QUESTIONI APERTE

Conservazione di dati biometrici e genetici

La decisione

Protezione dei dati personali – Dati biometrici e genetici – Periodo di conservazione – Stretta necessità – Diritto alla cancellazione (Direttiva UE 2016/680, artt. 4, §1, lett. c) ed e), 5, 10, 16, §§ 2 e 3; Carta dei diritti fondamentali dell'Unione europea art. 52, §1).

Contrasta con il diritto dell'Unione una normativa nazionale che prevede la conservazione da parte delle autorità di polizia a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, di dati personali, in particolare di dati biometrici e genetici, riguardanti persone che hanno subito una condanna penale definitiva per un reato doloso perseguibile d'ufficio, fino al decesso della persona interessata, anche in caso di riabilitazione di quest'ultima, senza porre a carico del titolare del trattamento l'obbligo di esaminare periodicamente se tale conservazione sia ancora necessaria, né riconoscere a detta persona il diritto alla cancellazione di tali dati, dal momento che la loro conservazione non è più necessaria rispetto alle finalità per le quali sono stati trattati, o, eventualmente, il diritto alla limitazione del loro trattamento.

CORTE GIUST. UE, GRANDE SEZIONE, 30 GENNAIO 2024, N.G., causa C-118/22.

Data protection e accertamento penale nel panorama europeo e nazionale

Sempre più di frequente le Corti europee sono chiamate ad affrontare delicate questioni sul trattamento dei dati personali per finalità preventive e repressive dei reati. In tale scenario, i Giudici di Lussemburgo, con una recente decisione, aggiungono un importante tassello per salvaguardare il diritto all'autodeterminazione informativa, delineando i limiti temporali entro i quali la *retention* dei dati biometrici e genetici è legittima. Ciononostante, le garanzie fornite dalla disciplina europea e dal sistema italiano non sembrano ancora in grado di foggiare un robusto "scudo" per preservare efficacemente i diritti individuali da interventi sproporzionati dell'autorità giudiziaria.

Data protection and criminal proceedings in the European and national panorama

The European Courts are often called upon to address delicate questions on the processing of personal data for the prevention and repressive purposes of crimes. In this context, the European Court of Justice, with the decision in question, affirms an important principle to safeguard the right to informational self-determination, outlining the time limits to consider the storage of biometric and genetic data legitimate. Nevertheless, the guarantees provided by European regulations and the Italian system do not yet seem capable of effectively safeguarding individual rights.

1. *Trattamento dei dati personali e autodeterminazione informativa.* L'incremento esponenziale dei dati personali, favorito dall'incessante sviluppo delle tecnologie digitali, pone complesse sfide nel delineare il punto di equilibrio tra la tutela del diritto alla *privacy* e la necessità di servirsi di queste informazioni per reprimere i fenomeni criminosi.

Attingendo a *database* (pubblici o privati) abili nell'archiviare, elaborare e incrociare, in tempi rapidissimi, un'enorme mole di dati inerenti alla sfera riservata del singolo, le autorità, giudiziarie e di *law enforcement*, possono tracciare profili estremamente accurati delle persone (permettendone, tra l'altro, di svelare inclinazioni sessuali, religiose e politiche, abitudini quotidiane, frequentazioni sociali)[1]; la qual cosa intensifica il pericolo di indebite ingerenze nella vita privata, idonee a compromettere le libertà degli individui (anche estranei alla vicenda giudiziaria) e, talvolta, di intaccare persino la loro dignità[2].

Peraltro, il progressivo percorso di "datificazione" della società[3] – coniugandosi con l'imperativo di preservare la sicurezza pubblica mediante la raccolta su larga scala di dati, anche sensibili, al fine di assicurare una più efficiente repressione dei reati[4] – agevola pratiche di sorveglianza di massa sempre più evolute (*data-surveillance*[5]), che incrementano la minaccia di pervasivi controlli clandestini capaci di intromettersi anche nella sfera più intima della persona.

---

[1] Sulle tecniche di profilazione realizzate combinando le informazioni presenti nelle banche dati digitali (c.d. *inferential relational retrieval*), v. SIGNORATO, *Le indagini digitali*, Torino, 2018, 85.

[2] In tal senso, è «facile intuire quanto possa essere scossa la personalità di un individuo che si trovi ad essere in balia di chi controlla sistematicamente» le informazioni sulla sua vita privata. «È in gioco il suo essere e, con esso, la sua dignità». In questi termini, ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, 3, 1152.

[3] Si tratta della tendenza, ormai globale, a tradurre qualsiasi entità osservabile in dati digitali; tale processo «si compone di tre fattori essenziali: l'aumento esponenziale della quantità di dati prodotti nel mondo; la capacità di analisi dei dati e di estrazione di informazioni dai dati, svolta da parte di macchine a ciò addestrate; la possibilità e la capacità di prendere decisioni attraverso queste nuove informazioni, anche grazie alla cd. *alghoritmic decision making*» (CALZOLAIO, *Introduzione.* Ubi data, ibi imperium*: il diritto pubblico alla prova della localizzazione dei dati*, in *Riv. it. inf. dir.*, 2021, 1, 5). Sulla "datificazione", si veda MAYER-SCHÖNBERGER - CUKIER, *Big Data: A Revolution that will Transform How We Live, Work and Think*, Londra, 2013, 154 ss.; SARRA, *Il mondo-dato. Saggi su datificazione e diritto*, Padova, 2019, 29 ss.; COULDRY-YU, *Deconstructing datafication's brave new world*, in *New media & society*, 2018, 1 ss.

[4] In proposito, PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Milano, 2020, *passim*.

[5] Sul tema, v. RALEY, *Dataveillance and Countervailance*, in *"Raw Data" Is an Oxymoron*, a cura di Gitelman, Cambridge, 2013, 121 ss.; VAN DIJCK, *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, in *Surveillance & Society*, 2014, 12, 2, 197 ss.

Su quest'ultimo versante, affiorano poi rischi ancor più densi di ricadute negative sulle prerogative individuali[6].

Accanto alle criticità connesse al trattamento dei dati genetici e biometrici – che in ragione della loro "sensibilità" meritano una specifica analisi[7] – se ne collocano ulteriori di più ampia portata: nell'attuale epoca contraddistinta dalla "*datafication*", la realtà corporea delle persone si "dissolve" per trasformarsi in freddi codici binari da custodire nelle banche dati digitali[8]; sicché, dietro questo processo si cela la concreta insidia di far perdere di vista che in quei *bit* vi sono, non solo elementi utili per identificare i soggetti coinvolti in attività delittuose, ma anche concrete vicende umane, talora estremamente delicate nella loro drammaticità, che dovrebbero essere poste a riparo da ingerenze ingiustificate dell'autorità[9].

Considerati i valori in gioco, dunque, pur essendo il rapporto tra *privacy* e procedimento penale contraddistinto da un «fisiologico squilibrio»[10] in favore di

---

[6] Sul punto si è sottolineato che «internet e strumenti digitali hanno radicalmente mutato il modo di essere degli individui, permettendo sviluppi dell'identità umana impensabili fino a poco fa; persino le relazioni, individuali e di gruppo, hanno cambiato volto, generando archivi privati dalle proporzioni straordinarie». SCALFATI, *Un ciclo giudiziario "travolgente"*, in *Proc. pen. giust.,* 2016, 4, 114.

[7] V. *infra* § 2.

[8] A tal riguardo, si è osservato che «nell'*Information Age* anche il corpo è stato subito considerato un insieme di dati, un sistema informativo». (RODOTÀ, *Trasformazioni del corpo*, in *Pol. dir.*, 2006, 1, 3).

[9] Si pensi, ad esempio, al trattamento dei dati sanitari mediante i quali è possibile conoscere, non solo eventuali patologie di cui è affetto l'interessato, ma anche scelte esistenziali drammatiche come, a titolo esemplificativo, quella di sospendere i trattamenti di sostegno vitale. Si considerino poi le implicazioni conseguenti all'accesso ai dati genetici, i quali sono in grado di rilevare informazioni tanto sulla persona dalla quale provengono, quanto sui suoi consanguinei. Sotto quest'ultimo profilo, «la memorizzazione in banca dati del profilo d'un soggetto implica» sia «una sorta d'inserimento "virtuale" dei consanguinei, quand'anche per costoro mancassero i presupposti a cui la legge subordina la schedatura», ma anche conseguenze ulteriori atteso che «il *familial searching* potrebbe portare alla luce una parentela ignorata, o sconfessarne una supposta, con imprevedibili ripercussioni sui soggetti coinvolti». Per tali considerazioni, si veda CAMON, *La disciplina delle indagini genetiche*, in *Cass. pen.*, 2014, 4, 1427. Sul punto, altresì, FANUELE, *La prova genetica: acquisire, conservare ed utilizzare i campioni biologici*, in *Dir. pen. proc.*, 2015, 1, 106.

[10] Così TORRE, Privacy *e indagini penali*, Milano, 2020, 3, il quale evidenzia che «il fine del procedimento penale [...] giustifica la compressione del pur fondamentale diritto alla *privacy* [...]. Diversamente opinando, risulterebbe frustrata l'esigenza – di matrice costituzionale (artt. 112, 25, 27 e 111 Cost.) – di prevenzione e di repressione dei fatti costituenti reato». Sullo squilibrio tra *privacy* e procedimento penale, si veda altresì ALESCI, *Spazio giudiziario europeo*, Milano, 2020, 69; BACCARI-CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla* privacy*: uno sguardo d'insieme*, in *Dir. pen. proc.*, 2021, 6, 711; FALATO, *L'uso (preventivo e repressivo) di dati personali come compressione di un diritto inviolabile*, in *Giust. pen.*, 2016, III, 548. In generale, sul tema, v. BONETTI, *Riservatezza e processo penale*, Milano, 2003.

quest'ultimo[11], l'accesso agli archivi digitali nei quali sono raccolti migliaia di dati personali non può divenire l'espediente per ledere in maniera indiscriminata i diritti individuali, mediante l'ipertrofica ricerca di informazioni spesso irrilevanti per l'accertamento giudiziario.

Ecco allora che, nel percorso evolutivo del concetto di *privacy*[12], emerge la necessità di garantire al singolo, non solo il riserbo sull'intimità della vita privata (c.d. *right to be left alone*[13]), ma soprattutto il potere di gestire i propri dati anche quando non sono più nella sua esclusiva disponibilità (c.d. autodeterminazione informativa)[14].

In una prospettiva dinamica, il diritto a proteggere i dati personali prescinde dall'aspettativa di mantenere riservate determinate informazioni, impedendone la conoscenza da parte di terzi; l'obiettivo, piuttosto, è quello di rendere accessibili e trasparenti le procedure con le quali i dati circolano e sono impiegati, una volta che sono stati legittimamente raccolti[15].

Siffatta prerogativa, non limitandosi a preservare l'interesse a non subire indebite interferenze altrui, punta a salvaguardare il diritto del singolo a controllare i dati che lo riguardano e, quindi, di conoscere le modalità e gli scopi del loro trattamento, nonché di chiederne la rettifica o la cancellazione.

D'altronde tale esigenza di tutela, oltre ad essere implicitamente garantita sul

---

[11] Su questo versante si è osservato che l'indagine penale «si configura come una continua violazione del diritto alla riservatezza». In questi termini 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 Negri, Roma, 2007, 6.

[12] A tal riguardo si veda, CISTERNA, *Cedu e diritto alla* privacy, in *I princìpi europei del processo penale*, a cura di Gaito, Roma, 2016, 193 ss.; PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e di discontinuità*, in *Diritto alla riservatezza e protezione dei dati personali*, a cura di Pardolesi, Milano, 2003, 1 ss.

[13] WARREN - BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, 1890, 193 ss.

[14] Sul punto, BOMBARDELLI, *Dati personali (tutela dei)*, in *Enc. dir.*, Milano, 2022, I, 352; CALIFANO, Privacy*: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, 96 ss.; CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, cit., 7; CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Diritto e impresa*, 2018, 3, 1098 ss.; FINOCCHIARO, Privacy *e protezione dei dati personali*, Bologna, 2012, 3 ss.; LUPÁRIA DONATI, Privacy, *diritti della persona e processo penale*, in *Riv. dir. proc.*, 2019, 6, 1454; RICCI, *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in *Diritto e impresa*, 2017, 2, 586; TORRE, Privacy *e indagini penali*, cit., 29; VALENTINI, *Forme di privazione del diritto di difesa nello Stato senza diritto (ovvero: come un gioco di parole diventa realtà)*, in *Arch. pen. web*, 2020, 2, 17.

[15] CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, cit., 7 ss.; TORRE, Privacy *e indagini penali*, cit., 29.

piano interno (art. 2 Cost.)[16] e convenzionale (art. 8 C.E.D.U.)[17], assurge, nel contesto eurounitario, a rango di diritto fondamentale (art. 8 C.D.F.U.E.)[18], il quale non può essere sacrificato *tout court* per soddisfare le finalità preventive e repressive dei reati.

Nell'ottica delle Corti europee, del resto, la mera raccolta e conservazione di dati personali costituisce un'ingerenza nella vita privata[19], anche qualora essi non siano utilizzati dall'autorità e non sia stato, in concreto, arrecato alcun pregiudizio all'interessato[20].

Da questa angolatura, particolari cautele vanno allestite per contrastare i maggiori rischi determinati dalla schedatura massiva, in grado di produrre – attraverso sofisticate tecnologie capaci di aggregare e incrociare informazioni di per sé neutre – più intense ricadute sulla sfera salvaguardata dalle fonti sovranazionali (artt. 8 C.E.D.U., 7 e 8 C.D.F.U.E.)[21].

Per evitare arbitrarie lesioni della riservatezza, l'equo bilanciamento delle contrapposte esigenze impone di regolare i requisiti e le condizioni abilitanti la raccolta e l'utilizzo dei dati personali, assicurando che questi ultimi siano trattati in maniera congrua, pertinente e non eccessiva rispetto alle finalità per le quali sono stati archiviati[22].

Seguendo questa direttrice, anche le fonti europee mirano ad assicurare nei

---

[16] In argomento, CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, cit., 13;

[17] Per un quadro di sintesi, CISTERNA, *Cedu e diritto alla* privacy, cit., 231 ss.; DE VRIES, *Right to Respect for Private and Family Life*, in *Theory and Practice of the European Convention on Human Rights*, a cura di Van Dijk-Van Hoof-Rijn-Zwaak, Cambridge, 2018, 672 ss.

[18] Sul ruolo determinante dell'art. 8 C.D.F.U.E., nel riconoscere «la libertà positiva di esercitare un controllo effettivo sul flusso dei propri dati personali», cfr. LUPÁRIA DONATI, Privacy, *diritti della persona e processo penale*, cit., 1454; sul punto si veda, altresì, BASSINI - POLLICINO, *Commento all'art. 8 della Carta*, in *Carta dei diritti fondamentali dell'Unione europea*, a cura di Mastroianni-Pollicino-Allegrezza-Pappalardo-Razzolini, Milano, 2017, 136.

[19] Corte EDU, Grande Camera, 26 marzo 1987, *Leander c. Svezia*; Corte EDU, Grande Camera, 4 dicembre 2008, *S. & Marper c. Regno Unito*. In ambito eurounitario cfr. Corte giust. UE, 8 aprile 2014, cause riunite C-293/12 e 594/12, *Digital Rights Ireland*, nonché, più di recente, Corte giust. UE, 2 marzo 2021, C-746/18, *H.K.*, in *Proc. pen. giust.*, 2021, 5, 1195, con nota di ANDOLINA, *La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di data retention?*.

[20] Corte EDU, Grande Camera, 16 febbraio 2000, *Amann c. Svizzera*; Corte EDU, 4 maggio 2000, *Rotaru c. Romania*.

[21] Corte EDU, 18 aprile 2013, *M.K. c. Francia*, in *Dir. pen. proc.*, 2013, 7, 809, con nota di SCARCELLA, *Conservazione delle impronte digitali degli "assolti" e violazione dell'art. 8 Conv. e.d.u.*

[22] Cfr. Corte EDU, 18 aprile 2013, *M.K. c. Francia*, cit., §12; Corte EDU, Grande Camera, 4 dicembre 2008, *S. & Marper c. Regno Unito*, cit., § 99.

diversi Paesi membri una piattaforma condivisa di regole in materia di *data protection*. In tal senso, accanto alla disciplina generale, nota con l'acronimo GDPR (*General Data Protection Regulation*), sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali (Regolamento UE/2016/679)[23], sono dettate regole specifiche sul loro impiego ai «fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali» (Direttiva UE/2016/680)[24].

La Direttiva – ponendosi in rapporto di complementarità con la fonte regolamentare[25] – intende conseguire l'ambizioso obiettivo di garantire un livello di tutela omogeno dei diritti, predisponendo un sistema generale di *data protection* idoneo a prevenire abusi da parte del potere giudiziario[26].

---

[23] In proposito, BISTOLFI-BOLOGNINO-PELINO, *Il regolamento privacy europeo*, Milano, 2016; *Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, a cura di Califano-Colapietro, Napoli, 2017; CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, cit., 1098 ss.; *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da Finocchiaro, Bologna, 2017; *GDPR e normativa privacy*, a cura di Riccio-Scorza-Belisario, Milano, 2018; *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, Milano, 2019. In seguito all'approvazione del GDPR, il legislatore ha profondamente modificato la disciplina in materia di *privacy* con il d.lgs. 10 agosto 2018, n. 101; sul punto si veda *La protezione dei dati personali in Italia*, a cura di Finocchiaro, Bologna, 2019; MANES-MAZZACUVA, *GDPR e nuove disposizioni penali del Codice privacy*, in *Dir. pen. proc.*, 2019, 2, 171; *Il "nuovo" codice in materia di protezione dei dati personali*, a cura di Scagliarini, Torino, 2019.

[24] Sul tema, BORGIA, *Il trattamento di dati personali a fini di prevenzione, di indagine, di accertamento e di perseguimento di reati o di esecuzione di sanzioni penali: quali passi avanti alla luce dei recenti sviluppi?*, in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, a cura di Mantelero-Poletti, Pisa, 2016, 495 ss.; GALGANI, *Giudizio penale,* Habeas data *e garanzie fondamentali*, in *Arch. pen. web*, 8 febbraio 2019, 1, 1 ss.; TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in *La nuova disciplina europea della privacy*, a cura di Sica-D'antonio-Riccio, Milano, 2016, 314 ss.. Per la letteratura straniera sulla Direttiva UE/2016/680, si vedano, COCQ, *Eu Data Protection Rules Applying to Law Enforcement Activities. Towards an Harmonised Legal Framework?*, in *New Journal of European Criminal Law*, 2016, 7, 3, 263 ss.; DE HERT-PAPAKONSTANTINOU, *The New Police and Criminal Justice Data Protection Directive. A First Analysis*, *ivi*, 1, 7 ss. L'Italia ha attuato la Direttiva UE/2016/680 con il d.lgs. 18 maggio 2018, n. 51; sul punto, anche per i riferimenti bibliografici, si veda *infra* §§ 4-5.

[25] In questa prospettiva, si è evidenziato che i due testi normativi (Regolamento UE/2016/679 e Direttiva UE/2016/680), nel superare i *deficit* di organicità della previgente disciplina comunitaria (Direttiva 1995/46/CE e Decisione quadro 2008/977/GAI), sono «finalizzati a realizzare un corpo normativo organico in materia di protezione dei dati personali, fondato su un sistema di principi generali, applicabile a tutti i settori di competenza dell'Unione». In questi termini, RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine accertamento e perseguimento di reati. Riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, in *Nuove leggi civili*, 2019, 3, 571-572.

[26] A tal proposito, TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, cit., 331.

Il compendio normativo è così improntato a contemperare gli eterogenei interessi in campo: la protezione dei dati personali acquisisce il valore di diritto fondamentale, ma non si configura come una prerogativa assoluta; pertanto, nel bilanciamento con le contrapposte esigenze di rilievo collettivo, sono ammessi interventi limitativi, funzionali a consentire l'efficace repressione dei reati[27].

In questo scenario, la Direttiva pur attribuendo all'interessato un ampio ventaglio di diritti – tra i più significativi, quello di essere informato sul trattamento in corso (art. 13), di accedere ai dati che lo riguardano (art. 14), di ottenerne la rettifica, la limitazione e la cancellazione (art. 16) – consente agli Stati membri di restringerne la portata qualora tale compressione è necessaria per non compromettere gli scopi dell'accertamento penale[28].

Nonostante l'ambiguità delle clausole derogatorie delineate dalle previsioni eurounitarie[29] – che, essendo connotate da eccessiva elasticità, assegnano un ampio margine di discrezionalità alle scelte politiche nazionali nel soppesare gli interessi antagonisti[30] – occorre scongiurare il pericolo che esse si tramutino nel grimaldello per intaccare il nucleo essenziale della *data protection*[31].

Da questo punto di vista, eventuali restrizioni delle guarentigie riconosciute dalla Direttiva UE/2016/680 sono tollerabili, in ossequio al principio di proporzionalità (art. 52 C.D.F.U.E.), solo se gli obiettivi dell'inchiesta giudiziaria non sono raggiungibili con altre misure meno pregiudizievoli per l'interessato[32]. Bisogna, in sintesi, arrecare il "minor sacrificio possibile" ai diritti di accesso e

---

[27] Cfr. il *Considerando* n. 44 della Direttiva UE/2016/680.

[28] In tal senso, la Direttiva consente ai Paesi membri di adottare misure limitative dei diritti riconosciuti dagli artt. 14 e 16 qualora tale restrizione costituisca «una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata per: 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» (artt. 15 co. 1 e 16 co. 4).

[29] Si sofferma sul punto GALGANI, *Giudizio penale,* Habeas data *e garanzie fondamentali,* cit., 8.

[30] Su tali aspetti si tornerà *infra*, § 5.

[31] Si è in proposito efficacemente scritto che la flessibilità dei parametri delineati dalla Direttiva UE/680/2016, crea un "*bug* autodistruttivo" che consente ai Paesi membri di adottare discipline di recepimento tali «da annichilire nella loro sostanza i diritti di accesso e controllo sulla gestione dei dati trattati per finalità di polizia e di giustizia». In questi termini, VALENTINI, *Forme di privazione del diritto di difesa nello Stato senza diritto (ovvero: come un gioco di parole diventa realtà),* cit., 21.

[32] In tal senso, si veda il considerando 26 della Direttiva in questione.

controllo sulla gestione dei dati[33].
Gli ordinamenti interni, quindi, dovrebbero contingentare il potere dell'autorità di trattare le informazioni personali, cosicché esso sia adeguato e non eccedente rispetto agli obiettivi preventivi e repressivi dei reati (c.d. principio di "minimizzazione dei dati")[34], imponendo la cancellazione dei dati non pertinenti a tali scopi.

2. *I dati biometrici e genetici nel sistema europeo.* È nel tratteggiato quadro assiologico che dunque vanno esaminate le recenti decisioni, tra cui quella in commento, con le quali la Corte di Lussemburgo, nell'affrontare le spinose questioni poste dall'impiego da parte dell'autorità di dati "sensibili" per fini di giustizia, tenta di delineare l'equilibrio tra i divergenti interessi, salvaguardando i diritti del singolo dalla minaccia di una raccolta sistematica e indifferenziata di elementi conoscitivi sulla sfera più intima della persona.
Sotto questo profilo, peculiare impegno è riservato alla tutela dei dati genetici e biometrici[35].
Entrambi, sono accomunati dall'attitudine a identificare, in maniera inconfondibile, un individuo[36]: i primi, tramite la tipizzazione del profilo del DNA ricavata dall'analisi dei campioni biologici della persona, forniscono «informazioni

[33] Sui riflessi del principio di proporzionalità nel procedimento penale, BONZANO, *Gli accertamenti medici coattivi*, Milano, 2017, 114 ss.; CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont.*, 2014, 3-4, 147; CAMON, *La prova genetica tra prassi investigative e regole processuali*, in *Proc pen. giust.*, 2015, 6, 167; DANIELE, *I chiaroscuri dell'OEI e la bussola della proporzionalità*, in *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, a cura di Daniele-Kostoris, Torino, 2018, 55 ss.; FALATO, *La proporzionalità innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale*, in *Arch. pen.* web, 18 gennaio 2018, 1; KOSTORIS, *Processo penale e paradigmi europei*, Torino, 2018, 141-142; NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, 1, 3 ss.; NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, Milano, 2020, 107 ss.; TABASCO, *Principio di proporzionalità e misure cautelari*, Milano, 2017; UBERTIS, *Equità e proporzionalità* versus *legalità processuale: eterogenesi dei fini?*, in *Arch. pen.*, 2017, 2, 389 ss.; nonché, volendo, BELVINI, *Principio di proporzionalità e attività investigativa*, Napoli, 2022.
[34] Sul punto, TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, cit., 336-337.
[35] Tra le decisioni più recenti della Corte di Lussemburgo, oltre a quella in commento, si veda Corte giust. UE, sez. V, 26 gennaio 2023, C-205/21, V.S., in *Dir. inform.*, 2023, 2, 264, con nota di RUBIS, *Sistemi di autenticazione mediante l'utilizzo di dati biometrici*.
[36] In proposito, *Dizionario Legal tech*, a cura di Ziccardi-Perri, Milano, 2020, 314 ss.

univoche sulla fisiologia o sulla salute»[37] di quest'ultima[38]; i secondi, invece, sono ottenuti mediante il trattamento tecnico delle caratteristiche fisiche, fisiologiche o comportamentali di un soggetto (ad es., impronte digitali, tratti del volto, topografia della mano, iride, retina, tonalità della voce, modalità di scrittura, cadenza dell'andatura)[39] che «ne consentono o confermano l'identificazione» in modo inequivocabile[40].

In particolare, l'itinerario mediante il quale i dati biometrici vengono acquisiti e comparati si articola in due momenti essenziali: il procedimento è avviato con la c.d. fase di *enrollment*, la quale consente, attraverso una componente *hardware*, di rilevare e acquisire la caratteristica biometrica convertendola in formato digitale per conservarla in un *repository*; successivamente, interviene un *software* che, servendosi di evoluti algoritmi, permette di confrontare le informazioni ottenute con quelle già presenti nel *database* per verificarne il livello di somiglianza (c.d. *matching*)[41].

Si tratta di operazioni che incrementano l'insidia di ingerenze indebite nella vita privata.

In proposito, va considerata, da un lato, la vertiginosa produzione, talvolta non del tutto consapevole, dei dati biometrici nello svolgimento di attività quotidiane (si pensi, a titolo esemplificativo, all'uso dei sensori degli *smartphone* per

---

[37] Così la definizione di dato genetico ai sensi dell'art. 3, n. 12, Direttiva UE/2016/680.

[38] Sul tema, senza pretesa di esaustività, CAMON, *La disciplina delle indagini genetiche*, cit., 1426; CAPITTA, *Conservazione dei DNA* profiles *e tutela europea dei diritti dell'uomo*, in *Arch. pen. web*, 2013, 1, 1 ss.; CASASOLE, *La conservazione di campioni biologici e di profili del DNA nella legge italiana, alla luce del dibattito europeo*, in *Cass. pen.*, 2009, 11, 4435; FANUELE, *Dati genetici e procedimento penale*, Padova, 2009; ID. *La prova del DNA*, in *Prova scientifica e processo penale*, a cura di Canzio-Lupária, Milano, 2022, 543 ss.; FELICIONI, *Accertamenti sulla persona e processo penale*, Cedam, 2007, 42 ss.; ID., *La prova del DNA*, in *La prova scientifica*, a cura di Conti-Marandola, Milano, 2023, 119; GABRIELLI, *Il prelievo coattivo di campioni biologici nel sistema penale*, Torino, 2012; ID., *L'archiviazione dei dati genetici a fini di giustizia penale: gli interessi in gioco, le prescrizioni europee, le soluzioni adottate dal legislatore italiano*, in *Rev. bras. dir. proc. pen.*, 2019, 5, 3, 1385 ss.; MARAFIOTI, *Le banche dati del DNA. Una nuova frontiera investigativa nel Trattato di Prüm,* in *Banca dati del DNA e accertamento penale*, a cura di Marafioti-Lupária, Milano, 2010, 1 ss.

[39] Sul distinguo tra le diverse caratteristiche (fisiche, fisiologiche e comportamentali) esaminate dalla scienza biometrica, si veda, SACCHETTO, *La prova biometrica*, in *La prova scientifica*, cit., 244.

[40] Cfr. la definizione di dato biometrico fornita dall'art. 3, n. 13, dir. UE/2016/680.

[41] Per ulteriori approfondimenti sul procedimento di digitalizzazione biometrica, v. SACCHETTO, *La prova biometrica*, cit., 247-249. In particolare, l'A. evidenzia che un «sistema biometrico basico è costituito di quattro fondamentali elementi: un modello sensoriale che acquisisce il campione grezzo; la caratteristica estratta e "misurata" dallo scanner; la corrispondenza dei moduli con i quali le caratteristiche sono confrontate; infine, lo schema decisionale grazie al quale viene riconosciuta l'identità del soggetto».

il riconoscimento dell'impronta digitale o dell'immagine facciale[42]), e, dall'altro, l'estrema semplicità con le quali le autorità pubbliche possono acquisirli (ad es. è decisamente agevole, accedendo al *web* o servendosi delle telecamere di sorveglianza disseminate sul territorio, ottenere immagini ritraenti volti umani da utilizzare per scopi identificativi mediante *software* di riconoscimento facciale[43]).

In ragione delle caratteristiche che accomunano i dati biometrici e genetici, il loro impiego – soprattutto quando essi sono catalogati in *database* e sottoposti a procedure comparative automatizzate dirette a tracciare profili dettagliati delle persone[44] – esige maggiori cautele per proteggere le libertà fondamentali degli interessati[45].

Su questo fronte, la disciplina europea di settore, per non frustrare oltremisura gli scopi preventivi e repressivi dei reati, non pone – a differenza di quanto

---

[42] La capacità di registrare dati biometrici e, più in generale, di consentire l'apprensione di elementi conoscitivi utili per l'accertamento penale, è poi notevolmente incrementata dagli strumenti IoT (*Internet of Things*), i quali consentono di rilevare le caratteristiche fisiologiche o comportamentali delle persone (ad esempio un impianto domotico). Sull'argomento, NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 4; SACCHETTO, *La prova biometrica*, cit., 248, QUATTROCOLO, *Processo penale e rivoluzione digitale da ossimoro a endiadi?*, in *Riv. dir. media*, 2020, 3, 126.

[43] Sui rischi per i diritti fondamentali realizzati dalle tecnologie di riconoscimento facciale, si veda la recente decisione della Corte di Strasburgo con la quale è stata accertata la violazione dell'art. 8 C.E.D.U. (Corte EDU, sez. III, 4 luglio 2023, *Glukhin c. Russia*, in *Proc. pen. giust.*, 2, 2024, 413, con nota di BRUNO, *La condanna per manifestazione pacifica (non preavvisata e) con riconoscimento facciale viola i diritti fondamentali*. Sul tema, altresì, BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *Leg. pen. web*, 11 dicembre 2021, 1 ss. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, 3, 1057 ss.; LOPEZ, *Il riconoscimento facciale tramite* software, in *Le indagini atipiche*, a cura di Scalfati, Torino, 2019, 239 ss.; ID., *Videosorveglianza biometrica tramite riconoscimento facciale: parere negativo del Garante per la* privacy, in *Proc. pen. giust.*, 2022, 3, 798 ss.; MARANDOLA, *Il riconoscimento facciale*, in *La prova scientifica*, cit., 495 ss.; MOBILIO, *Tecnologie di riconoscimento facciale*, Napoli, 2022; SACCHETTO, Face to face*: il complesso rapporto tra* automated facial recognition technology *e processo penale*, in *Leg. pen. web*, 16 ottobre 2020, 1 ss.; SAPONARO, *Le nuove frontiere tecnologiche dell'individuazione personale*, in *Arch. pen. web*, 2022, 1, 1 ss.; TORRE, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc.*, 2021, 8, 1050 ss.; ID., *Intelligenza artificiale e indagini penali: prospettive future e garanzie di sistema. Il sistema automatico di riconoscimento immagini*, in *Cybercrime,* diretto da Cadoppi-Canestrari-Manna-Papa, Torino, 2023, 1731 ss.

[44] In proposito, cfr. SCAFFARDI, *Dati genetici e biometrici: nuove frontiere per le attività investigative*, in *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, a cura di Scaffardi, Torino, 2018, 37 ss.

[45] Cfr. EL SABI, *La tutela della* privacy *nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, in *Dir. inform.*, 2023, 4-5, 793.

previsto dall'art. 9 GDPR – un divieto generale di trattamento, sia pure derogabile in casi tassativi, ma lo consente solo quando "strettamente necessario" e, purché sia assistito da adeguate garanzie per i diritti e le libertà dell'interessato, nei soli casi in cui è autorizzato dal diritto dell'Unione o dello Stato membro (art. 10 Direttiva UE/680/2016)[46].

Entro tale cornice, gli ordinamenti interni sono tenuti a disciplinare la raccolta e la conservazione di dati sensibili, individuando con nitore i presupposti che consentono all'autorità di adoperarli per soddisfare gli obiettivi dell'inchiesta penale[47].

Nello scrutinare la *quality of the law* che legittima il trattamento, si esigono precetti normativi chiari e dettagliati idonei a orientare il potere di gestire dati biometrici e genetici altrui entro argini prestabiliti e, al contempo, a garantire ai singoli di conoscere, con sufficiente margine di certezza, i casi e i modi entro i quali sono ammesse compressioni dei propri diritti, permettendo così di censurare eventuali interferenze indebite[48].

Il requisito della "stretta necessità", nell'intento di accordare una maggiore protezione ai dati sensibili, postula inoltre una condizione rafforzata di liceità del trattamento, imponendo controlli maggiormente rigorosi sul rispetto del già ricordato principio di minimizzazione (art. 4 Direttiva UE/2016/680)[49].

Su questo terreno, l'uso di siffatte categorie di informazioni è ammesso solo

---

[46] L'art. 10, inoltre, fissa ulteriori requisiti per trattare i dati sensibili, stabilendo che essi possono essere adoperati «b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato».

[47] A tal riguardo si è evidenziato come l'art. 10 della Direttiva UE/680/2016 è desinato «ad avere un forte impatto negli ordinamenti nazionali, precludendo qualsiasi possibilità di trattare dati genetici o biometrici, in ambito criminalistico, al di fuori dei casi in ciò sia espressamente autorizzato dalla normativa con «adeguate garanzie» e nei limiti della stretta necessità». Così, TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, cit., 340.

[48] Sui criteri di chiarezza, prevedibilità e accessibilità che devono improntare la disciplina interna che autorizza il trattamento di dati personali cfr., *ex multis*, Corte giust. UE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*, cit., § 54; Corte giust. UE, 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, § 91 e, con particolare riguardo ai dati genetici biometrici e genetici, Corte giust. UE, sez. V, 26 gennaio 2023, C-205/21, V.S., cit., § 76. D'altra parte anche la Corte di Strasburgo, al fine di evitare ingerenze indebite nell'area tutelata dall'art. 8 C.E.D.U., reputa essenziale che la norma di copertura interna detti regole chiare e dettagliate per quanto riguarda le condizioni di memorizzazione, utilizzo e cancellazione dei dati personali, Corte EDU, Grande Camera, 4 dicembre 2008, *S. & Marper c. Regno Unito*, cit., § 99.

[49] In tal senso la decisione in commento § 48, richiama Corte giust. UE, sez. V, 26 gennaio 2023, C-205/21, V.S., cit., §§ 117, 122 e 125.

qualora le finalità dell'accertamento giudiziario non sono efficacemente conseguibili con altre modalità meno lesive dei diritti fondamentali delle persone interessate; ciò implica di dimostrare che l'ingerenza è giustificata dall'impossibilità di soddisfare l'obiettivo avuto di mira ricorrendo a dati diversi da quelli indicati dall'art. 10 della Direttiva UE/2016/680.
D'altra parte, l'essenza delle libertà proclamate dalle Carte sovranazionali (artt. 8 C.E.D.U., 7 e 8 C.D.F.U.E.) subirebbe un inaccettabile indebolimento se la raccolta e l'utilizzo di dati genetici e biometrici fossero consentiti dagli Stati membri senza alcun limite concreto, proporzionato alla repressione dei reati.
Da questo angolo visuale, la stretta necessità – implicando la residualità del trattamento, al quale ricorrere solo se realmente indispensabile – delinea un criterio selettivo più stringente, idoneo ad arginare la minaccia di indiscriminate incursioni nella sfera più intima del singolo.
In una prospettiva attigua, il criterio in parola dovrebbe costituire l'antidoto per evitare inaccettabili *screening di massa*, obbligando gli ordinamenti interni a restringere la platea soggettiva delle persone i cui dati sensibili possono essere raccolti e conservati.
L'accesso ai profili genetici e biometrici, del resto, è giustificabile solo in presenza di una concreta esigenza di identificare e perseguire gli autori di attività criminose.
L'archiviazione generalizzata di profili genetici e biometrici anche di persone non sospettate di aver commesso reati[50], pertanto, collide inevitabilmente con il canone della necessarietà[51]: il sacrificio delle libertà individuali è ammissibile solo al cospetto di una piattaforma indiziaria idonea a corroborare l'ipotesi accusatoria, escludendo incursioni arbitrarie – fondate su mere congetture o relative a profili estranei all'inchiesta penale – sugli aspetti più intimi della vita privata.
Corollario indefettibile delle indicate guarentigie è poi la previsione di adeguati

[50] Si tratta di un approccio che in passato è stato adottato nel Regno Unito, i cui *database* genetici erano alimentati in modo tale da prevedere l'inserimento del maggior numero di dati acquisibili, anche di persone non attinte da una decisione di condanna penale. Sul tema, cfr. SCAFFARDI, *Giustizia genetica e tutela della persona*, Padova, 2017, 76 ss.
[51] Sui pericoli per i diritti individuali generati dalla raccolta massiva e indifferenziata, soprattutto dei profili genetici, si veda, tra gli altri, FANUELE, *Dati genetici e procedimento penale*, cit., 356; ID. *La prova del DNA*, cit., 578; FELICIONI, *La prova del DNA*, cit., 119 ss.; GABRIELLI, *L'archiviazione dei dati genetici a fini di giustizia penale*, cit., 1402 ss.; E. MAZZANTINI, *Diritto penale e banca dati del DNA: finalità dell'analisi genetica e problemi aperti*, in *Sist. pen.*, 2020, 7, 113 ss.

strumenti di controllo – sui requisiti e sulle modalità di accesso ai dati – per reprimere eventuali abusi (art. 54 Direttiva UE/2016/680).
Al soggetto interessato, quindi, va riconosciuto il potere di adire l'autorità giurisdizionale affinché verifichi che il trattamento sia strettamente necessario e conforme ai parametri delineati dall'art. 10 della Direttiva UE/2016/680, disponendo, se del caso, la limitazione o la cancellazione dei dati non pertinenti[52].
Nel complesso, l'insieme delle indicate garanzie sollecita un più attento scrutinio sulle scelte degli ordinamenti interni che, per dirsi aderenti ai parametri fissati dalla fonte eurounitaria, non possono essere improntate a logiche meramente efficentiste dirette a far prevalere gli interessi repressivi, bensì esigono regole più stringenti rispetto a quelle previste per l'ordinario approvvigionamento e uso dei dati personali.

3. Limiti temporali e stretta necessità del trattamento. Nel panorama sin qui illustrato, la Corte di giustizia UE affronta il tema dei limiti temporali entro i quali la conservazione dei profili biometrici e genetici può reputarsi legittima.
Nel caso specifico, la questione riguarda la disciplina bulgara, che consente di trattenere nei registri di polizia dati, anche sensibili, relativi a una persona definitivamente condannata sino al suo decesso, benché abbia ottenuto un provvedimento di riabilitazione.
La durata del trattamento, d'altronde, costituisce un aspetto determinante per stimarne la congruità rispetto all'obiettivo che lo giustifica: l'elemento temporale trasforma in maniera significativa il livello dell'ingerenza nell'area salvaguardata dalle norme sovranazionali (artt. 8 C.E.D.U., 7 e 8 C.D.F.U.E.)[53], ampliando, talvolta in termini radicali, l'intensità del sacrificio inferto al diritto alla vita privata[54].

---

[52] In particolare, secondo i Giudici dell'UE, tra i diversi profili da scrutinare per appurare la necessarietà della raccolta dei dati sensibili, deve essere assicurata la possibilità di azionare una opportuna verifica «sul provvedimento di accusa formale che costituisce la base giuridica» del trattamento «alla luce di sufficienti elementi di prova del fatto che l'interessato è colpevole» e ciò anche qualora «la fase preliminare del procedimento penale non sia seguita da una fase giudiziaria». (cfr. Corte giust. UE, sez. V, 26 gennaio 2023, C-205/21, V.S., cit., §§ 88 e 96).
[53] In tal senso si è evidenziato come «le differenze di quantità, superate un certo livello, diventano differenze di qualità». In questi termini CAMON, *Innovazioni tecnologiche e mezzi di ricerca della prova*, in *Dai "casi freddi" ai "casi caldi". Le indagini storiche e forensi fra saperi giuridici e investigazioni scientifiche*, a cura di Andretta-Fondaroli-Gruppioni, Padova, 2014, 215.
[54] Sul tema, NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 90 ss.

Sotto questo profilo, la Direttiva UE/2016/680, pur astenendosi dal dettare rigidi limiti di tempo, decorsi i quali i dati personali andrebbero in automatico rimossi, esige che gli Stati membri fissino «adeguati termini per la cancellazione» (art. 5) imponendo di provvedervi «senza ingiustificato ritardo» (art. 16 § 2).

Tuttavia, il lessico oltremodo vago e indeterminato, adoperato dalle previsioni in esame, nell'assegnare un ampio spazio di manovra agli ordinamenti interni - oltre a mal conciliarsi con l'intento armonizzatore[55] - rischia di svuotare di contenuti concreti le prerogative individuali riconosciute dalla fonte eurounitaria.

In tale scenario, allora, è il requisito della "stretta necessità" a costituire, ancora una volta, il paracadute per assicurare effettività alla *data protection*.

Scrutinati con le lenti della proporzionalità (art. 52 C.D.F.U.E.), i termini di durata fissati dalle norme nazionali devono essere parametrati alle esigenze per le quali sono stati raccolti i dati personali e, di conseguenza, questi ultimi devono essere cancellati qualora «la loro conservazione non sia più necessaria rispetto alle finalità che hanno giustificato il trattamento»; la qual cosa impone ai legislatori interni di determinare «le specifiche situazioni in cui la tutela dei diritti fondamentali dell'interessato» esige la rimozione dei dati[56].

Seguendo questa traiettoria, è indubitabile che l'archiviazione dei profili biometrici e genetici di una persona attinta da una decisione di condanna definitiva – potendo rivelarsi indispensabile per verificare se la stessa sia coinvolta in altri reati – costituisce un obiettivo in linea con gli scopi delineati dalla Direttiva UE/2016/680; ciononostante, la conservazione di questi dati, soprattutto se si prolunga per un arco temporale considerevole, non può reputarsi sempre "necessaria".

Nel vagliare la legittimità del periodo di tempo nel quale le informazioni "sensibili" possono essere trattenute nel *database*, occorre valutare una serie di parametri – tra cui la natura e la gravità del reato per il quale è inflitta la condanna, il collegamento con altri procedimenti in corso, il profilo personale del condannato[57] – dai quali poter desumere un elevato pericolo che l'interessato possa commettere ulteriori reati.

Su questo versante, dunque, ai Paesi membri è affidato il delicato compito di

---

[55] Lo sottolinea GALGANI, *Giudizio penale,* Habeas data *e garanzie fondamentali*, cit., 9.

[56] Cfr. §§ 45 e 52 della decisione in commento.

[57] § 67 della sentenza che si annota.

operare una cernita delle fattispecie delittuose che, in ragione delle loro specifiche caratteristiche, sono sintomatiche di un maggior rischio di recidiva; di conseguenza, riferimenti a categorie criminose eccessivamente ampie, capaci di includere tipologie eterogenee di reati, non sono idonei, essendo scarsamente selettivi, a giustificare la conservazione dei dati per un ampio periodo di tempo[58].

Tuttavia, a prescindere dalla gravità in astratto del reato, il trattenimento nei *database* dei profili genetici e biometrici della persona condannata non è mai consentito sino al suo decesso.

In effetti, una lettura poco attenta delle previsioni europee potrebbe far considerare il momento in cui si verifica la morte dell'interessato un "termine adeguato", ai sensi dell'art. 5 della Direttiva UE/2016/680, sia pure in «circostanze particolari che lo giustifichino debitamente»[59].

Se così fosse, sarebbe piuttosto agevole per i legislatori interni dimostrare che, con riferimento a determinate fattispecie criminose connotate da un elevato tasso di offensività, sussistono straordinarie ragioni per legittimare la conservazione dei *personal data* sino al decesso dell'interessato; ciò, in particolare, al cospetto di fenomeni delittuosi allarmanti (criminalità organizzata e terrorismo), rispetto ai quali fin troppo spesso le garanzie vengono sacrificate sull'altare dell'accertamento processuale.

Una conclusione del genere, nondimeno, contrasterebbe inevitabilmente con la logica, sottesa al criterio della stretta necessità, del "minor sacrificio" per i diritti individuali: un'ingerenza talmente intensa da protrarsi per tutta la vita della persona a cui appartengono i dati sensibili, non potrebbe mai dirsi proporzionata rispetto alle finalità repressive dei reati, qualunque ne sia la gravità.

Pertanto, sebbene non affermato esplicitamente dalla Corte di giustizia UE, il margine di discrezionalità riconosciuto agli ordinamenti interni riguarda soltanto la facoltà di graduare i periodi di conservazione dei dati in base alla diversa offensività dei reati, ma non potrebbe mai essere eluso l'obbligo di fissare un termine massimo decorso il quale i dati vanno cancellati.

---

[58] Sotto questo profilo, la Corte di giustizia UE censura la disciplina bulgara, la quale ammette la conservazione dei dati biometrici e genetici di una persona condannata per un "un reato doloso perseguibile d'ufficio" sino al suo decesso, in quanto le fattispecie rientranti in tale categoria delittuosa «non presentano tutte lo stesso grado di rischio» (§ 60).

[59] Così al § 69 della sentenza in commento.

Sul piano operativo, peraltro, i limiti temporali delineati in astratto dai legislatori nazionali non escludono il dovere di esprimere valutazioni calibrate sulla specificità del caso concreto che, tenendo conto di elementi dai quali desumere un pericolo meno elevato di recidiva, consentono di ridurre la durata della conservazione. In tal senso, l'intervenuta riabilitazione del condannato – la quale presuppone che egli non abbia commesso ulteriori reati dopo aver scontato la pena – costituisce l'indizio di una minore pericolosità e, quindi, un fattore idoneo a giustificare l'accoglimento della domanda di espunzione dei profili biometrici e genetici dal *database*[60], anche prima dei termini fissati dalle previsioni normative.

Nella visione pragmatica dei Giudici di Lussemburgo, dunque, non potendosi reputare legittimo custodire i dati sensibili di una persona condannata sino al suo decesso, grava sull'autorità interna l'obbligo di esaminare periodicamente la permanenza dei requisiti che ne giustificano la conservazione e, in ogni caso, va assicurato all'interessato il diritto di ottenerne la cancellazione nel caso in cui il trattenimento presso il *database* non è più necessario rispetto alle finalità per le quali sono stati raccolti.

La decisione in commento, d'altra parte, ben si colloca nel più ampio mosaico delle pronunce della Corte EDU, dalle quali si scorgono ulteriori significative indicazioni per assicurare l'efficace tutela della *privacy*.

Per i giudici di Strasburgo l'archiviazione *sine die* di massicce quantità di dati sensibili – sebbene orientata a incrementare le *chances* di identificare gli autori dei reati – è reputata in radicale conflitto con l'art. 8 C.E.D.U., in quanto equivarrebbe a giustificare la raccolta dei profili genetici e biometrici di tutta la popolazione, ledendo irreversibilmente il canone della stretta necessità[61].

D'altro canto, la circostanza che gli ordinamenti stabiliscano dei termini di durata massima per la *data retention* non esclude di per sé interferenze indebite nella vita privata.

Affinché le garanzie riconosciute al singolo siano "concrete ed effettive", occorre che la disciplina nazionale delinei con chiarezza i presupposti al ricorrere dei quali l'interessato può ottenere la rimozione dei dati che lo riguardano. In

[60] Sul punto, la decisione conferma, però, l'imprescindibilità di un approccio casistico, atteso che la riabilitazione di una persona, «che comporta la cancellazione della sua condanna dal casellario giudiziale [...] non può di per sé escludere la necessità della conservazione dei suoi dati nel registro di polizia, poiché quest'ultima risponde a finalità diverse a quella dell'elenco dei suoi precedenti penali in detto casellario giudiziale» (§61).

[61] Corte EDU, 13 febbraio 2020, *Gaughran c. Regno Unito*, §89, in *Giur. it.*, 2020, 529 ss.

questa prospettiva, qualora il quadro normativo sia caratterizzato da clausole eccessivamente elastiche, si assegna all'autorità interna un potere incontrollabile che rende l'accoglimento della domanda formulata dall'interessato un'ipotesi "teorica e illusoria"[62], tramutando il diritto alla cancellazione in mero simulacro.

A fortiori, le garanzie per l'interessato vanno decisamente irrobustite qualora la *data retention* riguarda persone solo sospettate di aver commesso un reato, ma poi non perseguite o assolte. Invero, nonostante agli ordinamenti interni non sia preclusa in assoluto la possibilità di archiviare i profili genetici e biometrici appartenenti a soggetti non condannati, in questo caso, non profilandosi il pericolo di commissione di ulteriori reati (escluso dalla decisione di proscioglimento o di non esercitare l'azione penale), difficilmente la conservazione delle informazioni in questione sarebbe giustificabile in quanto "necessaria in una società democratica" (art. 8 C.E.D.U.).

Ma, al di là di tale rilievo, la *retention* a tempo indeterminato dei profili genetici o biometrici appartenenti a una persona non perseguita o assolta, espone quest'ultima a un elevato rischio di stigmatizzazione, il quale stride con la regola di trattamento sottesa alla presunzione di innocenza (art. 6 §2 C.E.D.U.)[63]: in simili evenienze, il soggetto uscito indenne dalla vicenda giudiziaria subirebbe le medesime conseguenze, quanto alla conservazione dei dati sensibili, riservate a chi invece è stato condannato.

Da questo punto di vista, l'archiviazione indistinta, *sine die*, delle informazioni genetiche o biometriche della persona non attinta da una decisione di condanna collide con il divieto, imposto dalla fonte convenzionale (art. 6 §2 C.E.D.U.), di non esprimere convincimenti colpevolisti o sospetti sull'innocenza dell'accusato dopo che costui è stato prosciolto.

Si tratta, del resto, di un aspetto valorizzato anche dalla disciplina sulla *data*

---

[62] In proposito la Corte di Strasburgo ha condannato la Francia per violazione dell'art. 8 C.E.D.U., in quanto la normativa nazionale, nonostante stabilisse un termine massimo di conservazione di venticinque anni, imponeva di alimentare il *database* «con il maggior numero possibile» di informazioni personali, indicando tra gli scopi del trattamento, da un lato, la necessità di agevolare la ricerca e l'identificazione degli autori di crimini e delitti e, dall'altro, quella di «facilitare l'avvio, l'istruzione e il giudizio delle cause di cui sia investita l'autorità giudiziaria». Simili finalità rendevano pertanto in concreto assai remota l'ipotesi che l'istanza di cancellazione formulata dall'interessato potesse essere accolta. Cfr. Corte EDU, 18 aprile 2013, *M.K. c. Francia*, cit., §§ 25-26.

[63] Cfr. Corte EDU, Grande Camera, 4 dicembre 2008, *S. & Marper c. Regno Unito*, cit., § 124; Corte EDU, 18 aprile 2013, *M.K. c. Francia*, cit., § 23. In particolare, sul punto, si sofferma CAPITTA, *Conservazione dei DNA* profiles *e tutela europea dei diritti dell'uomo*, cit., 14 ss.

protection (art. 6 Direttiva 2016/680/UE) nella misura in cui – allineandosi con la Direttiva 2016/343/UE sull'irrobustimento della presunzione di non colpevolezza – sollecita i Paesi membri a operare «una chiara distinzione tra i dati personali delle diverse categorie di interessati» coinvolti, a vario titolo, nel procedimento penale (indagati, imputati, condannati, vittime del reato, testimoni)[64].

L'obiettivo principale è garantire un elevato *standard* di salvaguardia dei dati appartenenti a persone non destinatarie dell'addebito, evitando irragionevoli equiparazioni di trattamento tra i diversi soggetti implicati nell'accertamento giudiziario[65].

Il proposito rischia però di trasformarsi in una mera petizione di principio: le previsioni eurounitarie omettono di definire, con particolare riferimento alle persone "non sospettate", le conseguenze della distinzione soggettiva delineata dall'art. 6 della Direttiva 2016/680/UE[66]; in difetto di coordinate nitide, vi è quindi un ampio margine di discrezionalità per i legislatori interni nel delineare gli elementi che dovrebbero contraddistinguere il trattamento "differenziato" – sui limiti (anche temporali) per la conservazione dei dati, nonché sulle finalità di utilizzo – in base ai distinti ruoli processuali dei soggetti interessati[67].

Malgrado le segnalate criticità, la decisione in commento, pur non avendo di-

---

[64] Il nesso tra trattamento dei dati personali e presunzione di innocenza è valorizzato anche nel considerando § 31 della Direttiva 2016/680/UE.

[65] D'altronde si è evidenziato che il «diritto alla riservatezza nella sua più generale accezione» impone di individuare «un criterio di selezione *ratione personae* che porti a specificare chi può essere costretto a fornire i dati per archiviarli a fini preventivi o potenzialmente repressivi [...] La c.d. servitù di giustizia del terzo si configura nel processo penale, per fini specifici e sul presupposto che si ipotizzi un legame tra il terzo ed il reato; per contro, in ordinamenti che garantiscano i diritti fondamentali, non può configurarsi una generale "servitù di Stato" che possa prevalere sulla tutela delle istanze individuali anche a scopi preventivi, pena lo scadimento in un regime di polizia». Così, CONTI, *Il corpo dell'imputato come prova: il diritto di non collaborare tra prospettive sovraordinate, suggestioni storiche e polifunzionalità dei dati*, in *Dir. pen. proc.*, 2024, 1, 118.

[66] In tal senso, TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, cit., 339. Per ulteriori criticità sul punto, si veda GALGANI, *Giudizio penale,* Habeas data *e garanzie fondamentali*, cit., 9.

[67] D'altronde la stessa Corte di giustizia UE, pur affermando che «gli Stati membri devono provvedere affinché sia operata una chiara distinzione tra i dati delle diverse categorie di interessati in modo che [...] non sia loro imposta indistintamente un'ingerenza della medesima intensità nel loro diritto fondamentale alla protezione dei propri dati personali a prescindere dalla categoria a cui appartengono», precisa che si tratta di un obbligo non assoluto (Corte giust. UE, sez. V, 26 gennaio 2023, C-205/21, V.S., cit., §§ 83-84).

panato tutti i nodi, ha comunque il merito di aver aggiunto un importante tassello sulle caratteristiche essenziali della *data protection*, fungendo da ulteriore stimolo per gli Stati membri a incrementare il livello di tutela della *privacy*.

4. *Riflessi nello scenario interno e* deficit *di tutela: i tempi di conservazione....*
Sul piano dell'effettività occorre però chiedersi se l'archetipo delineato dalla Direttiva UE/2016/680, anche alla luce degli interventi della Corte di giustizia UE, sia davvero in grado di spronare i legislatori nazionali a foggiare un robusto "scudo" per il diritto all'autodeterminazione informativa, preservandolo da interventi ipertrofici dell'autorità.
Volgendo lo sguardo al sistema italiano, si ha la netta sensazione che il legislatore nel recepire la Direttiva (con il d.lgs. 18 maggio 2018, n. 51), abbia tradito, sotto diversi profili, l'aspettativa di allestire forme adeguate di tutela dei dati personali adoperati dalle autorità per scopi preventivi e repressivi.
Esaminando i contenuti più rilevanti della disciplina interna, in effetti, spicca una significativa lacuna proprio sul tema, vagliato di recente dai Giudici di Lussemburgo, relativo alla durata della *data retention*.
Limitandosi a trasporre in modo acritico i contenuti della fonte eurounitaria (artt. 5 e 16 § 2 Direttiva UE/2016/680), il d.lgs. 51 del 2018 stabilisce che la conservazione dei dati personali è limitata al «tempo necessario al conseguimento delle finalità per le quali sono trattati», imponendone la cancellazione «una volta decorso tale termine» (art. 3, co. 1, lett. e) «senza ingiustificato ritardo» (art. 12, co. 2).
Si ripropongono così le già segnalate ambiguità delineate dalla Direttiva sull'impiego di formule eccessivamente vaghe – "tempo necessario" e "senza ingiustificato ritardo" – che compromettono la portata del diritto dell'interessato alla rimozione dei dati[68].
Se però sul versante europeo è comprensibile l'uso di un lessico "impreciso" – nell'intento di armonizzare i diversi sistemi nazionali, senza intaccare oltremisura la sovranità degli Stati – il silenzio serbato dal legislatore italiano appare del tutto ingiustificato e foriero di significativi dubbi esegetici.
In difetto di riferimenti espliciti nel d.lgs. 51/2018, per individuare i termini di durata massima della *retention* bisognerebbe far riferimento a quelli specificati nella normativa di rango secondario (art. 10, d.P.R. 15 gennaio 2018, n. 15), la

[68] *Supra* § 3.

quale, in attuazione dell'art. 57 cod. *privacy*, detta le regole per «il trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia»[69].

Sennonché, la disposizione di "copertura" della fonte regolamentare (art. 57 cod. *privacy*) è stata abrogata proprio dalla normativa di recepimento della Direttiva (art. 49, co. 2, d.lgs. 51/2018).

Tuttavia il legislatore mette a riparo l'efficacia del d.P.R. 15/2018, affermando che le previsioni ivi contenute continuano ad applicarsi sino all'entrata in vigore di una diversa disciplina attuativa (art. 49, co. 3, d.lgs. 51/2018)[70].

Questo regime "transitorio" però non risolve i problemi: considerato che il d.P.R. 15/2018 è antecedente al d.lgs. 51/2018, si profila una complessa attività ermeneutica per stabilire la compatibilità dei precetti di livello secondario con la fonte superiore che ha recepito la Direttiva.

Si tratta, insomma, dell'ennesimo *pastiche* legislativo che potrebbe creare lacune allarmanti: l'ambito operativo del d.P.R. 15/2018, essendo circoscritto solo al trattamento effettuato per "finalità di polizia giudiziaria" e di "tutela dell'ordine e della sicurezza pubblica", è molto più modesto rispetto a quello delineato dal d.lgs. 51/2018; di conseguenza, quanto meno sul tema sin qui speculato, non può dirsi soddisfatto appieno l'obiettivo, imposto dalla Direttiva UE/2016/680, di delineare un compiuto apparato di regole idoneo a salvaguardare i dati personali.

Ma, anche a voler prescindere da queste perplessità, i tempi indicati dall'art. 10 d.P.R. 15/2018 – i quali variano da un minimo di diciotto mesi a un massimo di trenta anni, ulteriormente aumentati di due terzi se riguardano attività, preventive o repressive, concernenti i gravi reati di cui agli artt. 51, co. 3-*bis*, 3-*quater*, 3-*quinquies*, e 407, co. 2, lett. a) c.p.p. – appaiono oltremodo ampi e mal si conciliano con la logica della "necessità" del trattamento[71].

---

[69] Per le perplessità sulla scelta di affidare a una fonte di rango non legislativo la disciplina dei termini di durata del trattamento dei dati personali, si veda GALGANI, *Giudizio penale,* Habeas data *e garanzie fondamentali*, cit., 9; SIGNORATO, *Il trattamento dei dati personali per le finalità di polizia: la nuova disciplina prevista dall'art. 53 Codice Privacy e gli scenari europei*, in *Il nuovo "pacchetto" antiterrorismo,* a cura di Kostoris-Viganò, Torino, 2015, 95 ss.

[70] In proposito, v. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in *Cybercrime*, diretto da Cadoppi-Canestrari-Manna-Papa, Torino, 2023, 1884.

[71] D'altronde, anche con riferimento alla *retention* dei c.d. "metadati di traffico" «per finalità di accertamento e repressione di reati» la disciplina non pare del tutto allineata con il canone della necessarietà, nella misura in cui, in deroga ai limiti ordinari fissati dall'art. 132, co. 1 e 1-*bis*, cod. *privacy*, stabilisce in sei anni il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle

Nell'ottica della proporzionalità, in effetti, appare censurabile la scelta di ammettere che la *retention* possa prolungarsi per un arco temporale considerevole anche con riferimento ai dati relativi a indagini concluse con l'archiviazione (venti anni dall'emissione del provvedimento [art. 10, co. 3, lett. f), d.P.R 15/2018]) o, addirittura, a quelli che «non hanno dato luogo a procedimento penale» (quindici anni dall'ultimo trattamento [art. 10, co. 3, lett. i), d.P.R. 15/2018][72].

D'altra parte, persino ponendo lo sguardo sui tempi di conservazione dei dati "sensibili", le scelte non sono immuni da critiche.

Nell'ambito delle specifiche regole sulla banca dati nazionale del DNA[73] – il cui assetto non è stato alterato dal d.lgs. 51/2018 – il principio del "minor sacrificio necessario" è osservato nel caso di sentenza definitiva di assoluzione con formula ampiamente liberatoria, imponendo l'immediata cancellazione d'ufficio dei profili genetici (art. 13, co. 1, L. 85/2009)[74]; in questo modo, si punta a salvaguardare la *privacy*, ammettendone la limitazione solo quando davvero

---

chiamate senza risposta, «per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-*quater*, e 407, comma 2, lettera a), c.p.p.» (art. 24, L. 20 novembre 2017, n. 167). Sul punto, ANDOLINA, *L'acquisizione nel processo penale dei dati «esteriori» delle comunicazioni telefoniche e telematiche*, Padova, 2018, *passim*; CAPRARO, *L'approvvigionamento di dati "esteriori" alle comunicazioni*, in *Le indagini atipiche*, cit., 147 ss.; FILIPPI, *Le nuove norme su intercettazioni e tabulati*, Pisa, 2017, 47; SIGNORATO, *Contrasto al terrorismo e* data retention*: molte ombre e poche luci*, in *Il nuovo "pacchetto" antiterrorismo*, cit., 78 ss. Per le novità nella disciplina sull'acquisizione dei tabulati introdotte dal D.L. 30 settembre 2021, n. 132, convertito, con modificazioni, dalla L. 23 novembre 2021, n. 178, si veda ANDOLINA, *Acquisizione dei dati esterni*, in *La nuova disciplina delle intercettazioni*, a cura di Maggio, Torino, 2023, 402 ss.; CHELO, Tabula rasa *sui tabulati? Riflessioni a margine della recente giurisprudenza della Corte di giustizia dell'Unione europea*, in *Cass. pen.*, 2022, 9, 3268 ss.; DEMARTIS, *La nuova disciplina sui tabulati: un completo adeguamento agli* standard *europei?*, in *Dir. pen. proc.*, 2022, 3, 299 ss.; DINACCI, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative*, in *Proc. pen. giust.*, 2022, 2, 301 ss.; FILIPPI, *La nuova disciplina dei tabulati*, in *www.penaledp.it*, 1° ottobre 2021; ID., *Il decreto-legge sui tabulati*, in *Pen. dir. proc.*, 2021, 3, 527 ss.; GIANGRECO, Data retention*, acquisizione e utilizzabilità dei tabulati telefonici e telematici: una riflessione incrociata*, in *Cass. pen.*, 2022, 4, 1672 ss.; MALACARNE, *"Gravità" dell'ingerenza e "terzietà" dell'organo titolare del potere autorizzatorio: vecchi e nuovi principi in materia di* data retention, in *Riv. it. dir. proc. pen.*, 2021, 3, 1164 ss.; MARCOLINI, *L'istituto della* data retention *tra legalità interna ed internazionale*, in *Cybercrime*, cit., 2023, 1849 ss.; PASTA, *Luci e ombre nella disciplina dei tabulati nel processo penale*, in *Cass. pen.*, 12, 2022, 4458 ss.; SPANGHER, Data retention*: svolta garantista ma occorre completare l'impianto*, in *Guida dir.*, 2021, 39, 11 ss.; TAVASSI, *Acquisizione di tabulati, tutela della privacy e rispetto del principio di proporzionalità*, in *Arch. pen. web*, 1, 2022.

[72] In proposito si vedano le osservazioni critiche di GALGANI, *Giudizio penale,* Habeas data *e garanzie fondamentali*, cit., 11.

[73] Istituita con la L. 30 giugno 2009 n. 85.

[74] Sul punto FELICIONI, *La prova del DNA nel procedimento penale*, Milano, 2018, 378.

indispensabile[75].
Viceversa, in tutti gli altri casi, il criterio della "stretta necessità" – che, come ricordato, rappresenta la bussola che dovrebbe guidare le scelte legislative (art. 10 Direttiva UE/680/2016) – non pare adeguatamente valorizzato.
In linea generale, è lecito dubitare sulla congruità della scelta di consentire un'ampia durata della *retention*, fissando in trenta anni il termine di trattenimento nella banca dati dei profili del DNA (art. 25, co. 1, d.P.R. 7 aprile 2016, n. 87[76]; periodo che, peraltro, è prorogato di ulteriori dieci anni se il profilo appartiene a una persona condannata per reati di particolare gravità o dichiarata recidiva con sentenza definitiva[77]). Le perplessità, inoltre, si acuiscono tenuto conto della "flessibilità" del *dies a quo* dalla schedatura del dato genetico che, essendo agganciato alla «data dell'ultima registrazione» del profilo del DNA (art. 25, co. 1, d.P.R. 87/2016), può determinare un significativo slittamento in avanti del termine iniziale, allungando il tempo complessivo di permanenza nel *database*.
Sullo sfondo, si addensano poi ulteriori criticità laddove si consideri che tra i canali di approvvigionamento della banca dati del DNA[78] (art. 9, co. 1, L. 85/2009), rientrano anche i profili di persone che, pur avendo subito una coercizione della libertà personale nel corso del procedimento[79], hanno beneficiato di un provvedimento di archiviazione o di una sentenza di non luogo a procedere.

---

[75] In tal senso, FANUELE, *La prova del DNA*, cit., 581; FELICIONI, *Il regolamento di attuazione della banca dati nazionale del DNA: scienza e diritto si incontrano*, in *Dir. pen. proc.*, 2016, 6, 741; TONINI, *Manuale di procedura penale*, Milano, 2019, 605.

[76] Si tratta del decreto con il quale è stato delineato il regolamento di attuazione della banca dati del DNA; sul tema si veda, tra gli altri, FANUELE, *Il regolamento attuativo della banca dati nazionale del DNA: nuove garanzie e preesistenti vuoti di tutela*, in *Proc. pen. giust.*, 2017, 1, 121 ss.; FELICIONI, *Il regolamento di attuazione della banca dati nazionale del DNA: scienza e diritto si incontrano*, cit., 724 ss.; RICCI, *Un lampo di consapevolezza nella normativa italiana: il DNA oltre la suggestione e il mito*, in *Dir. pen. proc.*, 2016, 6, 743 ss.

[77] In particolare, si stabilisce che il periodo di conservazione è di quaranta anni nel caso di profili del DNA riferiti a persone condannate con sentenza irrevocabile per uno o più dei reati per i quali la legge prevede l'arresto obbligatorio in flagranza, o per taluno dei reati di cui all'art. 407, co. 2, lett. a), c.p.p. (art. 25, co. 2, d.P.R. 87/2016) o, ancora, nel caso in cui sia stata ritenuta la recidiva in sede di emissione della sentenza di condanna definitiva (art. 25, co. 3, d.P.R. 87/2016).

[78] Sul punto, da ultimo, FELICIONI, *La prova del DNA*, cit., 171 ss.

[79] L'art. 9, co. 1, l. 85/2009, stabilisce che tra i diversi soggetti sottoposti a prelievo di campioni biologici, ai fini dell'inserimento del profilo del DNA nella banca dati nazionale del DNA, rientrano anche coloro «a) [...] ai quali sia applicata la misura della custodia cautelare in carcere o quella degli arresti domiciliari» e «b) i soggetti arrestati in flagranza di reato o sottoposti a fermo di indiziato di delitto».

Viene, in sostanza, delineata una deprecabile categoria di soggetti "sospettabili onesti"[80] i quali, nonostante siano stati prosciolti da qualsiasi accusa, sono schedati nel *database* genetico e i cui profili potranno essere utilizzati per ipotetiche attività investigative da svolgere in futuro (nel caso di riapertura delle indagini *ex* artt. 414 o 436, co. 2, c.p.p.[81]).

Si tratta di una scelta che collide con la presunzione di non colpevolezza, nella misura in cui sottopone al medesimo trattamento riservato ai soggetti condannati i destinatari di un provvedimento (archiviazione o non luogo a procedere) che, sebbene privo del crisma dell'irrevocabilità, esclude i presupposti per esercitare o proseguire l'azione penale.

Ancor più deplorevole è l'opzione legislativa di limitare la cancellazione d'ufficio dei dati genetici solo con riferimento alle assoluzioni con "formula piena" (art. 13, l. 85/2009), permettendo di trattenere nel *database* – sempre per trenta anni come avviene per i condannati con sentenza irrevocabile – i profili del DNA di persone prosciolte con decisione definitiva di non doversi procedere o, addirittura, assolte perché il reato è stato commesso da persona non imputabile o non punibile[82]. Qualora il procedimento si concluda con uno di questi epiloghi, infatti, non si pone nemmeno l'eventuale probabilità della riapertura della fase investigativa[83].

L'assetto in questione, oltre a porsi in evidente contrasto con il divieto – imposto dai valori primari (art. 27, co. 2, Cost.) – di esprimere opinioni colpevoliste

---

[80] Così, SCAFFARDI, *Giustizia genetica e tutela della persona*, cit., 245. L'A. evidenzia il paradosso della disciplina italiana: «sarebbe meglio subire tre gradi di giudizio volti a dimostrare una definitiva innocenza (con conseguente cancellazione d'ufficio dei propri dati genetici), piuttosto che essere stati soltanto indagati, ma successivamente non meritevoli di giungere a processo magari per carenza di elementi di accusa. Un "proscioglimento" che al contrario, impone il mantenimento dei campioni e del profilo del DNA negli archivi statali». In tal senso, cfr. anche GENNARI, *Bioinformazione e indagini penali: la l. n. 85 del 30 giugno 2009,* in *Resp. civ. e prev.*, 2009, 12, 2636

[81] Peraltro, considerato che l'art. 22, co. 1, lett. h), d.lgs. 10 ottobre 2022, n. 150 (c.d. riforma Cartabia) ha novellato l'art. 414 c.p.p., rendendo più stringenti i requisiti per ottenere la riapertura delle indagini, appare ancor più criticabile la scelta di consentire che i profili genetici appartenenti a soggetti che hanno ottenuto un provvedimento di archiviazione, siano conservati, al pari di quelli dei condannati con sentenza irrevocabile, per un periodo di trenta anni. Sui nuovi presupposti per ottenere la riapertura delle indagini, si veda LA REGINA, *L'archiviazione nel vortice efficientista*, in *La riforma Cartabia*, a cura di Spangher, Pisa, 2022, 296 ss.

[82] Sul punto, ABRUSCI, *Cancellazione dei profili e distruzione dei campioni*, in *Banca dati del DNA e accertamento penale*, cit., 115 ss.; CAPITTA, *Conservazione dei DNA* profiles *e tutela europea dei diritti dell'uomo*, cit., 27 ss.

[83] Fatta salva l'infrequente e remota ipotesi, relativamente a una sentenza di non doversi procedere, di riproposizione dell'azione penale nei casi previsti dall'art. 345 c.p.p.

o formulare sospetti sull'innocenza della persona prosciolta, stride con i moniti della Corte di Strasburgo[84], in quanto produce un'ingerenza nella vita privata sproporzionata rispetto alla finalità perseguita; per porvi rimedio sarebbe auspicabile, quanto meno, stabilire termini di conservazione dei dati del DNA più ristretti rispetto a quelli imposti a coloro nei cui confronti è stata affermata irrevocabilmente la responsabilità penale[85].
In sintesi, nonostante siano trascorsi diversi anni dall'entrata in vigore del d.lgs. 51/2018, sono ancora molti i nodi insoluti e, nel complesso, l'articolato mosaico normativo non assicura che la durata della *retention* dei dati, anche sensibili, sia conforme al criterio della necessarietà delineato dalla Direttiva UE/680/2016.

5. ... l'ineffettività delle garanzie. Ampliando l'orizzonte agli altri contenuti del d.lgs. 51/2018, si scorgono ulteriori significativi *deficit* di tutela.
La trama normativa riconosce – con specifico riferimento «ai dati personali contenuti in una decisione giudiziaria, in atti o documenti oggetto di trattamento nel corso di accertamenti o indagini, nel casellario giudiziale o in un fascicolo oggetto di trattamento nel corso di un procedimento penale o in fase di esecuzione penale» (art. 14, co. 1, d.lgs. 51/2018) – talune prerogative funzionali a garantire al singolo la consapevolezza in ordine alle modalità con le quali i propri dati sono gestiti dall'autorità giudiziaria (artt. 10 e 11, d.lgs. 51/2018), corredandole con il diritto a ottenerne la rettifica, la cancellazione o, qualora non sia possibile rimuoverli, a pretendere di limitarne il trattamento (art. 12, d.lgs. 51/2018).
Sul terreno dell'effettività, però, le indicate guarentigie stentano ad affermarsi e prassi lassiste potrebbero sterilizzarne i frutti.
La salvaguardia dell'autodeterminazione informativa delle persone implicate nella vicenda giudiziaria – che negli auspici dovrebbe rappresentare l'obiettivo principale della *data protection* – è frustrata dalla smodata genericità con la quale sono confezionate le previsioni che restringono la portata dei diritti dell'interessato.
Questi ultimi, di fatto, «possono essere ritardati, limitati o esclusi» in un ampio ventaglio di ipotesi: qualora sia necessario «per non compromettere il buon

[84] Corte EDU, Grande Camera, 4 dicembre 2008, *S. & Marper c. Regno Unito*, cit., § 124.
[85] In proposito, GABRIELLI, *L'archiviazione dei dati genetici a fini di giustizia penale*, cit., 1414-1415.

esito» delle attività del procedimento penale o ad esso collaterali[86]; per «tutelare la sicurezza pubblica» o «nazionale»; per proteggere «diritti e libertà altrui» (art. 14, co. 2, d.lgs. 51/2018).

Il legislatore, nel recepire pressoché pedissequamente i contenuti della Direttiva UE/2016/680 (artt. 15, § 1, e 16, § 4), riproduce le medesime criticità della fonte eurounitaria[87] e – delineando scopi estremamente generici per derogare all'esercizio dei diritti individuali[88] – attribuisce al potere giudiziario un'enorme discrezionalità, che alimenta il pericolo di decisioni arbitrarie capaci di annichilire i diritti riconosciuti all'interessato[89].

Eppure, l'efficace tutela della *privacy* esige di delineare con precisione le ipotesi in cui essa può essere limitata: le previsioni normative dovrebbero delimitare entro coordinate ben determinate gli spazi di manovra della magistratura nel gestire i dati personali e, soprattutto, circoscrivere con chiarezza i motivi che giustificano la compressione delle garanzie.

Nell'attesa di un ripensamento legislativo, un corretto approccio alla disciplina, propenso a fortificare la concretezza della *data protection*, imporrebbe di considerare come eccezionali le ipotesi indicate dall'art. 14, co. 2, d.lgs. 51/2018, obbligando a interpretare in termini stringenti le deroghe ivi enunciate.

Muovendosi in questa direzione, allora, le restrizioni dei diritti dell'interessato andrebbero permesse solo se realmente indispensabili e proporzionate rispetto alle finalità del procedimento penale.

Occorre pertanto reperire i criteri utili a vagliare la congruità dell'ingerenza nella *privacy* e, in parallelo, a stabilire il confine oltrepassato il quale essa diventa illegittima, abilitando l'interessato a esercitare i diritti riconosciuti dal d.lgs. 51/2018.

---

[86] In tal senso l'art. 14, co. 2, lett. a), d.lgs. 51/2018, oltre alle attività di indagine, accertamento e perseguimento di reati, include tra le finalità che legittimano la limitazione dei diritti dell'interessato, anche le attività compiute per scopi preventivi o finalizzate all'esecuzione «di sanzioni penali, nonché l'applicazione delle misure di prevenzione personali e patrimoniali e delle misure di sicurezza».

[87] *Supra* § 2.

[88] L'eccessiva ampiezza delle finalità delineate dall'art. 14, co. 2, d.lgs. 51/2018 che permettono di restringere la portata dei diritti riconosciuti all'interessato, è stata criticata da BACCARI-CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla* privacy*: uno sguardo d'insieme*, cit., 715; LUPÁRIA DONATI, Privacy, *diritti della persona e processo penale*, cit., 1467; TORRE, *Protezione dei dati personali, processo penale e intercettazioni*, in *Dir. pen. proc.*, 2019, 183.

[89] Si è peraltro osservato come nell'art. 14 d.lgs. 51/2018 manca «qualunque traccia del dovere di risposta "per iscritto, senza ritardo e con apposita motivazione", previsto dalla disposizione europea per i casi di diniego del diritto di accesso». Così, VALENTINI, *Forme di privazione del diritto di difesa nello Stato senza diritto (ovvero: come un gioco di parole diventa realtà)*, cit., 22.

Seguendo tale itinerario, il parametro basilare per stimare la "necessarietà" del trattamento va rintracciato nel criterio di pertinenza che governa l'inchiesta penale sin dalle sue prime battute (art. 187 c.p.p.)[90]: solo delimitando l'intervento dell'autorità entro determinati argini – calibrati, nella fase preliminare, sulla *notitia criminis* e poi, nel processo, sull'imputazione – è possibile assicurare che la raccolta e la gestione dei dati personali arrechi il "minor sacrificio necessario" ai soggetti coinvolti nell'accertamento, evitando manovre meramente esplorative, dirette all'approvvigionamento indiscriminato di elementi probatori estranei alla verifica giudiziaria[91].

Accogliendo questa idea, il requisito della "necessarietà" rinvigorisce il criterio selettivo delle informazioni personali da acquisire e «segna i confini di liceità del trattamento»[92]; sicché qualora i dati si rivelino eccedenti rispetto alle finalità

---

[90] In proposito si è efficacemente scritto che «partendo da un'idea di maggiore legalità della fase preliminare, l'investigazione non ha un carattere esplorativo, ma si muove in un campo delimitato già dalla notizia di reato, attraverso la quale è possibile individuare un iniziale addebito; cosicché, l'oggetto dell'indagine coincide con i fatti desumibili da un quadro originario dal quale selezionare una contestazione che via via si affina». In questi termini, SCALFATI-SERVI, *Premesse sulla prova penale*, in *Prove e misure cautelari*, a cura di Scalfati (*Trattato di procedura penale*, diretto da Spangher), Torino, 2009, vol. 2, t. 1, 21-22. Propendono per una lettura estensiva dell'art. 187 c.p.p. anche con riferimento alla fase investigativa, tra gli altri, CAMON, *La fase che "non conta e non pesa": indagine governate dalla legge?*, in *Dir. pen. proc.*, 2017, 4, 430 ss.; CORVI, sub *art. 187 c.p.p.*, in *Codice di procedura penale commentato*, a cura di Giarda-Spangher, Milano, 2017, I, 1871-1872; GREVI, *Prove*, in *Compendio di procedura penale*, a cura di Conso-Grevi-Bargis, Padova, 2012, 305; MARZADURI, *Misure cautelari personali (principi generali e disciplina)*, in *Dig. pen.*, vol. III, Torino, 1994, 66; NOBILI, sub *art. 187 c.p.p.*, in *Commento al nuovo codice di procedura penale*, coordinato da Chiavario, II, Torino, 1992, 391 ss.; UBERTIS, *La ricerca della verità giudiziale*, in *La conoscenza del fatto nel processo penale*, a cura di Ubertis, Milano, 1992, 18. In senso contrario, v. BERNASCONI, *Prove*, in *Manuale di diritto processuale penale*, a cura di Scalfati, Torino, 2023, 258-259; SIRACUSANO, *Prova (nel nuovo codice di procedura penale)*, in *Enc. giur.*, Roma, 2003, 2.

[91] Si intuisce come il pericolo di intrusioni arbitrarie nella *privacy* è maggiore quando la ricerca probatoria è eseguita su dispositivi digitali (ad es. *smartphone* o *personal computer*) abili nel custodire un'elevata mole di dati personali, anche sensibili, capaci di svelare gli aspetti più intimi della persona e di ricostruire profili rilevanti della vita privata (permettendo di ricostruire le abitudini personali, inclinazioni sessuali, religiose, politiche). In questi casi è infatti quanto mai concreto il rischio che l'autorità giudiziaria si impossessi – anche servendosi di evoluti congegni tecnologici, tra i quali spicca il captatore informatico – di una quantità indistinta di dati, procurandosi conoscenze del tutto estranee al reato per il quale si sta procedendo. Proprio su questo versante, il criterio della necessarietà – quale componente indefettibile del canone di proporzione – impone particolare rigore nel selezionare i *files* custoditi nelle memorie digitali, circoscrivendone la ricerca e l'acquisizione a quanto effettivamente indispensabile per l'accertamento dell'addebito. Per ulteriori rilievi si veda, volendo, BELVINI, *Principio di proporzionalità e attività investigativa*, cit., in particolare, 177 ss., 188 ss. e 242 ss.

[92] RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine accertamento e perseguimento di reati*, cit., 579.

probatorie, bisognerebbe sempre assicurare all'interessato il diritto di ottenerne la cancellazione, permettendo così di espungerli dal panorama cognitivo e di riaverne l'esclusiva disponibilità[93].

Quanto sin qui illustrato dovrebbe costituire il primo passo per stabilire con maggior rigore i requisiti "sostanziali" per ottenere la cessazione del trattamento.

Ciononostante, è sul versante procedurale che si annidano le più consistenti criticità ostative all'effettivo esercizio delle prerogative individuali riconosciute dal d.lgs. 51/2018.

Su questo fronte si riconosce a chiunque vi abbia interesse di chiedere, nel corso del procedimento penale o dopo la sua conclusione, «la rettifica, la cancellazione o la limitazione dei dati personali» con le modalità prescritte dall'art. 116 c.p.p., stabilendo, inoltre, che il giudice provvede con le forme delineate dall'art. 130 c.p.p. (art. 14, co. 1, d.lgs. 51/2018).

Il richiamo alla procedura per emendare gli errori materiali (art. 130 c.p.p.) sembrerebbe delineare un percorso che, essendo sorvegliato dall'organo giusdicente e garantendo il contradditorio secondo la liturgia del rito camerale (*ex* artt. 130, co. 2, e 127 c.p.p.), è in qualche misura idonea a salvaguardare i diritti dell'interessato, consentendogli di attivare anche rimedi impugnatori in sede di legittimità (art. 127, co. 7, c.p.p.).

Le cose invece stanno diversamente quando la richiesta è formulata durante le indagini preliminari.

Qui lo scarno telaio delineato dall'art. 116 c.p.p. si rivela del tutto inadeguato a tutelare efficacemente la riservatezza dell'interessato: essendo attribuita solo al pubblico ministero la competenza a rispondere sull'istanza, non solo non è assicurata alcuna imparzialità della decisione, ma manca anche la possibilità di attivare gli opportuni controlli *ex post* sul provvedimento di diniego.

In questo caso, peraltro, non sarebbe nemmeno invocabile l'intervento del Garante per la *privacy*, atteso che il legislatore esclude dal sindacato dell'organismo indipendente i «trattamenti effettuati dall'autorità giudiziaria nell'esercizio

[93] Su questo terreno, alcune indicazioni sono offerte dalla giurisprudenza, che riconosce all'indagato – o al terzo attinto dalla misura – l'interesse a impugnare il provvedimento di sequestro probatorio eseguito su dispositivi digitali, al fine di ottenere l'esclusiva disponibilità dei dati personali e riservati estratti dai *digital devices*. In tal senso tra le più recenti, Cass., sez. VI, 10 maggio 2022, n. 18502, in *Cass. pen.*, 2023, 2, 554, con nota di CASCONE, *La disponibilità esclusiva del dato informatico: una nuova pronuncia della Corte di cassazione a tutela del "patrimonio informativo"*.

delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero» (art. 37, co. 6, d.lgs. 51/2018)[94].
Si tratta di una scelta densa di ricadute negative: la difesa dei diritti dell'interessato è rimessa in balia delle decisioni del titolare dell'inchiesta preliminare, il cui ampio dominio si espande inarrestabilmente, al punto tale da sottrare a qualsivoglia forma di verifica, anche postuma, la legittimità del trattamento operato dallo stesso organo inquirente.
Per preservare uno *standard* minimo di garanzie, considerate le esigenze in gioco, potrebbe però reputarsi che la formula adoperata dal legislatore, secondo la quale il «giudice provvede con le forme dell'articolo 130» c.p.p. (art. 14, co. 1, d.lgs. 51/2018), deroghi all'*iter* tracciato dall'art. 116 c.p.p., attribuendo sempre la competenza a decidere sulla domanda di «rettifica, cancellazione o limitazione dei dati personali» all'organo giusdicente, anche se l'istanza è presentata durante la fase investigativa.
Qualora tale soluzione non fosse reputata percorribile, bisognerebbe assicurare (sulla falsariga di quanto prescritto dall'art. 263 c.p.p.) che, contro il provvedimento di diniego del pubblico ministero, l'interessato possa proporre opposizione sulla quale dovrebbe decidere il giudice con le forme del rito camerale.
Certo, *de iure condito*, letture di questo genere potrebbero essere tacciate di eccessiva "creatività", in quanto si discostano dal tenore letterale dell'art. 14 d.lgs. 51/2018.
Tuttavia, la "forzatura" del dato normativo potrebbe rivelarsi opportuna per riallineare il sistema interno alle coordinate sovranazionali.
In effetti, il bisogno di assicurare sempre il controllo del giudice – anche sul trattamento effettuato dal pubblico ministero durante le indagini preliminari – è imposto dall'art. 54 della Direttiva UE/2016/680, il quale obbliga i Paesi membri a garantire all'interessato il diritto a un "ricorso giurisdizionale effettivo" per censurare le violazioni dello statuto europeo sulla *data protection*.
Di conseguenza, un atteggiamento ortodosso imporrebbe, quanto meno, di adire in via pregiudiziale la Corte di giustizia UE, affinché si pronunci sulla compatibilità della disciplina italiana con le previsioni europee che pretendono

[94] L'opzione normativa è davvero molto discutibile in quanto «con un capolavoro espressivo» il legislatore «sottrae logicamente il p.m. all'esercizio di funzioni giurisdizionali -di fatto inesistenti nel nostro ordinamento- ma al contempo lo colora di una qualifica assimilatoria, all'evidente fine di sottrarre il suo *opus* ad ogni verifica». In questi termini, VALENTINI, *Forme di privazione del diritto di difesa nello Stato senza diritto (ovvero: come un gioco di parole diventa realtà)*, cit., 22.

l'allestimento di specifici rimedi di natura giurisdizionale.
D'altronde, anche a voler prescindere dalle specifiche fonti di diritto derivato, sempre più di frequente le Corti europee, valorizzando le norme europee di rango primario poste a presidio delle libertà inviolabili (artt. 52 C.D.F.U.E. e 8 C.E.D.U.), esigono che il vaglio sulla proporzionalità dell'intrusione dell'autorità nella sfera riservata delle persone sia eseguita dall'organo giusdicente.
I Giudici di Lussemburgo, pronunciandosi sull'affine tema dell'impiego dei c.d. "metadati di traffico", affermano che, per salvaguardare il giusto equilibrio tra finalità processuali e diritti del singolo, la verifica sulla congruità dell'ingerenza non può essere demandata al pubblico ministero, ma, dovendosene assicurare l'imparzialità e l'obiettività, va affidata a un organo terzo non coinvolto «nella conduzione dell'indagine penale» che agisca in «posizione di neutralità nei confronti delle parti del procedimento penale»[95].
A questa logica non dovrebbe sottrarsi nemmeno lo scrutinio sulla "necessarietà" del trattamento delle informazioni personali effettuato dal magistrato inquirente: il pubblico ministero – nonostante l'indipendenza sul piano istituzionale (art. 104 Cost.) – esercita, durante l'*iter* giudiziario, pur sempre il ruolo di antagonista dell'indagato e, perciò, non è in grado di assicurare una decisione imparziale sulla richiesta di «rettifica, cancellazione o limitazione dei dati personali»[96].

---

[95] Corte giust. UE, 2 marzo 2021, C-746/18, *H.K.*, cit., § 54. Proprio per adeguarsi alle indicazioni di questa sentenza, il legislatore italiano ha stabilito che l'acquisizione dei tabulati di traffico telefonico e telematico è ammessa – qualora sussistano "sufficienti indizi di reato" e i dati siano "rilevanti per l'accertamento dei fatti" – con decreto motivato del giudice «su richiesta del pubblico ministero o su istanza della persona sottoposta a indagini, della persona offesa e delle altre parti private» (art. 132, co. 3, cod. *privacy*, così come modificato dall'art. 1, co. 1 lett. a), D.L. 132/2021); fermo restando il potere del pubblico ministero di disporne l'acquisizione – quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini – con decreto motivato da sottoporre, nelle successive quarantotto ore, alla convalida del giudice (art. 321, co. 3-*bis*, cod. *privacy*, così come modificato dall'art. 1, co. 1 lett. b), D.L. 132/2021). Per i riferimenti bibliografici sulla nuova disciplina v. *supra* nota 71.

[96] Sull'esigenza di affidare al giudice lo scrutinio di proporzionalità dell'ingerenza realizzata dagli organi inquirenti, i Giudici di Lussemburgo osservano come la «circostanza che il pubblico ministero sia tenuto, conformemente alle norme che disciplinano le sue competenze e il suo status, a verificare gli elementi a carico e quelli a discarico, a garantire la legittimità del procedimento istruttorio e ad agire unicamente in base alla legge ed al suo convincimento non può essere sufficiente per conferirgli lo status di terzo rispetto agli interessi in gioco» (Corte giust. UE, 2 marzo 2021, C-746/18, *H.K.*, cit., § 56). D'altra parte, *mutatis mutandis*, anche la Corte di Strasburgo, in alcuni casi, valorizza questo aspetto: l'Italia è stata condannata per violazione dell'art. 8 C.E.D.U. in quanto, nel caso di perquisizione disposta dal pubblico ministero

Sotto questo profilo, dunque, il quadro normativo interno – impedendo all'interessato di contestare la decisione del titolare delle indagini che nega all'interessato l'esercizio dei diritti riconosciuti dal d.lgs. 51/2018 – sembrerebbe contrastare con gli *standard* indicati dalla Corte di giustizia UE.
E, allora, sarebbe bene che il legislatore intervenisse tempestivamente nell'irrobustire i presidi di controllo, piuttosto che attendere l'ennesimo monito dei Giudici europei. Nell'attesa di un auspicato e doveroso ripensamento della disciplina, spetta alla prassi il delicato compito di vigilare sull'effettività delle garanzie tipiche della *data protection*, evitando interventi squilibrati propensi a preservare l'efficacia dell'accertamento giudiziario a discapito dei diritti del singolo.

LORENZO BELVINI

non seguita da un provvedimento di sequestro probatorio, non era previsto alcun controllo giurisdizionale, *ex ante* o *ex post*, sulla legittimità del decreto di perquisizione; in questo modo la disciplina italiana non offriva sufficienti garanzie per «evitare il rischio di abuso di potere da parte delle autorità incaricate dell'indagini penali» (Corte EDU, 27 settembre 2018, *Brazzi c. Italia*, in *Proc. pen. giust.*, 2019, 2, 426 ss. con nota di M. TORRE, *Perquisizioni domiciliari e art. 8 CEDU: la Corte europea censura la mancanza di un "controllo effettivo" sulla necessità dell'ingerenza*). Anche in questo caso, il legislatore è poi "corso ai ripari", riconoscendo il diritto di proporre opposizione contro il provvedimento perquirente del pubblico ministero non seguito dal sequestro dei beni (art. 252-*bis* c.p.p., introdotto dall'art. 12 d.lgs. 150/2022). Sul tema, cfr. CASSIBBA-MANCUSO, *Le indagini preliminari fra innovazione e continuità*, in *Riforma Cartabia. La nuova giustizia penale*, a cura di Castronuovo-Donini-Mancuso-Varraso, Milano, 2023, 620 ss.; DI GERONIMO, *Il controllo giurisdizionale sulla legittimità della perquisizione*, in *La riforma del sistema penale*, a cura di Bassi-Parodi, Milano, 2022, 133 ss.; MURONE, *Il controllo giurisdizionale sulla legittimità della perquisizione*, in *Dir. pen. proc.*, 2023, 1, 203 ss.; NOCERINO, *Il vaglio giurisdizionale sulle perquisizioni "negative"*, in *La riforma Cartabia*, cit., 222 ss.; PADUA, *Opposizione all'atto perquirente non seguito da sequestro*, in *Proc. pen. giust.*, 2022, 149 ss.