 2018, n. 51). Tali disposizioni cristallizzano – pur con alcune non trascurabili differenze – un divieto, passibile di alcune eccezioni, di disporre che decisioni basate unicamente su un trattamento automatizzato producano effetti giuridici negativi o incidano in modo significativo sull'interessato. Analogo tenore si ritrova, peraltro, nell'articolo 56 del citato Regolamento (UE) 2017/1939, laddove si chiarisce che «l'interessato ha il diritto di non essere sottoposto a una decisione dell'EPPO basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

Si tratta in tutti i casi di norme che, pur avendo una formulazione alquanto ambigua ([82]), sembrano costituire un solido scudo rispetto a un

---

([80]) Si veda, in proposito, C. Giust. UE, Grande Sezione, 21 dicembre 2016, Cause riunite C-203/15 e C-698/15, Tele2 Sverige AB, § 96.

([81]) Con riguardo a tale previsione, si legga G.N. La Diega, *Against the Dehumanisation of decision-Making. Algorithmic decisions at the Crossroads of Intellectual Property*, *Data Protection, and Freedom of Information*, in *JIPITEC* 31 maggio 2018, 18-19.

([82]) Cfr. J. Sajfert, T. Quintel, *Data Protection Directive (EU) 2016/680 for police and criminal justice authorities*, in *GDPR Commentary*, a cura di M. Cole, F. Boehm, in corso di stampa, 10.

utilizzo indiscriminato in Europa di algoritmi, moduli di intelligenza artificiale e modelli di *risk assessment* (83), simili a quelli che hanno preso piede negli Stati Uniti (84) e, seppur in misura minore, anche nel Regno Unito (85). Ci si riferisce, più precisamente, a strumenti computazionali che prendono in considerazione fattori (statici o dinamici (86)) relativi al passato di un soggetto (legati non solo alla sua storia criminale, ma anche allo *status* sociale, al luogo di residenza e così via (87)), per calcolare la probabilità futura che questi commetta un reato o si dia alla fuga.

Ad oggi, il novero di meccanismi di tal tipo concretamente adoperati nei Paesi di *common law* è davvero ampio, dal momento che si appalesa ogni giorno una fitta ed eterogenea rete di *tools*, elaborati direttamente dalle pubbliche autorità ovvero implementati totalmente da aziende private.

Uno dei più importanti e più conosciuti meccanismi di *risk assessment* privati è il *software Correctional Offender Mangement Profiling for Aleternative Sanction* (COMPAS) (88), programmato dall'azienda *Northpointe* (ora Equivant), il quale viene utilizzato come ausilio per i giudici in diverse fasi del processo penale, tra cui il *sentencing* (89), e che ha sollevato accese critiche nell'opinione pubblica (90) e significativi problemi giurisprudenziali (91). Giova ricordare, in proposito, anche il PSA (*Public Safety Asses-*

---

(83) In argomento v., per tutti, la recente analisi di M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Dir. pen. cont*. 29 maggio 2019.

(84) Una cospicua bibliografia sul tema può essere rinvenuta nel recente articolo di B.L. Garrett, J. Monahan, *Judging Risk*, in *California Law Review*, in corso di pubblicazione e di A.Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, in *Duke Law Journal* 2019, 1043 ss.

(85) Cfr. *Policing by Machine*, in *www.libertyhumanrights.org.uk/policy/report-policing-machine*. V. in particolare l'articolo di M. Oswald, J. Grace, S. Urwin, G.C. Barnes, *Algorithmic risk assessment policing models: lesson from the Durham HART model and «Experimental» proportionality*, in *Information & Communications Technology Law* 2018, 223 ss.

(86) Cfr. M. Gialuz, *Quando la giustizia penale*, cit., 5.

(87) Sul punto si veda il *paper Electronic privacy information center*, *Algorithms in the Criminal Justice System*, in *https://epic.org/algorithmic-transparency/crim-justice/*.

(88) Una guida all'utilizzo di tale meccanismo viene fornita dalla stessa azienda Northpointe: *Pratictoniers Guide to COMPAS*, in *www.northpointeinc.com* 17 agosto 2012.

(89) In argomento cfr. D. Kehl, P. Guo, S. Kessler, *Algorithms in the Criminal Justice System: Assessing the Use of Risk assessments in Sentencing*, in *Belkman Klein Center for Internet & Society. Harvard Law School* 2017, 11.

(90) Ci si riferisce al noto report, pubblicato dall'organizzazione *ProPublica*, di J. Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine Bias*, in *www.propublica.org* 23 maggio 2016, dove si è sostenuto che l'utilizzo degli algoritmi nel rito penale americano andrebbe a enfatizzare le disparità di trattamento tra persone di colore e non. V. anche J. Dressel, H. Farid, *The accuracy, fairness, and limits of predicting recidivism*, in *Science Advance* 17 gennaio 2018.

(91) Basti pensare al celebre caso State v. Loomis, 881 NW 2d 749 (Wis 2016), § 53-54.

sment) creato dalla «*Laura e John Arnold Foundation*» per coadiuvare i *judges* statunitensi nel momento della decisione sull'applicazione delle misure cautelari e del *bail* (92).

In alcuni Stati – tra cui California e Kentucky – i *risk assessment tools* hanno iniziato a mostrare applicazioni particolarmente estreme: per una serie di *misdemeanours*, i *pre-trail officers* possono disporre il rilascio immediato dei prevenuti, il cui rischio di fuga e commissione di reati risulti basso o moderato sulla base dell'utilizzo di un algoritmo, senza l'applicazione del *bail* e, cosa che qui appare più rilevante, senza che sia svolta un'udienza da parte di un giudice «persona fisica».

Orbene, proprio una siffatta applicazione dei meccanismi sembrerebbe essere del tutto preclusa in Europa grazie alla protezione fornita dagli artt. 22 del GDPR e 11 della Direttiva 2016/680/UE (93), dai quali si ricava un divieto assoluto di pronunce in cui «non vi è alcun coinvolgimento umano nel processo decisionale» (94).

È appena il caso di ricordare che – come chiarito già più di un decennio fa da Stefano Rodotà – la riservatezza trova il suo fondamento ultimo nei valori dell'eguaglianza, partecipazione, libertà e soprattutto della dignità umana (95), la quale è valore non bilanciabile, in quanto «è essa stessa la bilancia sulla quale disporre i beni costituzionalmente tutelati» (96). In quest'ottica, neppure per finalità securitarie (97) e di ricerca della verità si potrebbero importare nel nostro ordinamento strumenti di

---

Per un commento alla sentenza: *Criminal Law – Sentencing Guidelines – Wisconsin Supreme Court Requires Warnings before Use of Algorithmic Risk Assessment in Sentencing – State v. Loomis*, in *Harvard Law Review* 2017, 1530 ss.

(92) Cfr. *https://www.psapretrial.org/about*.

(93) Si rinvia ancora alla condivisibile ricostruzione operata da M. Gialuz, *Quando la giustizia penale*, cit., 18.

(94) Cfr. il documento del Gruppo di lavoro articolo 29 per la protezione dei dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 2017, 20.

(95) In tale prospettiva cfr. S. Rodotà, *Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, cit. Più in generale, sul rapporto tra dignità umana e *privacy* di sicuro interesse appare il recente contributo di L. Floridi, *On Human Dignity as a Foundation for the Right to Privacy*, in *Philosophy & Technology* 2016, 307 ss.

(96) Così, autorevolmente, G. Silvestri, *L'individuazione dei diritti della persona*, cit., 11.

(97) Il binomio *privacy* e sicurezza è stato di recente analizzato da M. Orfino, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Rivista di diritto dei media* 2018, 2, 1 ss. Cfr. altresì R. Sicurella, V. Scalia, *Data mining and profiling in the area of freedom, security and justice*, in *New J. of Europ. Crim. Law* 2013, 4, 409; I.E. Vassilaki, *Crime investigation versus privacy protection. An analysis of colliding interests*, in *Europ. J. of Crime and Criminal Justice* 1994, 39.

intelligenza artificiale in grado di incidere negativamente sulla dignità dell'individuo (98), quali paiono essere i già richiamati algoritmi utilizzati nelle aule di giustizia d'oltreoceano (99).

Peraltro, alla luce delle recenti dichiarazioni di intenti manifestate in ambito governativo (100), la possibilità che le decisioni automatizzate possano in qualche modo far capolino nel processo penale italiano pare tutt'altro che peregrina. Nel fosco orizzonte di un giudicante artificiale (101), si consenta dunque di concludere con l'auspicio che il nostro Codice di rito, se non riuscirà ad essere pienamente una normativa «per galantuomini», come propugnava Francesco Carrara (102), perlomeno rimanga un Codice (non per macchine ma) «per uomini».

LUCA LUPÁRIA DONATI
Professore ordinario nell'Università degli Studi Roma Tre

(98) Per un collegamento tra dignità umana e algoritmi cfr. A. Von Unger-Sternberg, *Autonomous driving: regulatory challenges raised making and tragic choices*, in *Research Handbook on the Law of Artificial Intelligence*, a cura di W. Barfield, U. Pagallo, Cheltenham 2018, 268 ss.

(99) Tra cui proprio il COMPAS, che, secondo il già citato report dell'organizzazione *Propublica*, sarebbe «*biased against blacks*».

(100) Secondo quanto riportato da E. Dellacasa, *Casaleggio e Bonafede: Sì all'intelligenza artificiale nei processi*, in *www.corriere.it* 30 marzo 2019.

(101) Su tale prospettiva, sia consentito rinviare a uno scritto redatto ben prima dell'emergere dell'attuale contesto fattuale: L. Lupária, *Prova giudiziaria e ragionamento artificiale: alcune possibili chiavi di lettura*, in *Il concetto di prova alla luce dell'intelligenza artificiale*, a cura di J. Sallantin, J.J. Szczeciniarz, Milano 2005, VII ss.

(102) *Prolusione al corso accademico di diritto penale dell'anno 1873-1874*, *Il diritto penale e la procedura penale*, Lucca 1873, 39.