



OSSERVATORIO NUOVE TECNOLOGIE E DIRITTI FONDAMENTALI N. 5/2025

1. CONSERVAZIONE DEI DATI BIOMETRICI E GENETICI PER FINI INVESTIGATIVI. IL BILANCIAMENTO TRA ESIGENZE DI SICUREZZA INTERNA E TUTELA DEI DATI PERSONALI NELLA DIRETTIVA (UE) 2016/680 ALLA LUCE DELLA RECENTE GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA NELLA CAUSA C-57/23

1. *Considerazioni introduttive*

Con la sentenza in commento del 20 novembre 2025, la Corte di giustizia (Quinta Sezione) si è pronunciata sulla domanda di rinvio pregiudiziale, operato dal Nejvyšší správní soud (Corte suprema amministrativa di Praga) nel procedimento *JH c. Policejní prezidium* (Direzione della polizia della Repubblica ceca; [C-57/23](#), ECLI:EU:C:2025:905) riguardante la raccolta e la conservazione di dati biometrici e genetici relativi al ricorrente nell'ambito di un procedimento penale e alla loro conservazione da parte della polizia ceca. La domanda di pronuncia pregiudiziale concerneva l'interpretazione di alcune disposizioni della [direttiva \(UE\) 2016/680](#) relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

Il caso ha rappresentato un'occasione importante di chiarificazione della portata della direttiva 2016/680, uno strumento giuridico dell'Unione relativamente nuovo sul quale, al momento, non esiste una giurisprudenza risalente della Corte di giustizia (v. P. MILAZZO, *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, in L. CALIFANO e C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017). La giurisprudenza sul [Regolamento 2016/679](#) (regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in prosieguo: il «RGPD») o sull'atto che l'ha preceduto, vale a dire la [direttiva 95/46](#), fornisce certamente utili elementi di interpretazione per una serie di questioni sollevate dai giudici nazionali. Tuttavia, non è chiaro in che misura la normativa risultante dal RGPD sia effettivamente trasponibile per analogia allo specifico ambito di applicazione della direttiva 2016/680 (v. P. MILAZZO, *La proliferazione delle banche dati di polizia e la tutela europea dei dati personali: alcune prospettive ed alcuni limiti della Direttiva (EU) 2016/680*, in [EUWEB Legal Essays](#), 1/2022). Del resto, se i due regimi dovessero essere senz'altro identici, non sarebbe in tal caso evidente il motivo per cui il legislatore dell'Unione abbia ritenuto necessario adottare una complessa normativa specifica sotto forma della direttiva 2016/680 in quanto

lex specialis rispetto al RGPD (v. M. LEISER, B. CUSTERS, *The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680*, in *European Data Protection Law Review*, 2019) Si può quindi ritenere che la tutela delle persone fisiche in relazione al trattamento dei dati personali ai fini della prevenzione, dell'indagine o del perseguimento dei reati, debba essere, in qualche modo, distinta rispetto al regime generale di protezione dei dati. Il fattore comune delle tre questioni sollevate dal giudice ceco è il tentativo di individuare in che cosa esattamente debba consistere tale differenza.

In tale contesto, il giudice del rinvio, oltre a dubitare della compatibilità con il diritto dell'Unione e la giurisprudenza della Corte della normativa nazionale di recepimento della direttiva, ha anche richiamato la giurisprudenza della Corte europea dei diritti dell'uomo (in prosieguo: « Corte EDU »), in particolare su alcuni aspetti della normativa nazionale relativa all'acquisizione e alla conservazione dei dati personali ai fini di una futura identificazione, in particolare dei dati personali sensibili sotto forma di profilo del DNA.

2. Breve illustrazione dei fatti e del procedimento

La vicenda trae origine dal ricorso proposto da JH nei confronti della polizia della Repubblica ceca, con il quale, a seguito della propria condanna per i reati di violazione dei doveri nella gestione del patrimonio altrui e di abuso d'ufficio, egli ha chiesto l'accertamento dell'illegittimità delle operazioni di identificazione cui era stato sottoposto, nonché della raccolta e della conservazione dei campioni biologici e delle informazioni a lui riferibili. Il ricorrente ha altresì contestato il successivo trattamento e il mantenimento dei dati personali così ottenuti nell'ambito del procedimento penale instaurato nei suoi confronti, deducendo che tali attività costituissero un'ingerenza indebita nei diritti fondamentali garantiti dall'ordinamento dell'Unione (causa C-57/23, punto 21).

La polizia della Repubblica Ceca nel dicembre 2015 ha avviato un procedimento penale nei confronti del ricorrente per il reato di violazione dei doveri nell'amministrazione del patrimonio di terzi. Nonostante l'opposizione del ricorrente, le autorità hanno comunque rilevato le impronte dattiloscopiche, effettuato un tampone buccale da cui ha creato un profilo DNA, hanno scattato fotografie ed effettuato una descrizione del ricorrente, informazioni personali e "sensibili" inserite poi nelle pertinenti banche dati della polizia.

Il ricorso è stato accolto dalla Corte regionale di Praga, la quale ha ritenuto sproporzionate, rispetto alla finalità di prevenzione dei reati, le operazioni di identificazione compiute dalla polizia nei confronti di JH, anche in ragione della natura non grave del reato ascrittogli. Il giudice ha infatti rilevato che al ricorrente era stata concessa la sospensione condizionale della pena, che egli risultava incensurato e che la fattispecie contestata non presentava un disvalore tale da giustificare la raccolta e la conservazione dei dati personali ai fini della prevenzione della recidiva. Tale pronuncia è stata successivamente impugnata dalle autorità di polizia dinanzi al giudice *a quo*.

Il ragionamento del giudice del rinvio si è concentrato sulla verifica della compatibilità del regime giuridico delineato dall'articolo 65 della [legge n. 273/2008](#) sulla polizia della Repubblica ceca, in quanto normativa interna di attuazione, con la direttiva (UE) 2016/680.

Occorre anzitutto precisare che la normativa in esame era già stata sottoposta a un giudizio di legittimità costituzionale, conclusosi con il rigetto, da parte della Corte costituzionale ceca, della questione relativa all'articolo 65 con decisione del 22 marzo 2022 (punto 23). Cionondimeno, il giudice del rinvio ha reiterato il vaglio di compatibilità, questa

volta sul piano del diritto dell'Unione, sottoponendo alla Corte di giustizia tre questioni pregiudiziali concernenti la conformità di tale disposizione alla direttiva (UE) 2016/680.

In primo luogo, il giudice del rinvio ha rilevato l'assenza, nella normativa nazionale, di criteri idonei a differenziare il trattamento dei dati personali in funzione della gravità dei reati contestati, carenza che incide direttamente sul rispetto del principio di proporzionalità e rischia di condurre a una raccolta indiscriminata di dati biometrici e genetici. A sostegno di tale rilievo, è stata richiamata la consolidata giurisprudenza della Corte europea dei diritti dell'uomo (v. in particolare le sentenze *Trajkovski e Chipovski c. Macedonia del Nord*, 13 febbraio 2020, ricorsi nn. 53205/13 e 63320/13; *Gaughran c. Regno Unito*, 13 febbraio 2020, ricorso n. 45245/15; *Aycaguer c. Francia*, 22 giugno 2017, ricorso n. 8806/12; nonché *S. e Marper c. Regno Unito*, 4 dicembre 2008, ricorsi nn. 30562/04 e 30566/04), secondo cui il diritto al rispetto della vita privata, garantito dall'articolo 8 CEDU, impone che la raccolta e la conservazione dei dati genetici siano differenziate in base alla natura e alla gravità dei reati, al fine di evitare trattamenti sproporzionati e generalizzati. Orbene, l'articolo 65 della legge sulla polizia polacca non fornisce criteri che consentano di valutare la proporzionalità dell'ingerenza nel trattamento dei dati personali. L'unica verifica prevista dalla disposizione riguarda il fatto che la polizia, per procedere al trattamento dei dati sensibili dei sospettati, accerti che il reato commesso sia di natura dolosa. In tal senso, il giudice ha chiesto se una normativa nazionale che autorizzi la raccolta di dati genetici da parte della polizia nei confronti di tutte le persone imputate o sospettate di un reato doloso sia compatibile con il diritto dell'Unione, e in particolare con il principio di proporzionalità sancito dalla direttiva 2016/680 (punto 32). Ciò riguarda in particolare l'articolo 4, paragrafo 1, che sancisce il principio di minimizzazione dei dati, e l'articolo 6, che richiede agli Stati membri di prevedere nelle proprie normative distinzioni tra sospettati e condannati, tra vittime o potenziali vittime e tra testimoni in grado di fornire informazioni rilevanti ai fini dell'accertamento dei reati (punto 35).

La seconda questione riguarda la durata ragionevole della conservazione dei dati di identificazione da parte delle autorità di polizia. Né la direttiva 2016/680 né la normativa nazionale prevedono limiti temporali precisi. Dall'articolo 4, paragrafo 1, lettera e), della direttiva, nonché dai principi generali e dalla giurisprudenza della Corte di giustizia, risulta soltanto che i dati personali devono essere conservati per il tempo strettamente necessario al perseguimento delle finalità del trattamento. Tuttavia, il giudice nazionale deve confrontarsi con il problema di come applicare tale principio in contesti in cui lo scopo dichiarato è la prevenzione, la ricerca o l'accertamento di attività criminali, che per loro stessa natura hanno una dimensione prospettica e potenzialmente illimitata nel tempo (punto 36).

Quanto all'ultimo quesito sottoposto alla Corte, esso verte sulla validità delle garanzie a tutela dei dati personali sensibili quando queste non discendano da una disciplina legislativa espressa, bensì dall'interpretazione giurisprudenziale del diritto interno. In sostanza, il giudice del rinvio si è interrogato sulla possibilità che la giurisprudenza nazionale rientri nella nozione di «diritto dello Stato membro» ai sensi dell'articolo 8 della direttiva 2016/680.

3. Brevi premesse sul quadro normativo di riferimento: la Law Enforcement Directive

Prima di entrare nel merito delle questioni giuridiche affrontate dalla Corte, appare opportuno richiamare il quadro normativo nel quale si colloca la pronuncia in commento, al fine di coglierne appieno la portata sistematica e i profili di originalità.

La decisione della Corte interviene nell'ambito applicativo della direttiva (UE) 2016/680 (c.d. *Law Enforcement Directive* – LED), adottata come parte integrante del [EU data](#)

protection package, insieme al Regolamento generale sulla protezione dei dati personali, e destinata a disciplinare i trattamenti di dati personali effettuati dalle autorità competenti per finalità di prevenzione, accertamento e repressione dei reati (si rimanda a M. BOTTINO, *Approvato il nuovo regolamento generale per la protezione dei dati personali nell'UE*, in [Eurojus.it](#), 2016); v. anche, F. ROSSI DAL POZZO, *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, in *I Post di AISDUE*, I/2019). Sebbene ne condivida le basi giuridiche, rispettivamente l'articolo 8 della *Carta* dei diritti fondamentali dell'Unione europea, e l'articolo 16 TFUE, a differenza del RGPD, la direttiva *LED* si innesta nel peculiare ambito della cooperazione giudiziaria e di polizia in materia penale, cui il legislatore europeo ha riconosciuto una specificità tale da giustificare l'introduzione di un regime normativo autonomo (sugli articoli 7 e 8 della Carta, v. O. POLLICINO, M. BASSINI, *Commento all'art. 8*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *La Carta dei diritti fondamentali dell'Unione europea*, Milano, 2016, p. 133 ss.; G. MARTINICO, *Commento all'art. 7 CdfUE*, *ibidem*, p. 114; J. HERVEG, J.-M. VAN GYSEGHEM, *La protection des données à caractère personnel en droit européen*, in *Journal européen des droits de l'homme*, 2018, p. 33). Già la Dichiarazione n. 21 allegata al Trattato di Lisbona aveva, del resto, preso atto della particolarità del settore del *law enforcement*, chiarendo come, in tale contesto, la protezione dei dati personali possa legittimamente essere configurata in modo differenziato rispetto al modello generale, in considerazione della natura degli interessi pubblici perseguiti dalle autorità di polizia e giudiziarie (v. C. DI FRANCESCO MAESA, *Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)*, in [Eurojus.it](#), 2016). In questa prospettiva, la scelta dello strumento della direttiva risulta coerente con la natura altamente sensibile del settore, tradizionalmente riconducibile al nucleo essenziale della sovranità statale e fortemente inciso da valutazioni di politica criminale interna (per un *excursus* sulle tappe che hanno condotto all'odierno regime v. J. SAJFERT, T. QUINTEL, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*, in [Cole/Boehm GDPR Commentary](#), 2017). La direttiva *LED* si propone, quindi, di assicurare un livello elevato di protezione dei diritti fondamentali, riconoscendo al contempo agli Stati membri un margine di apprezzamento nell'attuazione delle regole europee.

Una delle differenze strutturali più significative rispetto al RGPD riguarda l'estensione dei diritti dell'interessato, in particolare del diritto di informazione e del diritto di accesso. L'operatività integrale di tali prerogative, se trasposta automaticamente nel contesto delle indagini penali, rischierebbe infatti di comprometterne l'efficacia, esponendo l'attività investigativa a condizionamenti incompatibili con le finalità di prevenzione e repressione dei reati. La direttiva, pertanto, introduce limitazioni funzionali giustificate da esigenze di sicurezza pubblica, costruendo un sistema orientato al bilanciamento tra tutela dei diritti fondamentali e interessi collettivi primari (v. E. GRILLO, *Sulla conservazione sistematica e generalizzata di dati genetici e biometrici per finalità di polizia*, in *NGCC*, 4/2024).

Sotto il profilo sistematico, ne deriva una bipartizione del diritto europeo della protezione dei dati in ambito giudiziario (si veda M. BREWCZYŃSKA, *A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation*, in E. KOSTA, R. LEENES & I. KAMARA (a cura di), *Research handbook on EU data protection law*, Cheltenham, 2022, pp. 91-114). Una rappresentazione concreta di tale bipartizione emerge con particolare evidenza nell'ambito dell'*investigative genetic genealogy*, ove le attività di trattamento si sviluppano lungo due direttrici parallele. Da un lato, si collocano i trattamenti effettuati da soggetti privati titolari di banche dati genealogiche, cui gli utenti

conferiscono volontariamente i propri profili genetici per finalità di natura personale, scientifica o commerciale; trattamenti che rientrano ordinariamente nell'ambito applicativo del RGPD. Dall'altro lato, si collocano le operazioni svolte dalle autorità di contrasto, che utilizzano tali banche dati quale strumento investigativo sussidiario per individuare indizi o soggetti sospetti, ambito nel quale trova applicazione la direttiva (UE) 2016/680, come del resto espressamente confermato dal Considerando 11, secondo cui il regolamento (UE) 2016/679 continua ad applicarsi ai trattamenti effettuati dalle autorità pubbliche per finalità diverse da quelle di prevenzione, accertamento e repressione dei reati (si veda, T. KURU, *Investigative genetic genealogy in Europe: Why the “manifestly made public by the data subject” legal basis should be avoided*, in *Computer Law & Security Review*, 56/2025). Proprio l'interazione tra questi due livelli normativi mostra in modo emblematico come il criterio dirimente ai fini dell'individuazione del regime applicabile non sia il soggetto che effettua il trattamento, bensì la finalità perseguita. Ne consegue che il medesimo dato genetico può transitare, nel corso del medesimo procedimento fattuale, dal perimetro del RGPD a quello della direttiva *LED*, in funzione dell'uso che ne viene fatto, accentuando così quella frammentazione sistemica che rende talvolta incerti i confini applicativi tra i due strumenti.

Nel caso sottoposto alla Corte, la questione verte sulla compatibilità della normativa ceca con la direttiva 2016/680 in relazione alla conservazione di dati genetici e biometrici del ricorrente, dunque su una categoria di informazioni che, per loro natura, sono idonee a incidere in modo particolarmente intenso sui diritti fondamentali dell'interessato. L'articolo 3 della direttiva definisce i dati biometrici come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici» (v. anche articolo 4, paragrafo 1, n. 14) RGPD). Tra questi potrebbero rientrare i dati personali che rivelano l'origine razziale o etnica. Tuttavia, non rientrano *tout court* nelle categorie particolari di dati personali, a meno che non «siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica» (considerando 51; si veda, G.M. RICCIO, G. SCORZA, E. BELLISSARIO (a cura di), *GDPR e Normativa Privacy. Commentario*, Wolters Kluwer, 2018). I dati genetici, invece, sono definiti come «dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione» (articolo 3, n. 12) direttiva *LED* e articolo 4, paragrafo 1, n. 13) RGPD), ricomprendendo sostanzialmente i dati biologici e i campioni biologici, a mente del considerando 35 RGPD, tra i «dati relativi alla salute», intesi come «i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute» (sulla riconducibilità delle informazioni tratte dal DNA dell'individuo alla categoria dei dati personali si veda, Gruppo di lavoro per la protezione dei dati – Art. 29 in occasione del parere 6/2000 sul problema del Genoma, approvato il 13 luglio 2000 ([5062/00/IT/Definitivo – WP 34](#))).

Nel modello del RGPD, il trattamento di tali categorie rientra nell'ambito di un divieto generale, salvo limitate eccezioni, e sempre nel rispetto dei principi di necessità, proporzionalità e minimizzazione dei dati (si veda in dettaglio F. MOLLO, *Il trattamento dei dati genetici tra libera circolazione e tutela della persona*, in [JusCivile.it](#), 2022). Nella direttiva *LED*, per contro, esso non è vietato in via assoluta, ma ammesso esclusivamente a condizioni rafforzate. L'articolo 10 stabilisce infatti che il trattamento di dati genetici e biometrici è

consentito solo “se strettamente necessario”, soggetto a garanzie adeguate per i diritti dell’interessato e autorizzato dal diritto dell’Unione o dello Stato membro, ovvero in ipotesi tassative ulteriori. Il requisito della “stretta necessità” assurge così a condizione qualificata di liceità del trattamento e implica un controllo particolarmente rigoroso sulla proporzionalità dell’ingerenza. Ne deriva un obbligo di minimizzazione “rafforzata”, che impone di verificare non solo la pertinenza dei dati raccolti, ma anche la durata della loro conservazione e l’inesistenza di misure alternative meno invasive idonee al conseguimento delle finalità perseguite (come previsto dagli articoli 13 e 14 della direttiva 2016/680). Incombe inoltre sul titolare del trattamento l’obbligo di prevedere meccanismi di verifica periodica della persistenza delle condizioni di liceità (considerando 26 direttiva 2016/680). È proprio su tale assetto normativo, caratterizzato da una protezione qualificata ma funzionalmente orientata, che si innesta l’interpretazione fornita dalla Corte nella sentenza in esame, destinata a incidere significativamente sul modo in cui gli Stati membri possono disciplinare la raccolta e la conservazione dei dati biometrici e genetici in ambito penale.

4. *La decisione della Corte: un’opera di bilanciamento di interessi più che di tutela di diritti*

Addentrando nelle maglie della sentenza, i giudici di Lussemburgo hanno affrontato preliminarmente il terzo quesito sollevato dalla Corte ceca, concernente la portata e il contenuto della nozione di «diritto dello Stato membro» (punto 42). La Corte ha esaminato il combinato disposto degli articoli 8 e 10 della direttiva 2016/680, rispettivamente dedicati alle condizioni di liceità del trattamento dei dati personali e al trattamento di categorie particolari di dati, comprendenti quelli genetici e biometrici. In particolare, l’articolo 8, paragrafo 1, stabilisce che, oltre al principio di necessità del trattamento, esso deve poggiare su un adeguato fondamento giuridico, sia a livello di diritto dell’Unione sia di diritto nazionale. A tal riguardo, è fondamentale che il diritto nazionale indichi almeno gli obiettivi perseguiti, la tipologia di dati trattati e le finalità del trattamento (punto 47). La Corte ha posto particolare attenzione ai dati genetici e biometrici, per i quali l’articolo 10 richiede l’esistenza di condizioni di liceità specifiche e più rigorose. Secondo la Corte, tale interpretazione si impone anche alla luce del considerando 37 della direttiva 2016/680, il quale prevede garanzie rafforzate per la tutela dei dati genetici e biometrici. Ciò è dovuto alla loro natura particolarmente sensibile: modalità di trattamento, finalità perseguite e soggetti coinvolti possono infatti comportare rischi concreti e significativi per l’esercizio dei diritti fondamentali dell’interessato (punto 48). Più precisamente, tali dati personali non dovrebbero essere trattati se non a condizione che il trattamento sia sottoposto a garanzie adeguate, stabilite per legge, a tutela dei diritti e delle libertà dell’interessato, e che sia autorizzato nei casi previsti dalla normativa dell’Unione o dello Stato membro (punto 49). Secondo la Corte, la nozione di «diritto dello Stato membro» riflette l’intento del legislatore dell’Unione di concretizzare, nell’ambito della direttiva, quanto previsto dall’articolo 52 della Carta dei diritti fondamentali dell’Unione europea: qualsiasi limitazione all’esercizio dei diritti fondamentali deve essere stabilita dalla legge. Tale interpretazione risulta ancor più coerente se letta alla luce dell’articolo 8, paragrafo 2, della Carta, che stabilisce che qualsiasi trattamento di dati personali non basato sul consenso deve fondarsi esclusivamente su un altro fondamento previsto dalla legge (punto 51).

Orbene, se queste sono le premesse normative da cui partire, la Corte si è premurata di richiamare, in una prospettiva orientata ai diritti fondamentali, la giurisprudenza della Corte europea dei diritti dell’uomo, a cui il giudice del rinvio ha frequentemente fatto

riferimento (sul tema si veda anche A. BONFANTI, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *Rivista di diritto dei media*, 3/2018, p. 8 e ss.). Nella fattispecie, la Corte ha evidenziato due orientamenti distinti e ben definiti adottati dal consesso di Strasburgo. Da un lato, non è sufficiente che una misura o un trattamento siano «previsti da una legge» (come disposto dall'articolo 8, paragrafo 2 della Carta dei diritti fondamentali) solo perché esiste una norma scritta che li autorizza in astratto. È necessario, invece, che tale legge abbia una qualità sufficiente a garantire effettivamente la protezione dei diritti fondamentali (v. Cour EDH, 18 giugno 1971, *De Wilde, Ooms et Versyp c. Belgio*, ricorsi nn. [2832/66](#), [2835/66](#) e [2899/66](#), punto 93). In altri termini, una legge non legittima un'ingerenza nei diritti fondamentali semplicemente perché esiste, ma solo se è idonea a garantire una tutela reale della persona. Dall'altro lato, una giurisprudenza adattiva della Corte europea dei diritti dell'uomo ha interpretato il termine “legge” anche come normativa in vigore così come interpretata dai giudici nazionali competenti (si veda in tal senso, Corte EDU, 23 gennaio 2025, *H. W. c. Francia*, [CE:ECHR:2025:0123JUD001380521](#)). La Corte ha individuato due principali direttrici di riflessione. In primo luogo, ha affermato che ogni trattamento di dati personali deve fondarsi su una base giuridica chiaramente identificabile nella normativa nazionale. Tuttavia, tale base non deve essere solo formale: la legge deve possedere requisiti sostanziali, prevedendo almeno gli obiettivi del trattamento, le categorie di dati personali interessati e le finalità perseguite (punto 56). In tal senso, l'articolo 8, paragrafo 2, della direttiva 2016/680 richiede che il diritto dello Stato membro sia chiaro, preciso e prevedibile, così da consentire ai destinatari di conoscere in anticipo le conseguenze del trattamento, in conformità con la giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo (considerando 33 della direttiva 2016/680).

Secondo la Corte EDU, infatti, ogni norma che costituisca la base giuridica di un trattamento deve essere accessibile, prevedibile e compatibile con i diritti fondamentali, definendo con sufficiente precisione l'estensione dei poteri attribuiti alle autorità competenti (v., *ex multis*, *Sunday Times c. Regno Unito*, 1979, punti 25 e 52; *Liberty e a. c. Regno Unito*, 2008, punti 62-63; *S. e Marper c. Regno Unito*, 2008, punto 95). Analogamente, la Corte di giustizia ha precisato che una normativa che comporti un'ingerenza nei diritti garantiti dagli articoli 7 e 8 della Carta deve includere garanzie adeguate contro abusi e accessi illeciti, mediante regole chiare e precise sulla portata e sull'applicazione della misura (v. sentenza della Corte del 8 aprile 2014, *Digital Rights Ireland c. Minister for Communications and Others*, [cause riunite C-293/12 e C-594/12](#), EU:C:2014:238, punto 54; sentenza della Corte del 6 ottobre 2015, *Schrems c. Data Protection Commissioner*, [causa C-362/14](#), EU:C:2015:650, punto 91).

In secondo luogo, la Corte ha riconosciuto un ruolo alla giurisprudenza nazionale nell'interpretazione dei criteri di liceità previsti dal diritto dello Stato membro, a condizione che tale giurisprudenza sia accessibile e sufficientemente prevedibile (punti 54 e 60).

Analizzando le ulteriori due questioni sollevate dal giudice del rinvio, la Corte ha fatto ampio richiamo alla propria giurisprudenza consolidata, con particolare attenzione alla sentenza del 26 gennaio 2023 nella causa [C-205/21](#) (*V.S. c. Ministerstvo na vatreshnite rabotie*) e alla pronuncia nella causa [C-118/22](#) del 30 gennaio 2024 (*NG c. Direktor na Glavna direktsia «Natsionalna politzia» pri Ministerstvo na vatreshnite raboti – Sofia*), entrambe relative alla raccolta sistematica di dati biometrici e genetici da parte della polizia bulgara (per un commento si veda E. CIRONE, *Analysis: “When is the systematic collection of genetic data for the fight against crime legitimate? (Ministerstvo na vatreshnite raboti and génétiques par la police, C-205/21)”*, in *EuLawLive*, 2023; A. MIGLIO, *Op-Ed: “The Court of Justice interprets Directive 2016/680 and limitations on storage*

of personal data in police records (Direktor na Glavna direktsia "Natsionalna politisia" pri MVR – Sofia, C-118/22)", in *EuLawLive*, 2024).

In merito al primo quesito, la Corte ha precisato che il trattamento di dati personali sensibili, ai sensi dell'articolo 10 della direttiva 2016/680, è lecito solo se rispetta il criterio della "stretta necessità", valutato con particolare rigore alla luce delle finalità perseguite (punti 77–83). Ha inoltre ribadito che tale requisito è strettamente connesso al principio di minimizzazione dei dati previsto dall'art. 4, par. 1, lett. c), della direttiva (punti 76 e 85).

Per quanto concerne l'art. 6 della direttiva, la Corte ha chiarito che l'obbligo di distinguere le categorie di interessati non è assoluto, ma deve essere applicato "se del caso e nella misura del possibile" (punto 72), in funzione delle finalità del trattamento. Applicando questo criterio, la Corte ha ritenuto che le categorie delle persone imputate e di quelle sospettate che, secondo il diritto ceco, «richiedono, nell'ambito di un procedimento preliminare accelerato, che siano stati raccolti sufficienti elementi che dimostrino che esse hanno commesso un reato», possano rientrare entrambe nella categoria di cui all'articolo 6, lettera a), qualora le finalità del trattamento non impongano una distinzione (punti 73-75).

Da tale interpretazione emerge che la Corte ha conferito alla distinzione tra categorie di interessati un carattere funzionale, non meramente formale, collegandone l'operatività alle finalità del trattamento e al grado di coinvolgimento dell'interessato nella commissione del reato. Ne consegue che lo status processuale da solo non è determinante, laddove entrambe le categorie presentino un livello di sospetto tale da giustificare un trattamento unitario dei dati personali. La distinzione prevista dall'articolo 6, quindi, non opera in maniera automatica, ma dipende dalla concreta incidenza del trattamento sui diritti fondamentali e dalla sua proporzionalità rispetto allo scopo perseguito.

Rispetto alla precedente pronuncia nella causa C-205/21, l'elemento di discontinuità è emerso nella diversa natura della normativa nazionale esaminata. Nella sentenza del 26 gennaio 2023, la Corte ha censurato una disciplina che imponeva in modo automatico e generalizzato la raccolta dei dati biometrici e genetici di qualsiasi persona formalmente accusata di un reato doloso perseguibile d'ufficio, senza prescrivere un obbligo concreto, a carico dell'autorità competente, di verificare in ciascun caso la stretta necessità del trattamento e l'assenza di misure meno invasive idonee a conseguire gli stessi obiettivi (causa C-205/21, punti 135–136). Al contrario, nel caso qui in esame, la normativa nazionale si è limitata a conferire una "facoltà" ai servizi di polizia di procedere al rilevamento dei dati biometrici e genetici, senza introdurre un automatismo generalizzato (punto 90), circostanza che ha indotto la Corte a valutare diversamente la conformità al diritto dell'Unione. Essa ha infatti precisato che una normativa attributiva di mera facoltà non comporta, di per sé, una violazione dell'art. 10 della direttiva 2016/680, purché il diritto nazionale, inclusa la giurisprudenza interna, definisca in modo adeguato le finalità specifiche del trattamento e vincoli l'azione amministrativa al rispetto effettivo dei criteri della stretta necessità e della minimizzazione dei dati (punti 90-92). In tal modo, la Corte ha spostato il baricentro dell'analisi dalla struttura astratta della norma al modo concreto in cui essa è stata applicata, valorizzando il ruolo del giudice nazionale quale garante del controllo sostanziale sulla proporzionalità del trattamento. In merito poi ai profili di incompatibilità tra diritto nazionale e diritto dell'Unione, la Corte ha ricordato che, in presenza di una normativa nazionale che attribuisce ai servizi di polizia la facoltà di raccogliere dati biometrici e genetici, spetta ai giudici nazionali verificare, caso per caso, se tale raccolta sia stata effettuata in conformità ai principi generali sul trattamento dei dati personali, enunciati all'articolo 4 della direttiva 2016/680, nonché ai requisiti specifici applicabili ai dati personali sensibili, previsti

dall'articolo 10 della medesima direttiva, come interpretati alla luce degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (punto 92). In tal senso, i giudici nazionali devono assicurarsi che la normativa interna non venga applicata in modo da compromettere la tutela effettiva dei diritti fondamentali degli interessati.

Proseguendo nella disamina della sentenza, con riferimento alla seconda questione pregiudiziale, la Corte ha confermato, come nella pronuncia nella causa C-118/22, che uno Stato membro non è tenuto a prevedere un limite temporale assoluto per la conservazione dei dati, purché siano fissati termini adeguati di verifica periodica della necessità di conservare i dati e che, in tale verifica, la stretta necessità sia valutata caso per caso (punti 101-105, 110). La novità che emerge nella sentenza in esame riguarda principalmente il collegamento con la normativa nazionale ceca (articoli 65 e 82 della legge sulla polizia), che stabilisce obblighi specifici per i servizi di polizia di riesaminare periodicamente, almeno ogni tre anni, la necessità di conservare i dati biometrici e genetici (punto 108). Tale verifica deve considerare le finalità del trattamento, la gravità del reato, il profilo dell'interessato e i suoi precedenti (punti 106-108). In tal modo, il legislatore nazionale ha introdotto un meccanismo concreto di controllo della necessità e della proporzionalità del trattamento, che consente di attuare il principio di stretta necessità previsto dall'art. 10 della direttiva 2016/680 e di rispettare il principio di minimizzazione dei dati di cui all'art. 4, par. 1, lett. c), della medesima direttiva.

Tale approccio differisce dalla causa C-118/22, nella quale la normativa bulgara non fissava alcun termine specifico di revisione dei dati conservati e la Corte ha sottolineato la necessità di garantire almeno un controllo periodico (causa C-118/22, punti 52, 45, 48 e 50), senza entrare nel dettaglio dei criteri di valutazione. La sentenza odierna evidenzia quindi come la previsione di un termine di verifica periodica, unitamente alla valutazione della necessità di mantenere i dati alla luce delle circostanze specifiche, rappresenti un elemento di conformità essenziale al quadro normativo dell'Unione, garantendo un bilanciamento tra le esigenze investigative e la protezione dei diritti fondamentali degli interessati.

5. *Alcune osservazioni conclusive*

Procedendo ad una valutazione complessiva della sentenza in esame, i giudici di Lussemburgo hanno chiarito che il diritto nazionale può consentire alle autorità di polizia di conservare dati biometrici e genetici anche in assenza di limiti temporali predeterminati, purché tale trattamento avvenga nel rispetto delle garanzie previste dal diritto dell'Unione per i dati sensibili. La sentenza ha confermato, infatti, che la conservazione dei dati è compatibile con il diritto dell'Unione anche quando non sia fissato un termine massimo, a condizione che siano previsti controlli periodici effettivi e una motivazione attuale della persistente necessità del trattamento. In altri termini, la Corte ha riconosciuto agli Stati membri un ampio margine di manovra, ma al contempo ha sottolineato che la conservazione dei dati è consentita solo se risulti realmente indispensabile in relazione alle finalità perseguite.

Di conseguenza, la decisione, destinata ad incidere concretamente sui modelli investigativi europei, ha rafforzato i poteri delle autorità di polizia, ma ha ribadito che l'uso di informazioni particolarmente invasive rimane sottoposto a vincoli stringenti. Tra libertà individuali ed esigenze di sicurezza, la Corte ha quindi delineato un equilibrio in cui agli Stati è riconosciuto un margine di azione, ma non una discrezionalità assoluta. Ne deriva che il limite al trattamento non è temporale, ma funzionale e motivazionale. Una conservazione automatica o meramente amministrativa è inammissibile, bensì è richiesta una valutazione individualizzata e documentata. Tale impostazione, ad un esame più attento, si colloca in

piena continuità con l'orientamento della giurisprudenza della Corte europea dei diritti dell'uomo, la quale ha costantemente ridimensionato il margine di apprezzamento riconosciuto agli Stati, esigendo che i regimi di conservazione dei dati personali siano sorretti da criteri di proporzionalità stringenti e muovano da un effettivo bilanciamento tra le esigenze di interesse pubblico e i diritti fondamentali dell'individuo. Il caso *S. e Marper c. Regno Unito* risulta emblematico nel delineare i requisiti cui deve conformarsi un regime di conservazione dei dati personali. In primo luogo, l'ingerenza deve essere "prevista dalla legge", intesa non in senso meramente formale, ma come fonte dotata di qualità sufficiente (qui si innesta il ragionamento della Corte di giustizia, in merito al ruolo integrativo della giurisprudenza nazionale; punto 54). In secondo luogo, la disciplina deve perseguire una finalità legittima, quale la tutela della sicurezza pubblica e la prevenzione dei reati. Da ultimo, essa deve soddisfare il requisito della "necessità" (in una società democratica), declinato in termini di proporzionalità, richiedendo l'introduzione di criteri oggettivi, soggettivi e temporali idonei a limitare la conservazione dei profili genetici in funzione della gravità del reato, dello status dell'interessato e della durata della misura. (sul tema si rimanda a O. M. TUAZON, B. CUSTERS, G-J. ZWENNE, *Genometric data privacy within the ECHR regime*, in [International Data Privacy Law](#), 1/2025).

Uno dei profili più "sensibili" esaminati dalla Corte ha riguardato la possibilità di raccogliere dati biometrici e genetici in modo indifferenziato nei confronti di chiunque sia perseguito o sospettato di un reato doloso. Sul punto, la Corte ha adottato un approccio pragmatico. Il diritto dell'Unione, segnatamente gli articoli 4, 6 e 10 della direttiva 2016/680, non ha vietato in astratto una normativa nazionale che consenta una raccolta indistinta di tali dati. Tuttavia, tale possibilità è stata subordinata a due condizioni fondamentali. In primo luogo, la finalità del trattamento deve essere tale da non richiedere una distinzione tra indagati, imputati e condannati. Quando la raccolta dei dati sia funzionale a obiettivi di identificazione o prevenzione dei reati, un trattamento uniforme può risultare giustificato. In secondo luogo, i titolari del trattamento sono comunque tenuti a rispettare i principi applicabili ai dati sensibili, tra cui necessità, proporzionalità, minimizzazione, sicurezza e controllo dell'accesso (v. E.J. KINDT, *Having yes, using no? About the new legal regime for biometric data*, in [Computer Law & Security Review](#), 3/2018).

Orbene, la pronuncia della Corte nel caso in esame ha rappresentato un'importante occasione di chiarificazione della portata applicativa della direttiva 2016/680, inserendosi nel più ampio processo di costituzionalizzazione della tutela dei dati personali nell'ordinamento dell'Unione (v. S. MONTALDO, *La Corte di giustizia dell'Unione europea e la cooperazione giudiziaria in materia penale: profili istituzionali e prospettive per la tutela giurisdizionale*, in [Diritto Penale Contemporaneo](#), 2025). La direttiva è stata adottata con l'obiettivo di assicurare un elevato livello di tutela dei diritti fondamentali degli individui, consentendo, allo stesso tempo, agli Stati di mantenere un margine di manovra nelle modalità di adeguamento al nuovo quadro giuridico. Come risulta dall'analisi della pronuncia della Corte, il valore aggiunto effettivo della direttiva dipende principalmente dal modo in cui essa viene recepita nei singoli ordinamenti nazionali e, soprattutto, dall'atteggiamento delle giurisdizioni nazionali e sovranazionali nel garantire un'interpretazione conforme e uniforme. Pur riproducendo alcuni dei principi sanciti dal RGPD, la direttiva non recepisce integralmente l'impianto garantistico del Regolamento. In particolare, taluni requisiti relativi alla liceità e correttezza del trattamento non sono richiesti alle autorità competenti, come ad esempio il consenso dell'interessato, che risulta incompatibile con la natura coercitiva delle attività di *law enforcement*. Il bilanciamento tra diritto individuale alla protezione dei dati e interesse pubblico

alla repressione dei reati viene quindi demandato, in larga misura, al legislatore nazionale, cui la direttiva lascia ampio spazio per introdurre limitazioni ai diritti dell'interessato al fine di garantire l'efficacia delle indagini e la salvaguardia della sicurezza nazionale. Sebbene tale riduzione appaia coerente con le esigenze investigative, essa genera tensioni tra protezione dei diritti fondamentali e poteri di controllo delle autorità. Il rischio, segnalato anche in dottrina, è quello di creare un'illusione di controllo da parte dell'interessato, laddove il consenso o l'opposizione al trattamento risultano, nei fatti, inattuabili (si veda sul tema O. LYNKEY, *Criminal justice profiling and EU data protection law: precarious protection from predictive policing*, in *International Journal of Law in Context*, 15/2019). La sentenza in esame si colloca dunque al centro di questa tensione sistemica, offrendo un'interpretazione della direttiva 2016/680 orientata a garantire, al contempo, l'efficacia dell'azione repressiva e la sostanza del diritto fondamentale alla protezione dei dati personali. Si conferma quindi il ruolo di vigilanza del giudice dell'Unione sull'evoluzione dell'integrazione europea, che esercita, dove necessario, un'influenza correttiva sul percorso intrapreso. Tale funzione, tuttavia, incontra un limite preciso nello stato di avanzamento definito dagli Stati membri e dal legislatore dell'Unione.

LUIGI PIGNA