

## Il quadro giuridico europeo sulla sorveglianza biometrica\*

*Giuseppina Pizzolante*

SOMMARIO: 1. Introduzione. L'applicazione delle tecnologie biometriche nell'Unione europea. – 2. L'uso della sorveglianza biometrica in materia di migrazione, asilo e controllo delle frontiere. – 3. Il difficile bilanciamento tra i diversi interessi e valori sottesi alle norme che disciplinano la sorveglianza biometrica. – 4. La sorveglianza biometrica nei settori della migrazione, dell'asilo e del controllo delle frontiere e i sistemi di intelligenza artificiale “ad alto rischio”. – 5. La sorveglianza biometrica e le pratiche di intelligenza artificiale vietate per rischio inaccettabile: i sistemi di categorizzazione biometrica e l'identificazione biometrica remota in tempo reale. – 6. Il quadro giuridico della biometria: un delicato equilibrio tra innovazione e protezione dei dati. – 7. La sorveglianza biometrica e la tutela dei diritti fondamentali. – 8. Considerazioni conclusive.

### *1. Introduzione. L'applicazione delle tecnologie biometriche nell'Unione europea*

L'impiego della tecnologia nei processi di migrazione, asilo e controllo delle frontiere sta diventando sempre più comune nei Paesi europei che cercano di definire nuovi modelli per il controllo dei confini e degli individui che li attraversano. I territori ai margini dell'Europa sono divenuti di conseguenza il banco di prova per sperimentare le più avanzate tecniche di sorveglianza.

Le applicazioni tecnologiche riguardano diversi ambiti, quali l'analisi dei dati, il processo decisionale e la sicurezza, con l'obiettivo dichiarato di rendere più efficiente la gestione delle migrazioni ma con l'intento più realistico di prevenire l'attraversamento delle frontiere da parte dei migranti considerati “indesiderabili”. Le nuove tecnologie al servizio delle frontiere, ad esempio, al fine di impedire l'ingresso irregolare nel territorio UE, si indirizzano, tra l'altro, verso la previsione dei percorsi che i migranti intraprenderanno. Così, l'Agenzia dell'Unione europea per l'asilo (EUAA) ha sviluppato il Sistema di allarme rapido e di preparazione (Early warning and Preparedness System - EPS) che viene impiegato per intercettare i flussi

---

\* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a *double-blind peer review*.

migratori verso l'UE, fornendo informazioni aggiornate per la pianificazione e l'azione. Il sistema predisposto, attraverso un algoritmo di apprendimento automatico, rielabora costantemente gli indicatori, nonché i dati estratti da *database* contenenti resoconti di *media* globali, come il progetto GDELT e l'Armed Conflict Location and Event Dataset<sup>1</sup>, anticipando gli eventi che potrebbero dare origine a spostamenti su larga scala e stimando il successivo numero di domande di asilo nell'UE.

Attraverso la sorveglianza biometrica, la mobilità umana è sia controllata, sia soggetta a valutazione del rischio, con la conseguenza che essa incide prepotentemente nella sfera privata se solo si pensi che le sofferenze patite dai migranti in mare sono certamente attribuibili all'inadeguatezza delle operazioni di salvataggio ma anche alle rotte migratorie illegali che molti di essi sono costretti ad intraprendere proprio per eludere "la tecnologia"<sup>2</sup>. La sorveglianza biometrica asseconda inoltre il desiderio degli Stati membri di controllare e gestire le operazioni di frontiera ben oltre i confini UE allo scopo di esternalizzare il più possibile anche la violenza.

Come è noto, la biometria è una tecnologia che consente di identificare un individuo in base alle sue caratteristiche fisiche, biologiche e comportamentali, mediante dati unici e immutabili che includono elementi quali DNA, impronte digitali, sagoma del viso, forma della mano, analisi dell'iride, riconoscimento vocale.

A partire dal 2012, le reti neurali e gli algoritmi di apprendimento automatico hanno compiuto enormi progressi nell'elaborazione delle informazioni, soprattutto nel riconoscimento delle immagini<sup>3</sup>, determinando una rapida crescita dell'uso della biometria nella sorveglianza. Essa, oltre a garantire semplicità nell'utilizzo, offre maggiore tracciabilità e sicurezza specie nel caso di autenticazione multimodale in cui convergono più tecnologie biometriche combinate tra loro. La mappa delle tecnologie biometriche applicate alla sicurezza può essere suddivisa in due ampie

---

<sup>1</sup> Si veda J. Napierala - J. Hilton - J.J. Forster - M. Carammia - J. Bijak, *Toward an Early Warning System for Monitoring Asylum-Related Migration Flows in Europe*, in *International Migration Review*, 2021, p. 33 ss.; C. Melachrinou - M. Carammia - T. Wilkin, *An Innovative Framework for Analysing Asylum-Related Migration*, in *Harnessing Data Innovation for Migration Policy: A Handbook for Practitioners*, in publications.iom.int, 2022, p. 54 ss.

<sup>2</sup> D. Ozkul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*, Refugee Studies Centre, University of Oxford, 23 January 2023; F. Delioglu, *Technology at the Borders: Surveillance, Control and Resistance in EU Migration Governance*, in *Balsillie Papers*, 2025.

<sup>3</sup> V.J. Schmidhuber, *Annotated History of Modern AI and Deep Learning*, in *Technical Report IDSLA*, people.idsia.ch, 29 dicembre 2022.

categorie: le applicazioni di autenticazione e le applicazioni di sorveglianza. La sorveglianza biometrica remota, sottocategoria di queste ultime, utilizza identificatori biometrici in uno spazio pubblico, in modo continuo e permanente, servendosi del confronto con i dati contenuti in una banca dati<sup>4</sup>.

Questo modello di sorveglianza, in cui gli individui sono monitorati attraverso *feed* audio e video elaborati algoritmicamente, desta particolari preoccupazioni poiché può facilmente trasformarsi in sorveglianza lesiva dei diritti umani<sup>5</sup>. Giova citare a questo riguardo la risoluzione del 6 ottobre 2021<sup>6</sup>, con cui il Parlamento europeo, pur riconoscendo i benefici di alcune applicazioni di intelligenza artificiale (d'ora innanzi anche IA) per le autorità di contrasto e giudiziarie, ha sottolineato i rischi per i diritti fondamentali e le democrazie, e dunque ha rimarcato il divieto di trattamento dei dati biometrici, comprese le immagini facciali, per finalità di applicazione della legge, tale da determinare sorveglianza di massa negli spazi accessibili al pubblico.

Appare certamente importante conoscere i diversi utilizzi della sorveglianza biometrica perché ciascuna specifica configurazione tecnologica tra dispositivi di rilevamento, dati biometrici e strumenti di elaborazione algoritmica consente applicazioni radicalmente diverse e può quindi avere differenti tipi di impatto sui diritti fondamentali degli individui<sup>7</sup>. La Commissione europea, seguendo un approccio “a piramide” confluito poi nel regolamento sull'intelligenza artificiale<sup>8</sup>, ha precisato che il pericolo

---

<sup>4</sup> Si veda, da ultimo, la definizione di “sistema di identificazione biometrica remota” contenuta nell'art. 3, n. 41 del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), d'ora innanzi anche regolamento sull'IA. Su questo regolamento si veda P. Voigt - N. Hullén, *The EU AI Act: Answers to frequently asked questions*, Berlin, 2024.

<sup>5</sup> Sul rispetto dei diritti umani fondamentali si veda per tutti U. Villani, *Istituzioni di diritto dell'Unione europea*, VII ed., Bari, 2024, p. 62 ss.

<sup>6</sup> Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI)), paragrafi 30-31.

<sup>7</sup> V., di recente, F. Seatzu, *Assessing the Council of Europe's AI Convention: Challenges and Prospects for Protecting Human Rights and Democracy in the Age of AI*, in *Studi sull'integrazione europea*, 1/2025, p. 9 ss.

<sup>8</sup> V. *infra* paragrafi 4 e 5. V. M. Ho-Dac, *The EU AI Act and the challenge of protecting fundamental rights*, in *Common Market Law Review*, 2025, p. 1299 ss., in cui si esamina il

per le libertà democratiche varia notevolmente a seconda dei sistemi e delle applicazioni in questione<sup>9</sup>: alcuni modelli comportano un elevato rischio di violare i diritti fondamentali e pertanto non dovrebbero mai essere consentiti come nel caso dei sistemi che distorcono il comportamento di un individuo con tecniche subliminali o sfruttando vulnerabilità specifiche al fine talvolta di contemplare l'attribuzione di un punteggio sociale; altri sistemi, ad esempio quelli utilizzati in ambito lavorativo per le assunzioni o, in ambito finanziario, per valutare l'affidabilità creditizia, realizzano applicazioni "ad alto rischio" che possono essere utilizzate in determinate circostanze e con garanzie predeterminate; ulteriori modelli infine, come il caso delle *chatbot*, prevedendo usi più elementari delle tecnologie, andrebbero sottoposti soltanto a requisiti minimi di trasparenza.

La valutazione giuridica dei differenti modelli non può quindi prescindere da una comprensione dettagliata del funzionamento e degli usi delle tecnologie sottostanti. Oggetto della nostra indagine saranno gli impieghi della sorveglianza biometrica a cui gli Stati membri UE si affidano nelle loro attività relative a migrazione, asilo e gestione delle frontiere.

D'altro canto, la digitalizzazione delle frontiere rientra nell'obiettivo dell'UE di rendere più efficiente e automatizzato il tracciamento delle persone alle frontiere interne ed esterne. In particolare, a partire dal 2007<sup>10</sup>, l'UE ha finanziato diversi progetti al fine di sperimentare meccanismi di controllo automatizzato, di identificazione e verifica biometrica, e di raccolta e analisi dei dati in materia migratoria. Nella stessa risoluzione del 6 ottobre 2021, testé citata<sup>11</sup>, il Parlamento europeo ha espresso profonda preoccupazione per i progetti di ricerca che diffondono l'IA alle frontiere

---

concetto di rischio introdotto da questo regolamento che combina il classico approccio volto alla sicurezza dei prodotti con una nuova versione di rischio che trae origine dalla tutela internazionale dei diritti umani.

<sup>9</sup> Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Promuovere un approccio europeo all'intelligenza artificiale, Bruxelles, 21 aprile 2021, COM(2021) 205 final, par. 4.

<sup>10</sup> Le "smart borders" presuppongono una gestione moderna, efficace ed efficiente delle frontiere esterne, volta a realizzare un equilibrio tra agevolazioni per i viaggiatori e sicurezza interna. In questo quadro rientra il sistema di ingressi/uscite (EES).

<sup>11</sup> Risoluzione del Parlamento europeo del 6 ottobre 2021, cit., paragrafi 30-31. Il programma di finanziamenti della Commissione Eu, Horizon 2020, ha promosso con 1,3 miliardi di euro numerosi progetti per il controllo dei confini come il progetto iBorderCtrl, avviato nel 2016 che, con un supporto di circa 5 milioni di euro, ha sviluppato tecnologie di riconoscimento facciale e *lie detection* fomentando aspre polemiche sul rispetto dei diritti fondamentali. Ciononostante, questa esperienza è stata trasfusa nel 2018 nel progetto TRESSPASS.

esterne, come il progetto iBorderCtrl, un “sistema intelligente di rilevamento delle menzogne” invitando la Commissione a interrompere il finanziamento della ricerca o la diffusione della biometria qualora essa finisse col realizzare una sorveglianza di massa indiscriminata nei luoghi pubblici<sup>12</sup>.

La generosità dei fondi europei per progetti di questo tipo ha corroborato, nei fatti, l’approccio securitario delle politiche migratorie sopra evidenziato. Così, oggi, gli Stati membri UE dispongono di *database* contenenti impronte digitali, immagini facciali e profili del DNA che possono essere consultati tramite gli algoritmi informatici; ma, se, per un verso, la politica di migrazione e asilo intende rafforzare le frontiere esterne, al contempo, mira a raggiungere una migliore cooperazione tra le autorità di contrasto al fine di favorire l’accesso allo spazio Schengen ai cittadini degli Stati terzi ritenuti in buona fede e quindi la libera circolazione all’interno dell’area Schengen. Emergono allora le esigenze di bilanciamento, dovendosi contemperare l’obiettivo della sicurezza con i diritti fondamentali<sup>13</sup>.

Il quadro giuridico di riferimento europeo della sorveglianza biometrica in relazione a migrazione e asilo è rappresentato dalla legislazione primaria in materia di diritti fondamentali, dunque, dalla Convenzione europea dei diritti dell’uomo (CEDU) e dalla Carta dei diritti fondamentali dell’UE<sup>14</sup>. Tra le norme “di base”, in materia di sorveglianza biometrica, va annoverato il regolamento sull’intelligenza artificiale. Ulteriore importante riferimento è il quadro giuridico relativo alla protezione dei dati ovvero il regolamento generale sulla protezione dei dati (d’ora innanzi anche RGPD)<sup>15</sup> e la direttiva 2016/680 del 27 aprile 2016

---

<sup>12</sup> Il sistema, attraverso un’analisi basata sull’IA di 38 micro-gesti, permette di tracciare il profilo dei viaggiatori sulla base di un’intervista computerizzata effettuata con la webcam del passeggero prima del viaggio.

<sup>13</sup> Per un inquadramento generale, v. per tutti B. Nascimbene, *Il mercato unico digitale è una nuova frontiera dell’integrazione europea?*, in *rivista.eurojus.it*, 3/2005, p. 105 ss.

<sup>14</sup> V., per tutti, U. Villani, *Dalla Dichiarazione universale alla Convenzione europea dei diritti dell’uomo*, II ed., Bari, 2015.

<sup>15</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

(d'ora innanzi anche direttiva polizia)<sup>16</sup>. Daremo conto di questa normativa di riferimento nel corso dell'analisi.

*2. L'uso della sorveglianza biometrica in materia di migrazione, asilo e controllo delle frontiere*

La sorveglianza biometrica, in materia di migrazione, asilo e controllo delle frontiere, viene adoperata per garantire il funzionamento dello Spazio di libertà, sicurezza e giustizia<sup>17</sup>. Alla protezione dei confini e al controllo dei flussi migratori, le istituzioni europee e gli Stati membri hanno dedicato un imponente sforzo organizzativo, culminato con l'istituzione di Frontex, l'Agenzia europea volta a supportare gli Stati membri dell'UE e i Paesi associati a Schengen nella gestione delle frontiere esterne<sup>18</sup>, e di eu-LISA, l'Agenzia europea che promuove lo sviluppo e la gestione di sistemi informatici (IT) su larga scala per la sicurezza delle frontiere<sup>19</sup>.

---

<sup>16</sup> Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

<sup>17</sup> Sul punto v. G. Caggiano, *L'evoluzione dello Spazio di libertà, sicurezza e giustizia nella prospettiva di un'Unione di diritto*, in *Studi sull'integrazione europea*, 2007, p. 335 ss.; M. Kontak, *Biometric Borders Envisaged by Frontex: Fundamental Rights in the Backseat*, in *European Papers*, 2024, p. 621 ss.

<sup>18</sup> L'Agenzia europea della guardia di frontiera e costiera (Frontex), istituita nel 2004, è disciplinata dal regolamento (UE) 2019/1896, del 13 novembre 2019, relativo alla guardia di frontiera e costiera europea che conferisce all'Agenzia un mandato rafforzato e competenze maggiori rispetto al previgente regolamento (UE) 2016/1624, assumendo ad esempio la forma del Corpo permanente della guardia di frontiera e costiera europea (il primo servizio in uniforme dell'UE).

<sup>19</sup> Essa è stata costituita dal regolamento (UE) n. 1077/2011 del Parlamento europeo e del Consiglio, del 25 ottobre 2011, che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, poi abrogato nel 2018 dal regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo all'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), che modifica il regolamento (CE) n. 1987/2006 e la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (UE) n. 1077/2011. Si veda I. Ingravallo, *L'evoluzione dell'Agenzia Europea della guardia di frontiera e costiera*, in V. Faggiani (dir.), *Desafíos y límites de la política migratoria en Europa y América. Perspectivas de derecho comparado*, Cizur Menor, 2022, p. 75 ss.; Id., *Gli strumenti di controllo sul rispetto dei diritti fondamentali nelle attività operative di Frontex*,

Le tecnologie biometriche sono utilizzate principalmente in situazioni in cui la polizia di frontiera adopera strumenti come rilevatori di presenza umana per individuare movimenti nascosti o battiti cardiaci all'interno dei veicoli che attraversano l'UE, oppure droni aerei dotati di riconoscimento delle immagini per sorvegliare le vaste frontiere marittime dell'UE<sup>20</sup>. La sorveglianza biometrica può altresì essere messa in campo per identificare minori non accompagnati o per ridurre i tempi di attraversamento dei confini da parte dei migranti. Questo primo impiego già evidenzia la duplicità degli obiettivi a cui si è accennato perché se la polizia di frontiera, in particolare Frontex, utilizza queste tecnologie per salvare vite in mare, essa è anche accusata di adoperare le stesse tecnologie per realizzare l'intercettazione in mare e respingere i migranti sulle coste libiche<sup>21</sup>.

Il ruolo di Frontex è altresì rafforzato dai sistemi informativi UE. Difatti un altro impiego significativo della biometria riguarda i vari sistemi informativi su larga scala ovvero le banche dati dell'Unione europea in materia di immigrazione che spesso fanno uso di riconoscimento facciale e che creano il problema della loro interoperabilità<sup>22</sup>. Esistono diversi sistemi di informazione o quadri di scambio di informazioni UE che applicano i dati biometrici.

Alcune delle banche dati funzionano oramai in modo consolidato<sup>23</sup>. Abbiamo la banca dati SIS (Sistema d'informazione Schengen), creata nel 1995 in seguito all'abolizione dei controlli alle frontiere interne, e che dunque risale alla Convenzione di applicazione dell'Accordo di Schengen

---

in *Quaderni AISDUE*, Convegno Forum IFA del 13 ottobre 2023, fascicolo speciale 4/2024, p. 1 ss.

<sup>20</sup> Si veda anche il rapporto finale di uno studio commissionato da Frontex per esaminare le capacità basate sull'intelligenza artificiale per le applicazioni di guardia di frontiera e costiera: Frontex, *Artificial Intelligence-based capabilities for the European Border and Coast Guard - Final Report*, [www.frontex.europa.eu](http://www.frontex.europa.eu), 31 March 2021.

<sup>21</sup> Si vedano altresì gli accordi conclusi tra Frontex e Windward al fine di studiare i "rischi" nei mari dell'Unione europea, investigare i movimenti delle imbarcazioni e trasferire le sospette attività in una "mappa delle minacce" da aggiornare costantemente con l'ausilio di un *software* dotato di funzionalità di auto-apprendimento. Cfr. M. Monroy, *Artificial intelligence: Frontex improves its maritime surveillance*, in [digit.site36.net](http://digit.site36.net), 15 January 2021.

<sup>22</sup> V., per tutti, G. Caggiano, *L'interoperabilità fra le banche-dati dell'Unione sui cittadini degli Stati terzi*, in *Diritto, Immigrazione e Cittadinanza*, 2020, p. 170 ss.; N. Vavoula, *Algorithmic Accountability Through the "Human over the Loop" in Interoperable and EU AI-reliant Large-scale IT Systems for Migration and Security*, in *European Papers*, 2024, p. 1228 ss.

<sup>23</sup> V., per tutti, S. Marinai, *Il rafforzamento del controllo digitale nel nuovo Patto sulla migrazione e l'asilo*, in *I Post di AISDUE*, II, 2020, p. 119 ss., nonché il sito [www.consilium.europa.eu/it/infographics/eu-wide-it-systems-for-security-and-migration/](http://www.consilium.europa.eu/it/infographics/eu-wide-it-systems-for-security-and-migration/).

del 19 giugno 1990. Il SIS è stato ampliato nel tempo per rispondere a nuove esigenze di sicurezza e cooperazione tra i Paesi membri dello spazio Schengen. Inizialmente, nel 1995, il SIS era incentrato sulla condivisione di informazioni per i controlli alle frontiere interne dello spazio Schengen. Successivamente, nel 2013, è stato introdotto il SIS di seconda generazione (SIS II) che ha ampliato le funzionalità del sistema, includendo la possibilità di inserire dati biometrici come impronte digitali; al fine di migliorare la sicurezza e i controlli di frontiera, esso è stato rafforzato nel 2023 per comprendere nuove tipologie di dati biometrici, come impronte palmari e registri DNA<sup>24</sup>. Il sistema ha continuato ad evolversi attraverso aggiornamenti e miglioramenti per ottenere una maggiore efficacia nella identificazione di persone e oggetti.

Un'impostazione sostanzialmente analoga si registra con riguardo al *database* europeo di dattiloscopia per l'asilo (Eurodac) che funziona come un sistema automatico di identificazione delle impronte digitali. Eurodac ha subito un'estensione del suo ambito di applicazione poiché inizialmente era collegato al sistema Dublino trattandosi di una banca dati funzionale col meccanismo volto ad individuare lo Stato membro competente a pronunciarsi sulla domanda di protezione internazionale e ad impedire a un migrante di presentare domanda di asilo in un paese diverso da quello di raccolta delle sue impronte digitali. Invero il meccanismo ha finito per limitare la mobilità dei migranti costretti spesso ad utilizzare metodi illegali per cercare asilo. Il regolamento (UE) 2024/1358, nell'ambito del nuovo

---

<sup>24</sup> Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare; regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006; regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione.

Ai sensi della decisione di esecuzione (UE) 2023/201 della Commissione del 30 gennaio 2023 che fissa la data di entrata in funzione del sistema d'informazione Schengen ai sensi del regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio e del regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, le operazioni del SIS "rafforzato" sono iniziate il 7 marzo 2023. I regolamenti (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862 sono dunque pienamente applicabili.

Patto sulla migrazione e l'asilo<sup>25</sup>, ha previsto che vengano inseriti, non solo i dati di coloro che chiedono protezione internazionale, ma anche i dati necessari al contrasto dell'immigrazione irregolare, e che vengano raccolte, non solo impronte digitali, ma anche immagini facciali. Difatti, a partire dal 2026, Eurodac tratterà i dati biometrici di tutte le persone migranti e richiedenti asilo di età superiore ai 6 anni<sup>26</sup>.

Un altro importante impiego della sorveglianza biometrica è volto al rilascio e alla gestione digitale dei visti ed è realizzato attraverso la banca dati VIS<sup>27</sup> (Sistema informativo visti) che pure ha subito nel corso del tempo un ampliamento del suo ambito di applicazione. Inizialmente, infatti, essa conteneva informazioni concernenti i visti di breve durata; solo successivamente ha inglobato i dati concernenti i visti di lunga durata che tuttavia continuano ad essere disciplinati a livello nazionale. Inoltre, mentre in origine era previsto solo l'inserimento dei dati dattiloscopici del richiedente il visto, è stata poi introdotta l'immagine del volto.

Va altresì segnalata la banca dati che gestisce il sistema di informazioni in entrata e in uscita, nota come Sistema di ingressi/uscite (EES)<sup>28</sup>. EES crea un apparato centralizzato di ingresso/uscita per i cittadini extra UE che

---

<sup>25</sup> Regolamento (UE) 2024/1358 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che istituisce l'«Eurodac» per il confronto dei dati biometrici ai fini dell'applicazione efficace dei regolamenti (UE) 2024/1351 e (UE) 2024/1350 o del Parlamento europeo e del Consiglio e della direttiva 2001/55/CE del Consiglio e ai fini dell'identificazione dei cittadini di paesi terzi e apolidi il cui soggiorno è irregolare, e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, che modifica i regolamenti (UE) 2018/1240 e (UE) 2019/818 del Parlamento europeo e del Consiglio e che abroga il regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio. Sul nuovo Patto, v. G. Morgese (a cura di), *Il futuro del diritto e della politica migratoria europea: il Nuovo Patto e oltre*, *Rivista Quaderni AISDUE*, n. 4/2024.

<sup>26</sup> Cfr. E. Celoria - V. Ferraris, *Eurodac: dalla gestione delle domande di protezione internazionale al controllo della mobilità*, in G. Morgese (a cura di), *op. cit.*

<sup>27</sup> Il sistema VIS è stato istituito dalla decisione 2004/512/CE del Consiglio, dell'8 giugno 2004. Si veda anche il regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata.

<sup>28</sup> Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011; regolamento (UE) 2017/2225 che modifica il codice frontiere Schengen per quanto riguarda l'uso del sistema di ingressi/uscite.

attraversano le frontiere esterne, sia per soggiorni di breve durata (fino a 90 giorni), sia per ingressi multipli (nell'arco di un periodo di 180 giorni).

Il nuovo sistema è entrato in funzione il 12 ottobre 2025 sebbene i Paesi UE che lo applicano attueranno gradualmente il meccanismo alle loro frontiere esterne. Dunque la raccolta dei dati sarà introdotta progressivamente anche ai valichi di frontiera, realizzando la piena esecuzione entro il 10 aprile 2026. La banca dati tratta i dati biometrici e i dati anagrafici di cittadini di Paesi terzi che attraversano le frontiere esterne dell'area Schengen, registrando e conservando data, ora, luogo d'ingresso e di uscita; calcolando automaticamente la durata del soggiorno autorizzato e generando *alert* destinati agli Stati membri allo scadere del soggiorno. Va segnalato che il personale autorizzato di Frontex, coinvolta nello sviluppo del meccanismo e dei suoi aspetti biometrici, avrà accesso ai dati EES.

La banca dati ETIAS (European Travel Information and Authorization System)<sup>29</sup>, adottata nel 2018, è invece un sistema di informazione e autorizzazione ai viaggi che farà parte dell'architettura di interoperabilità poiché le pertinenti domande ETIAS saranno verificate rispetto ai dati già presenti in sistemi come SIS, EES, VIS, Eurodac, nonché rispetto ai dati contenuti in Europol e nelle banche dati Interpol. Si tratta di un meccanismo elettronico di autorizzazione al viaggio rivolto a cittadini di Paesi terzi esenti da visto che desiderano accedere allo spazio Schengen e che entrerà in funzione nell'ultimo trimestre del 2026. Non si tratta di un visto bensì di un'autorizzazione preventiva che, prima dell'arrivo del viaggiatore, gestisce i rischi di sicurezza, migrazione irregolare o epidemie.

---

<sup>29</sup> Regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226; regolamento (UE) 2018/1241 del Parlamento europeo e del Consiglio, del 12 settembre 2018, recante modifica del regolamento (UE) 2016/794 ai fini dell'istituzione di un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS).

I regolamenti (UE) 2021/1134 del Parlamento europeo e del Consiglio del 7 luglio 2021 che modifica i regolamenti (CE) n. 767/2008, (CE) n. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 e (EU) 2019/1896 del Parlamento europeo e del Consiglio e che abroga le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, ai fini della riforma del sistema di informazione visti e 2021/1152 del Parlamento europeo e del Consiglio del 7 luglio 2021 che modifica i regolamenti (CE) n. 767/2008, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861 e (UE) 2019/817 per quanto riguarda la definizione delle condizioni di accesso agli altri sistemi di informazione dell'UE ai fini del sistema europeo di informazione e autorizzazione ai viaggi, garantiscono l'interoperabilità delle banche dati con l'ETIAS.

Il sistema è potenzialmente in grado di introdurre elementi a carattere discriminatorio laddove a tale gestione contribuisca la provenienza dell'individuo o l'origine del gruppo<sup>30</sup>. Qualora dal confronto tra dati si attivi un *alert*, l'art. 22 del regolamento ETIAS disciplina il trattamento manuale da parte dell'unità centrale ETIAS.

Va segnalata, in questo contesto, anche la proposta della Commissione europea per l'applicazione di viaggio digitale dell'UE (EU Digital Travel Application) che mira a digitalizzare i documenti di viaggio e le carte d'identità, semplificando al contempo l'uso delle credenziali di viaggio digitali per l'attraversamento delle frontiere Schengen<sup>31</sup>. La proposta, che va senz'altro apprezzata, mostra tuttavia la necessità di una esplicita interoperabilità con gli attuali quadri normativi dell'UE in materia di identità digitale. In particolare, il testo non è chiaro in merito all'obbligo per gli Stati membri di istituire un'infrastruttura nazionale per la creazione di credenziali di viaggio digitali collegate ai documenti di viaggio e alle carte d'identità. Allo stesso modo, andrebbe definito se la funzione relativa alla *governance* dei dati debba essere affidata ad eu-LISA a cui comunque viene attribuito un ruolo che supera le finalità originarie relative alle attività di polizia e giudiziarie per cui tale agenzia è stata istituita (considerando 13-18 della proposta di regolamento per l'applicazione di viaggio digitale dell'UE). Questo nuovo ruolo richiede una maggiore attenzione in materia di protezione dei dati personali.

Esistono altrettante ambiguità riguardo all'uso delle credenziali di viaggio digitali per l'attraversamento delle frontiere dovendosi esplicitare se, durante tale attraversamento, le credenziali digitali debbano sempre essere presentate per il mezzo del *router* del viaggiatore, che, in forza del considerando 9, ha il compito di inviare i dati di viaggio trasmessi dal viaggiatore alle autorità di frontiera per la verifica di frontiera anticipata e la pre-accettazione.

---

<sup>30</sup> V. *infra* par. 3.

<sup>31</sup> Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un'applicazione per la trasmissione elettronica dei dati di viaggio ("applicazione di viaggio digitale dell'UE") e che modifica i regolamenti (UE) 2016/399 e (UE) 2018/1726 del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2252/2004 del Consiglio per quanto riguarda l'uso delle credenziali di viaggio digitali, Strasburgo, 8 ottobre 2024, COM(2024) 670 final.

Va segnalato infine l'ECRIS (European Criminal Records Information System)<sup>32</sup>, il sistema informativo europeo che permette lo scambio di informazioni tra gli Stati membri UE sui precedenti penali a carico di cittadini di Paesi terzi. Questo sistema interconnette telematicamente i casellari giudiziari nazionali, facilitando lo scambio di dati in un formato standard. In sostanza, ECRIS rende più efficace l'informazione reciproca sulle condanne penali migliorando la cooperazione giudiziaria. Si tratta di informazioni di cittadini di Stati terzi che, anche in questo caso, vengono adoperate, sia in funzione di prevenzione dell'immigrazione irregolare, sia per svolgere attività di contrasto all'immigrazione.

*3. Il difficile bilanciamento tra i diversi interessi e valori sottesi alle norme che disciplinano la sorveglianza biometrica*

Per quanto riguarda il quadro giuridico di riferimento, oltre alle fonti istitutive dei sistemi informativi di volta in volta in rilievo, esso va ricostruito muovendo dalle esigenze di rispettare la vita privata e familiare nonché la protezione dei dati di carattere personale che la raccolta di questi dati pone. Difatti, inizialmente ciascuna delle banche dati istituite aveva lo scopo di perseguire obiettivi specifici ma negli ultimi anni le istituzioni europee, come pure si è accennato, intendono raggiungere l'interoperabilità tra sistemi informativi. Essa consente alle banche dati di dialogare tra loro permettendo alle diverse autorità – consolari, di contrasto o di frontiera – di avere contestuale accesso ai dati evidentemente di individui extra UE<sup>33</sup>.

---

<sup>32</sup> ECRIS è stato disposto dalla decisione 2009/316/GAI del Consiglio, del 6 aprile 2009, che istituisce il sistema europeo di informazione sui casellari giudiziari (ECRIS) in applicazione dell'articolo 11 della decisione quadro 2009/315/GAI. La decisione, tuttavia, è ancora applicabile solo in Irlanda e Danimarca, poiché, a partire dal 28 giugno 2022, essa è stata sostituita dalla direttiva 2019/884 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziari (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio.

<sup>33</sup> Nel maggio 2019, il Consiglio UE ha adottato due regolamenti per stabilire un quadro di interoperabilità tra i sistemi d'informazione, al fine di migliorare la gestione delle frontiere, della sicurezza e della migrazione. Le nuove norme hanno predisposto un portale al livello europeo per favorire ricerche simultanee attraverso più sistemi di informazione; un servizio comune di confronto finalizzato a controlli incrociati sui dati biometrici; un

Laddove la citata interoperabilità fosse pienamente realizzata, sarebbe fortemente favorita l'attività di contrasto alla criminalità ma allo stesso tempo verrebbe leso uno dei principi fondamentali in materia di protezione dei dati in forza del quale deve essere assicurata la legittima finalità in materia di trattamento ovvero i dati devono essere raccolti per una finalità specifica, legittima, esplicita. In particolare, in conformità dell'art. 5, par. 1, lett. b), RGPD, i dati personali sono «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità»<sup>34</sup>. Alla stessa stregua dispone anche l'art. 5, lett. b), della Convenzione n. 108 del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, secondo cui i dati a carattere personale oggetto di elaborazione automatica devono essere «registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini».

Il riconoscimento facciale, che impiega appunto dati biometrici, è strettamente legato all'identità di una persona e può avere un impatto significativo su vari diritti e libertà garantiti dalla Carta dei diritti fondamentali dell'UE<sup>35</sup>. Questi diritti includono, non solo la tutela della vita privata e familiare e la protezione dei dati, applicandosi gli stessi principi generali di trasparenza, correttezza, finalità, *data minimization*, necessità e

---

archivio comune volto a conservare i dati identificativi di cittadini di Paesi terzi (CIR, che, in conformità degli articoli 17-18 regolamento 2019/818, crea un fascicolo individuale contenente dati sia personali sia biometrici per ciascuna persona registrata nell'EES, nel VIS, nell'ETIAS, nell'Eurodac e nell'ECRIS); un rilevatore di identità multiple per allertare le autorità in caso di frode di identità. Questa nuova architettura di interoperabilità che fornisce dunque un'interfaccia unica per le ricerche e un servizio di confronto biometrico per facilitare l'identificazione, è in fase di graduale adozione (tra la metà del 2024 e la fine del 2026). Cfr. regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio; regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816.

<sup>34</sup> Una normativa che preveda una conservazione dei dati personali deve sempre rispondere dunque a criteri oggettivi che pongano un rapporto tra i dati personali da conservare e l'obiettivo perseguito. In tal senso, Corte giust., parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, punto 191 e giurisprudenza citata, nonché Corte giust., 3 ottobre 2019, C-70/18, *A e a.*, punto 63. V. *infra* par. 6.

<sup>35</sup> V. *infra* par. 7.

proporzionalità, ma anche la dignità umana, la libertà di movimento e la libertà di riunione, visto che gli individui potrebbero essere scoraggiati dal partecipare a manifestazioni pubbliche o dall'esprimere le proprie idee.

L'uso della sorveglianza biometrica nel settore delle migrazioni solleva quindi importanti questioni relative alla protezione dei diritti individuali. Invero i dati raccolti sono molto utili in funzione dell'attività di contrasto potendosi, ad esempio, prevenire false identità, ma risulta indispensabile una verifica sui modelli in base ai quali i *software* sono stati creati, sulle informazioni immesse e sulle immagini impiegate. Secondo una serie di studi emerge che la gran parte di questi *software* ha adoperato immagini di individui di pelle bianca e prevalentemente di sesso maschile; dunque, potrebbero delinearsi una serie di casi di falsi positivi che probabilmente creerebbero effetti discriminatori nei confronti di alcuni gruppi di etnie<sup>36</sup>.

Va altresì evidenziato che se le autorità di contrasto necessitano di strumenti avanzati per identificare rapidamente gli autori di crimini gravi e atti terroristici, l'utilizzo di tali strumenti deve essere conforme al quadro giuridico vigente e rispettare i principi di necessità e proporzionalità, alla luce dell'art. 52, par. 1, della Carta dei diritti fondamentali dell'UE. Inoltre, pur dovendosi riconoscere un importante valore aggiunto alle moderne tecnologie nel supportare le indagini, è importante non considerarle una soluzione miracolosa, ma piuttosto parte di un approccio più ampio e bilanciato<sup>37</sup>.

L'European Data Protection Board (EDPB) e il Garante europeo della protezione dei dati (GEPD) hanno circoscritto alcune applicazioni

---

<sup>36</sup> Così G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, p. 218 ss.

Il riconoscimento facciale è una tecnologia biometrica che utilizza algoritmi per riconoscere automaticamente gli individui attraverso le immagini dei loro volti. Il regolamento considera due tipi di sistemi di riconoscimento facciale: i sistemi di categorizzazione che non mirano a identificare la persona, ma a classificarla in categorie in base a caratteristiche come età, etnia o genere, estraendo dati biometrici dall'immagine del volto e i sistemi di identificazione biometrica che si basano sulla comparazione tra il modello biometrico costruito dall'algoritmo e i volti presenti in una banca dati, per identificare la persona. Questo processo avviene a distanza, senza contatto fisico, e può essere effettuato in tempo reale o successivamente su immagini registrate o reperite *online*.

<sup>37</sup> Si vedano anche le linee guida EDPB 05/2022, adottate il 26 aprile 2023, sull'uso della tecnologia di riconoscimento facciale nell'ambito delle attività di contrasto, che forniscono indicazioni ai legislatori europeo e nazionali, nonché alle autorità preposte all'applicazione della legge, sull'implementazione e sull'utilizzo dei sistemi di tecnologia di riconoscimento facciale.

delle tecnologie di riconoscimento facciale che presentano rischi inaccettabili per la società e per gli individui richiedendo per esse un divieto generale<sup>38</sup>. Tra queste, l'identificazione biometrica remota in spazi pubblici è considerata una forma di sorveglianza di massa non ammessa in una società democratica. Inoltre, l'EDPB ritiene che i sistemi di riconoscimento facciale basati sull'IA che classificano le persone in gruppi in base a caratteristiche come l'etnia, il genere o l'orientamento sessuale siano incompatibili con la Carta dei diritti fondamentali dell'UE. L'EDPB si oppone anche all'uso del riconoscimento facciale per dedurre le emozioni degli individui, considerandolo particolarmente indesiderabile, salvo talune eccezioni debitamente giustificate. Infine, l'EDPB ritiene che la creazione di banche dati tramite la raccolta indiscriminata di dati personali *online* non sia conforme al citato requisito di stretta necessità previsto dal diritto dell'Unione.

*4. La sorveglianza biometrica nei settori della migrazione, dell'asilo e del controllo delle frontiere e i sistemi di intelligenza artificiale "ad alto rischio"*

Il regolamento sull'intelligenza artificiale offre una analisi approfondita della biometria, definendo, per la prima volta in ambito UE, concetti quali la categorizzazione biometrica e riconoscendo nei suoi considerando i rischi per la tutela della vita privata e familiare, la non discriminazione e la dignità umana sollevati dalla biometria (in particolare, considerando 48). Come avremo modo di illustrare meglio, la materia "migrazione, asilo e gestione del controllo delle frontiere" si pone, nel regolamento, a cavallo tra art. 5, dedicato, seguendo un approccio basato sulla piramide del rischio, alle pratiche di IA vietate "per rischio inaccettabile", e art. 6, concernente i sistemi di IA "ad alto rischio"<sup>39</sup>.

---

<sup>38</sup> Parere congiunto EDPB-EDPS, del 17 giugno 2021, 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale). Nelle linee guida 05/2022, l'EDPB ha ribadito la richiesta di vietare l'uso della tecnologia di riconoscimento facciale in alcuni casi.

<sup>39</sup> Sia il regolamento sull'intelligenza artificiale sia il regolamento generale sulla protezione dei dati sono basati sul rischio. Tuttavia, le nozioni di "alto rischio" nel regolamento generale sulla protezione dei dati, che determina *ex art.* 35, par. 1, l'obbligo di condurre una valutazione dell'impatto del trattamento previsto sulla protezione dei dati personali, e nel regolamento sull'intelligenza artificiale, al fine di determinare, *ex art.* 6, la classificazione di un sistema di IA, non sono gli stessi. Sebbene infatti la classificazione "ad

Nel regolamento sull'intelligenza artificiale viene prevista espressamente la possibilità di utilizzare i meccanismi di IA anche in materia di immigrazione. Dunque, va valutato positivamente il considerando 60 in cui si dà atto della circostanza che gli individui che possono essere interessati da *software* che applicano tecnologie di questo tipo sono migranti spesso in una posizione particolarmente vulnerabile e il cui futuro dipende dalle scelte compiute dalle autorità pubbliche competenti, ritenendosi necessarie per essi maggiori verifiche e cautele nel trattamento dei dati.

La natura non discriminatoria e la trasparenza dei sistemi di IA sono finalizzati, tra l'altro, a garantire il rispetto dei diritti fondamentali delle persone migranti, specialmente i diritti alla libera circolazione, alla non discriminazione, alla tutela della vita privata e dei dati personali, alla protezione internazionale e alla buona amministrazione. Di conseguenza, vengono considerati "ad alto rischio" i sistemi di IA, richiamati all'art. 6, par. 2 e contenuti nell'allegato III del regolamento, ovvero i sistemi riguardanti i settori "migrazione, asilo e gestione del controllo delle frontiere", nella misura in cui il pertinente diritto dell'Unione o nazionale ne permetta l'uso (allegato III, par. 7 del regolamento sull'intelligenza artificiale). Si tratta dei sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti o dalle istituzioni, organi e organismi dell'Unione, come poligrafi o strumenti analoghi; a valutare un rischio (tra cui, nei settori della sicurezza, della migrazione irregolare o della salute) causato da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro; a coadiuvare le autorità pubbliche competenti rispetto all'esame delle domande di asilo, di visto o di permesso di soggiorno, nonché ai relativi reclami con particolare riguardo all'affidabilità degli elementi probatori; ad individuare, riconoscere o identificare persone fisiche, nel contesto della migrazione, dell'asilo o della gestione del controllo delle frontiere, con l'eccezione della verifica dei documenti di viaggio.

Il regolamento sull'IA ha cura di precisare che i sistemi di IA nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere non devono ledere in alcun modo il principio di non respingimento, garantendo allo stesso tempo vie legali di ingresso, sicure ed

---

alto rischio" di un sistema in base al regolamento sull'intelligenza artificiale debba essere presa in considerazione da parte del titolare del trattamento ai fini della determinazione dell'alto rischio in materia dati personali, si tratta di modelli normativi diversi di valutazione del rischio che non devono essere confusi. Cfr. R. Gellert, *The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?*, in *Journal of Ethics and Legal Technologies*, 3/2021, p. 14 ss.

efficaci, nel territorio dell'Unione, nonché il diritto alla protezione internazionale.

I sistemi ad alto rischio che includono, dunque, i sistemi di informazione biometrica utilizzati in materia di migrazione, asilo e controllo delle frontiere, devono soddisfare i requisiti stabiliti prevedendosi alcune esenzioni o deroghe speciali. Il regolamento crea una piramide del rischio imponendo un sistema graduale di restrizioni e obblighi ai fornitori e agli utenti. Prima di immettere un sistema di IA ad alto rischio sul mercato, i fornitori dovranno sottoporlo a una valutazione di conformità come qualità dei dati (art. 10), documentazione e tracciabilità (articoli 11 e 12), trasparenza (art. 13), sorveglianza umana (art. 14), accuratezza, robustezza e cibernsicurezza (art. 15).

Gli stessi sistemi, utilizzati da autorità pubbliche, vanno registrati in una banca dati pubblica dell'UE (art. 49 del regolamento sull'IA). Tuttavia, l'art. 49, par. 4, del regolamento sull'IA, per il settore della migrazione e della gestione delle frontiere, dispone che la registrazione debba avvenire in una sezione non pubblica della banca dati dell'UE che sarà accessibile solo alle autorità di controllo competenti, impedendosi nella sostanza un monitoraggio adeguato sull'impatto di questi sistemi sulla vita dei migranti. Parimenti, in tema di spazio di sperimentazione normativa per l'IA, la sintesi del progetto di IA che va pubblicata sul sito web delle autorità competenti, *ex* art. 59, par. 1, j), non riguarda i dati operativi sensibili in relazione alle attività delle autorità competenti in materia di controllo delle frontiere, di immigrazione o di asilo.

La peculiarità della nostra materia è confermata dal considerando 159, ai sensi del quale ciascuna autorità di vigilanza del mercato per i sistemi di IA ad alto rischio nel settore della biometria, nella misura in cui tali sistemi siano utilizzati nell'ambito di migrazione, asilo e gestione del controllo delle frontiere, dovrebbe disporre di poteri di indagine e correttivi efficaci, tra cui almeno il potere di ottenere l'accesso ai dati personali trattati ed alle informazioni necessarie per lo svolgimento dei suoi compiti.

Per contrastare il rischio di falsi positivi durante l'identificazione biometrica si prevede una supervisione umana per tutti i sistemi ad alto rischio (art. 14, regolamento sull'IA). Ne consegue che i risultati da essi prodotti devono essere verificati e confermati da un essere umano prima di poter assumere qualsiasi decisione.

Valorizzandosi l'importanza di un approccio antropocentrico nella valutazione dei sistemi di sorveglianza biometrica<sup>40</sup>, la supervisione umana, attraverso la correzione degli *output*, è principalmente volta a prevenire i rischi per la salute, la sicurezza e i diritti fondamentali. Per raggiungere questi obiettivi, l'art. 14 obbliga i fornitori<sup>41</sup> a creare le condizioni tecniche e operative per una supervisione efficace. Ciò è confermato dall'art. 26, par. 2, che impone ai *deployers*<sup>42</sup> di affidare la sorveglianza umana a persone fisiche che dispongano della competenza, della formazione, dell'autorità nonché del sostegno necessari. Inoltre, gli strumenti di intelligenza artificiale utilizzati dalle banche dati sulle migrazioni devono osservare le garanzie e le misure di protezione previste dall'art. 86 del regolamento sull'IA, secondo cui qualsiasi individuo che sia investito da una decisione, che produca effetti giuridici, o comunque incida significativamente, sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali, adottata dal *deployer* sulla base dell'*output* di un sistema ad alto rischio di cui all'allegato III ha il diritto di ottenere da quest'ultimo spiegazioni chiare e importanti sul ruolo giocato dal sistema di IA nella procedura decisionale e sui principali elementi della decisione assunta.

L'art. 86 citato è espressione del diritto a una tutela giurisdizionale effettiva tutelato dall'art. 47 della Carta dei diritti fondamentali, come ha

---

<sup>40</sup> Così M. Fink, *Human Oversight under Article 14 of the EU AI Act*, in *ssrn.com*, 14 February 2025, in cui si sottolinea che l'evidenza empirica suggerisce limitazioni sensibili all'efficacia della supervisione umana, anche a causa dei vincoli cognitivi umani e del *bias* dell'automazione. Dunque, il successo dell'art. 14 richiede un'attenta attuazione che riconosca tali limiti ed eviti di fare eccessivo affidamento sulla supervisione umana come misura di salvaguardia a sé stante. In questo senso anche A. Panezi, *Requirements of high-risk AI systems: AI Act. Article 14. Human oversight*, in *ssrn.com*, 1 July 2024.

L'EDPB e l'EDPB, nel citato parere congiunto 5/2021, hanno chiarito che l'importante ruolo attribuito alla supervisione umana nel regolamento sull'intelligenza artificiale è fondamentale per garantire il rispetto del diritto a non essere soggetti a una decisione basata esclusivamente sul trattamento automatizzato ai sensi del regolamento generale sulla protezione dei dati.

<sup>41</sup> Fornitore è «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito» (art. 3, n. 3, regolamento sull'IA).

<sup>42</sup> In conformità dell'art. 3, n. 4, *deployer* è «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

ricordato Corte di giustizia nel caso *Ligue des droits humains*<sup>43</sup>, in cui, con riferimento alla direttiva PNR (Passenger Name Record)<sup>44</sup>, si evidenzia che il ricorso alle tecnologie in parola e uno scarso accesso alle informazioni rischierebbero di privare di efficacia l'esame individuale dei riscontri positivi<sup>45</sup>. Infatti, considerata l'opacità che caratterizza il funzionamento delle tecnologie di intelligenza artificiale, può risultare impossibile comprendere la ragione per la quale un dato programma sia arrivato ad un riscontro positivo.

A questi obblighi, per rendere effettiva la supervisione, è necessario aggiungere i requisiti di trasparenza stabiliti dall'art. 13 del regolamento sull'IA.

Alla luce del quadro delineato, occorre certamente valutare positivamente la circostanza che la materia della migrazione rientri, in linea di principio, tra quelle ad alto rischio a cui sono applicabili una serie di cautele che il regolamento sull'IA dispone. D'altra parte, se il regolamento considera ad alto rischio questo settore, contempla una serie di eccezioni, come è il caso, ad esempio, dell'appena citato principio della supervisione umana che può essere evitata per esso quando il diritto UE o i diritti nazionali ritengano che l'adempimento risulti sproporzionato. Il testo non chiarisce quali siano i termini della sproporzione e dunque non definisce gli interessi contrastanti che giustifichino tale eccezione creando un vuoto normativo che può essere sfruttato in modo abusivo ed avallando l'applicazione di decisioni automatizzate, talvolta errate, senza la dovuta responsabilità umana.

Così, l'art. 14, par. 5, co. 2, in conformità del considerando 73, regolamento sull'IA, dispone che il requisito di una verifica separata da parte di almeno due persone fisiche – previsto in generale per i sistemi ad alto rischio – non si applichi ai sistemi di IA ad alto rischio utilizzati a fini di migrazione, controllo delle frontiere o asilo, qualora il diritto dell'Unione o nazionale ritenga sproporzionata l'applicazione di siffatto requisito.

---

<sup>43</sup> Corte giust., GS, 21 giugno 2022, C-817/19, *Ligue des droits humains*, punto 195.

<sup>44</sup> Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

<sup>45</sup> Il riscontro positivo previsto nella direttiva PNR si riferisce all'esito dell'attività di analisi dei dati PNR effettuata dall'Unità di Informazione sui Passeggeri (UIP) nazionale. In particolare, il riscontro positivo – che richiede evidentemente ulteriori verifiche o azioni da parte delle autorità competenti – indica l'individuazione di un passeggero sospettato di essere implicato in reati di terrorismo o gravi reati.

*5. La sorveglianza biometrica e le pratiche di intelligenza artificiale vietate per rischio inaccettabile: i sistemi di categorizzazione biometrica e l'identificazione biometrica remota in tempo reale*

Il regolamento sull'intelligenza artificiale pone un divieto ai sistemi di IA che determinano un rischio inaccettabile per la sicurezza e i diritti degli individui. Molte delle pratiche vietate sono di natura biometrica (art. 5) ed infatti, alla luce dei valori e dei diritti che la categorizzazione biometrica rischia di ledere, è prevalsa la linea secondo cui la tutela dei diritti inviolabili sottesa alle pratiche di intelligenza artificiale vietate deve imporsi sulle logiche di mercato e sulle misure di sicurezza.

In particolare, con riguardo alle interferenze con la materia della migrazione, dell'asilo e del controllo delle frontiere, il regolamento vieta (art. 5, par. 1, lett. e) i sistemi di IA che creano *database* di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso. Sono altresì vietati, in conformità dell'art. 5, par. 1, lett. g), i sistemi di categorizzazione biometrica per dedurre caratteristiche sensibili degli individui, come razza, orientamento sessuale, opinioni politiche o affiliazione religiosa. L'obiettivo della norma è prevenire discriminazioni e proteggere la tutela della vita privata e familiare degli individui, impedendo che dati biometrici vengano utilizzati per profilazioni ingiustificate.

Rientrano nel divieto, ad esempio, le tecnologie che riconoscono la razza o l'etnia delle persone in base a dati biometrici per finalità commerciali o governative. Sono disposte alcune eccezioni per usi ancillari legati a servizi commerciali, come i filtri per la classificazione di caratteristiche facciali nei *social network*. Tuttavia, questi sistemi devono essere strettamente necessari al servizio principale e non possono essere impiegati per scopi di controllo o sorveglianza.

L'art. 5, par. 1, lett. d) vieta i sistemi di IA al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione. Tale divieto è rilevante rispetto all'art. 32, par. 1, lett. a), vi) del Codice visti, in forza del quale l'ingresso o la concessione di un visto a un cittadino di un Paese terzo possono essere negati se tale individuo è considerato una minaccia per l'ordine pubblico o la sicurezza interna.

Il regolamento dispone un divieto generale di utilizzo delle tecnologie di identificazione biometrica, ma consente eccezioni specifiche e

strettamente regolate, previa autorizzazione giudiziaria. In questi casi, le tecnologie biometriche sono classificate come sistemi di intelligenza artificiale ad alto rischio e devono essere sottoposte a una valutazione di conformità prima di essere immesse sul mercato.

È richiesta un'attenta valutazione dell'impatto potenziale di queste tecnologie sui diritti fondamentali, dovendosi bilanciare i benefici del loro utilizzo con i rischi e le conseguenze negative che potrebbero derivare dal loro mancato uso. Così il regolamento, all'art. 5, par. 1, lett. h) e, dal par. 2 al par. 8, all'art. 5, stabilisce le condizioni in base alle quali l'identificazione biometrica remota in tempo reale può essere utilizzata per attività di contrasto.

Questo tipo di sorveglianza biometrica, come abbiamo già anticipato, comporta un forte impatto sui diritti fondamentali di chiunque vi sia sottoposto. Dunque il regolamento impone limiti stringenti, statuendo che i sistemi di identificazione biometrica remota in tempo reale in spazi pubblici per scopi di sicurezza non possono essere impiegati in modo indiscriminato, ma solo in tre casi specifici: ricerca di vittime di sottrazione, tratta o sfruttamento sessuale di esseri umani, nonché ricerca di persone scomparse; prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; identificazione e localizzazione di una persona sospettata di aver commesso un grave reato (per l'elenco dei reati si veda l'allegato II). Inoltre, l'identificazione biometrica remota in tempo reale da parte delle autorità di contrasto sarà subordinata a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o amministrativa indipendente (art. 5, par. 3).

La Commissione europea ha recentemente pubblicato le linee guida per l'attuazione dell'art. 5 del regolamento sull'intelligenza artificiale, stabilendo con maggiore chiarezza le pratiche vietate nell'uso dell'intelligenza artificiale<sup>46</sup>. Per quanto riguarda i divieti e le restrizioni all'uso dei sistemi di categorizzazione biometrica e dei sistemi di identificazione biometrica remota in tempo reale a fini di attività di contrasto, le linee guida della Commissione chiariscono che il regolamento, rispetto all'art. 10 della direttiva polizia, si applica in quanto *lex specialis*

---

<sup>46</sup> Comunicazione della Commissione, Orientamenti relativi alle pratiche di intelligenza artificiale vietate ai sensi del regolamento (UE) 2024/1689 (regolamento sull'IA), Bruxelles, 29 luglio 2025, C(2025) 5052 final.

disciplinando esso in modo esaustivo il trattamento dei dati biometrici interessati<sup>47</sup>.

Le ulteriori disposizioni di tale direttiva si aggiungono alle condizioni stabilite nel regolamento sull'IA, in particolare con riferimento all'uso di sistemi in tempo reale (identificazione biometrica remota) per attività di contrasto, e fatte salve le appena citate eccezioni di cui all'art. 5, par. 1, lett. h), del regolamento sull'IA. Più in generale, la direttiva polizia deve essere rispettata anche per quanto riguarda il trattamento di dati personali da parte di autorità di contrasto competenti quando il trattamento dei dati è a fini di attività di contrasto. D'altro canto, conformemente all'art. 2, par. 7, del regolamento sull'IA, la direttiva polizia e gli atti dell'Unione in materia di protezione dei dati restano salvi e continueranno ad applicarsi parallelamente al regolamento sull'IA che è coerente e complementare all'*acquis* dell'UE in materia di protezione dei dati.

Se, a differenza delle proposte precedenti, il regolamento non esclude dal proprio ambito di applicazione i sistemi biometrici su larga scala dell'UE, esso concede a tali sistemi un periodo di tempo maggiore per conformarsi alle pertinenti disposizioni. In particolare, all'art. 111, par. 1, fatte salve le pratiche di IA vietate (art. 5), prevede che i sistemi di IA che sono componenti di sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, contemplati nell'allegato X, tra cui il Sistema di informazione Schengen, il Sistema di informazione visti, Eurodac, il Sistema di ingressi/uscite, il Sistema europeo di informazione e autorizzazione ai viaggi, il Sistema europeo di informazione sui casellari giudiziari riguardo ai cittadini di Paesi terzi e apolidi, si uniformeranno al regolamento entro il 2030.

#### *6. Il quadro giuridico della biometria: un delicato equilibrio tra innovazione e protezione dei dati*

L'applicazione delle tecnologie biometriche in materia di migrazione, asilo e controllo delle frontiere è regolata anche dalla legislazione sulla protezione dei dati.

I dati biometrici sono definiti nell'art. 4, n. 14, RGPD 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

---

<sup>47</sup> Comunicazione della Commissione del 29 luglio 2025, cit., par. 46.

Giuseppina Pizzolante

*Il quadro giuridico europeo sulla sorveglianza biometrica*

l'immagine facciale o i dati dattiloscopici», restringendosene l'applicazione solo ai dati che risultino da un processo tecnico ed allo scopo dell'identificazione univoca.

Il regolamento generale sulla protezione dei dati, come è noto, fissa le norme relative al trattamento dei dati personali per tutte le finalità, ad eccezione dei casi in cui, in forza dell'art. 2, par. 2, lett. d), esso sia effettuato dalle autorità competenti «a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse». Il regolamento generale, dunque, non si applica a tutti i dati biometrici poiché quando i dati personali vengono trattati a fini di contrasto si applica la direttiva polizia. L'art. 3, n. 13 di quest'ultima definisce i dati biometrici allo stesso modo dell'art. 4, n. 14, RGPD.

Invero, l'applicazione delle tecnologie biometriche può giuridicamente rientrare sia nel trattamento di dati personali, nel caso di tecnologie biometriche che hanno lo scopo di categorizzazione, sia nel trattamento di dati biometrici, se riguarda il trattamento con mezzi tecnici ai fini dell'identificazione univoca<sup>48</sup>. In taluni casi, in base a quanto disciplinato dal diritto UE, gli individui non sono necessariamente identificati in modo univoco dalla biometria e dunque il trattamento dei pertinenti dati biometrici dovrebbe rientrare nel contesto più ampio del trattamento dei dati personali.

Rispetto alla nozione di dato personale, il RGPD, all'art. 4, n. 1, e la direttiva polizia, all'art. 3, n. 1, si riferiscono a «qualsiasi informazione riguardante una persona fisica identificata o identificabile». La Corte di giustizia ha chiarito che i dati personali sono definiti in senso ampio, onde permettere l'identificazione di un individuo in combinazione con altre informazioni disponibili anche se conservate da un soggetto diverso dal titolare del trattamento<sup>49</sup>.

Dunque, le tecnologie biometriche nel contesto della migrazione, dell'asilo e dei controlli alle frontiere vengono utilizzate per il trattamento di dati biometrici o, in caso di categorizzazione, per il trattamento di dati personali. Sia il RGPD che la direttiva polizia prevedono, rispetto ai dati

---

<sup>48</sup> V. nota 36. In forza del considerando 51 del regolamento generale sulla protezione dei dati, il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica.

<sup>49</sup> Corte giust., 19 ottobre 2016, C-582/14, *Breyer*, punti 40-42.

personali, un quadro normativo specifico per il trattamento dei dati sensibili, inclusi i dati biometrici, stabilendo condizioni eccezionali per le quali i dati possono essere trattati.

Rispetto al regolamento generale, la direttiva polizia è meno restrittiva nel consentire il trattamento dei dati biometrici. Il RGPD vieta, nell'art. 9, in linea di principio il trattamento dei dati biometrici e poi elenca le eccezioni a tale divieto, incluso il trattamento dei dati biometrici per motivi di interesse pubblico rilevante. In particolare, l'art. 9, par. 2, lett. g), RGPD fornisce la base giuridica per il trattamento dei dati biometrici da parte delle autorità pubbliche, ammettendolo purché sia necessario «per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato». Queste condizioni prevedono un test di proporzionalità al pari di quello previsto nella Carta dei diritti fondamentali e della CEDU<sup>50</sup>.

La direttiva polizia, invece, consente il trattamento di categorie particolari di dati personali, inclusi i dati biometrici, ove strettamente necessario e autorizzato dalla legge dovendosi in ogni caso applicare i principi in tema di trattamento dei dati contenuti nell'art. 4 della stessa direttiva. Ai sensi dell'art. 10, le autorità competenti possono trattare i dati biometrici ove strettamente necessario, richiedendosi una attenta analisi di bilanciamento tra il trattamento e la sua finalità. In questi casi il trattamento deve essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato ed ammesso soltanto se autorizzato dal diritto dell'Unione o dello Stato membro; per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o se il trattamento riguarda dati resi manifestamente pubblici dall'interessato. Evidentemente la base giuridica più rilevante per condurre la sorveglianza biometrica ai sensi della direttiva polizia è quella in cui il trattamento sia autorizzato dalla legge.

Secondo la Corte di giustizia<sup>51</sup>, il trattamento di dati biometrici da parte delle autorità di polizia è consentito ai fini di attività di contrasto qualora si fondi su una legge nazionale sufficientemente chiara e precisa, anche ove tale legge dovesse richiamare in modo errato il RGPD anziché la direttiva polizia. La Corte nella causa *Ministerstvo na vatrešnite raboti* ha sottolineato che, mentre un trattamento di dati biometrici da parte delle autorità competenti per fini rientranti nell'ambito di applicazione della

---

<sup>50</sup> Così M. Kontak, *op. cit.*, p. 629. V. meglio *infra* par. 7.

<sup>51</sup> Corte giust., 26 gennaio 2023, C-205/21, *Ministerstvo na vatrešnite raboti*.

direttiva polizia può essere autorizzato purché, conformemente ai requisiti enunciati all'art. 10 citato, sia strettamente necessario, soggetto a garanzie adeguate e previsto dal diritto dell'Unione o dello Stato membro, ciò non avviene necessariamente nel caso di un trattamento degli stessi dati rientrante nell'ambito di applicazione del RGPD<sup>52</sup>. Pertanto, il legislatore nazionale deve accertare l'assenza di ambiguità quanto all'applicabilità dell'uno o dell'altro atto UE alla raccolta dei dati biometrici<sup>53</sup> ed, in caso di conflitto tra le disposizioni nazionali che sembrano consentire e quelle che sembrano precludere il trattamento, la soluzione del conflitto consiste nel favorire un'interpretazione che salvaguardi l'effetto utile della direttiva polizia<sup>54</sup>.

L'art. 22 del regolamento generale, dedicato al processo decisionale automatizzato, si occupa della garanzia dell'intervento umano, distinguendo tra le decisioni, ai sensi dell'art. 22, par. 1, che includono nel ciclo del processo decisionale tale intervento come componente essenziale e le decisioni, *ex art. 22, par. 2*, fondate unicamente sul trattamento automatizzato che prevedono la garanzia dell'intervento umano su richiesta, al di fuori del ciclo del processo decisionale<sup>55</sup>. Dubbi emergono rispetto all'avverbio unicamente poiché è dall'interpretazione di questo termine che consegue l'ambito di applicazione della norma dovendosi determinare la soglia minima di intervento umano necessaria per non rendere un processo decisionale esclusivamente automatizzato.

Basandosi sull'interpretazione approvata dall'EDPB, per entrambi i meccanismi, il tipo di intervento umano richiesto dal RGPD dovrebbe essere "significativo"<sup>56</sup>, intendendosi evidentemente che l'intervento umano

---

<sup>52</sup> *Ivi*, punti 62-63.

<sup>53</sup> *Ivi*, punto 67.

<sup>54</sup> *Ivi*, punto 72.

<sup>55</sup> Una disposizione simile è contenuta anche nella direttiva (UE) 2016/680, il cui art. 11, par. 1, prevede che «gli Stati membri dispongono che una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato sia vietata salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento».

<sup>56</sup> Così G. Lazcoz - P. de Hert, *Humans in the GDPR and ALA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities*, in *Computer Law & Security Review*, 50/2023. V. anche sul punto A.Z. Huq, *A Right to a Human Decision*, in *Virginia Law Review*, 2020, p. 611 ss. Le Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 sono state adottate

deve garantire innanzitutto la contestabilità e che esso induce i titolari del trattamento ad una maggiore responsabilità rispetto ai dati processati.

Le procedure biometriche di sorveglianza sottese ai sistemi informativi su larga scala si basano sui dati raccolti nel momento in cui il soggetto migrante chiede di entrare in territorio europeo. L'analisi delle caratteristiche dell'interessato attraverso l'esame automatico dei suoi dati è quindi legittimo, ma il migrante deve essere informato dei suoi diritti, compreso quello di far intervenire un essere umano per analizzare concretamente il caso.

### *7. La sorveglianza biometrica e la tutela dei diritti fondamentali*

Il quadro giuridico della sorveglianza biometrica, come è ampiamente emerso nel corso dell'analisi, solleva importanti questioni relative ai diritti fondamentali, in particolare per quanto riguarda il rispetto della vita privata e familiare, la non discriminazione e la dignità umana. Ne parliamo nella parte finale dell'indagine proprio perché si tratta di un quadro giuridico onnicomprensivo.

La Carta dei diritti fondamentali UE prevede norme distinte con riguardo al rispetto della vita privata e della vita familiare (art. 7) e alla protezione dei dati di carattere personale (art. 8) sebbene la Corte di giustizia le abbia tradizionalmente applicate simultaneamente quando ha esaminato la conformità con la Carta delle disposizioni europee o nazionali relative al trattamento dei dati personali<sup>57</sup>.

L'art. 52, par. 1, della Carta ammette limitazioni all'esercizio di siffatti diritti purché esse siano previste dalla legge e rispettino il contenuto essenziale dei diritti e, in conformità del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dal diritto UE o all'esigenza di proteggere i diritti e le libertà altrui.

---

definitivamente il 6 febbraio 2018. Durante la sua prima riunione plenaria, l'EDPB ha approvato le GDPR related WP29 Guidelines. Endorsement 1/2018, reperibili *online* al sito [https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb\\_es](https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_es). Si veda anche Corte giust., 7 dicembre 2023, C-634/21, *SCHUFA Holding (Scoring)*.

<sup>57</sup> Corte giust., 17 ottobre 2013, C-291/12, *Schwarz*, punto 25, e 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger e a.*, punto 29. V. anche conclusioni dell'Avvocato generale Cruz Villalón, del 12 dicembre 2013, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger e a.*, punto 64, in cui si sostiene che, nel caso di dati personali non inerenti alla vita privata, dovrebbe applicarsi solo l'art. 8 della Carta.

La Convenzione europea dei diritti dell'uomo (CEDU) comprende nel proprio ambito di applicazione le tecnologie biometriche attraverso l'art. 8 CEDU, dedicato, come è noto, al diritto al rispetto della vita privata e familiare ma applicato estensivamente anche al diritto alla protezione dei dati. L'art. 8, par. 2 CEDU stabilisce che l'ingerenza di un'autorità pubblica nel diritto alla vita privata di un individuo è giustificata se è necessaria in una società democratica nell'interesse della sicurezza nazionale, della sicurezza pubblica o del benessere economico del paese, per la difesa dell'ordine e la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui.

Nel valutare la liceità della raccolta di dati biometrici, la Corte EDU ha sancito la violazione dell'art. 8 CEDU da parte di una legislazione nazionale, laddove la natura generale e indiscriminata delle competenze di conservazione delle impronte digitali, dei campioni cellulari e dei profili DNA di persone sospette non riesca a trovare un giusto equilibrio tra i concorrenti interessi, pubblici e privati<sup>58</sup>. Di conseguenza tale tipo di conservazione costituisce un'interferenza sproporzionata con il diritto al rispetto della vita privata e non può essere considerata necessaria in una società democratica, riconoscendosi che l'uso di dati biometrici, come l'origine etnica, può rendere gli individui interessati vulnerabili alla stigmatizzazione e alla discriminazione.

L'impatto sui diritti fondamentali va stimato alla luce della tecnologia biometrica utilizzata poiché differenti tecnologie possono avere impatti differenti sul diritto alla vita privata e familiare, come ad esempio la profilazione del DNA rispetto al rilevamento delle impronte digitali. Inoltre, è importante esaminare la durata della conservazione dei dati biometrici, l'accesso ai dati, le categorie di soggetti coinvolti nonché il tipo di normativa che disciplina l'uso della tecnologia biometrica. In particolare, secondo il giudizio della stessa Corte, è cruciale determinare la possibilità di revisione delle decisioni di conservazione dei dati nonché l'efficacia dei controlli.

La Corte EDU ha così statuito che la detenzione a tempo indeterminato dei dati biometrici delle persone condannate è contraria al diritto alla vita privata, ai sensi dell'art. 8 CEDU<sup>59</sup>, e che il *software* di riconoscimento facciale utilizzato dalle autorità pubbliche contro un manifestante solitario e pacifico viola gli ideali e i valori di una società

---

<sup>58</sup> Corte EDU, GC, 4 dicembre 2008, ric. 30562/04 e 30566/04, *S. e Marper c. Regno Unito*, paragrafi 122-126. La sentenza ha anche ricordato che i dati sono condivisi a livello europeo attraverso la banca dati SIS.

<sup>59</sup> Corte EDU, 13 febbraio 2020, ric. 45245/15, *Gangbrun c. Regno Unito*.

democratica tutelati sempre dall'art. 8 CEDU<sup>60</sup>. Nello specifico, il trattamento dei dati biometrici mediante la tecnologia di riconoscimento facciale nell'ambito di un procedimento per infrazione amministrativa che, a partire dalle fotografie e dai video pubblicati su internet, ha perseguito lo scopo di identificare il ricorrente, di localizzarlo e di fermarlo, non ha risposto a un bisogno sociale imperativo e non può essere considerato necessario in una società democratica. La Corte EDU ha pertanto evidenziato che la raccolta di dati biometrici viola il diritto al rispetto della vita privata e familiare, dovendosi ravvisare un obiettivo legittimo per giustificare l'interferenza da parte delle autorità pubbliche.

La giurisprudenza della Corte di giustizia UE ha avuto modo di chiarire che le tecnologie biometriche possono essere consentite in determinati casi e che il loro utilizzo deve essere esaminato ai sensi degli articoli 7 e 8 della Carta dei diritti fondamentali, nonché della legislazione secondaria sulla protezione dei dati. Essa ha sottolineato che il rispetto della vita privata con riguardo al trattamento dei dati personali, riconosciuto dagli articoli 7 e 8 citati, concerne qualsiasi informazione relativa a una persona fisica identificata o identificabile come è il caso dei dati biometrici che contengono informazioni univoche sulle persone fisiche<sup>61</sup>. La Corte di giustizia ha poi statuito che l'inserimento obbligatorio delle impronte digitali nei passaporti di nuova emissione, come previsto dal regolamento 2252/2004, deve essere considerato un trattamento di dati personali<sup>62</sup>, indicando che in tale inserimento sussiste un'ingerenza giustificata con il diritto al rispetto della vita privata e familiare al fine di prevenire il furto d'identità e l'immigrazione illegale<sup>63</sup>. Successivamente ha aggiunto che le

---

<sup>60</sup> Corte EDU, 4 luglio 2023, ric. 11519/20, *Glukhin c. Russia*. Si veda F. Di Matteo, *La riservatezza dei dati biometrici nello Spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale*, in *Freedom, Security & Justice: European Legal Studies*, 2023, p. 74 ss.; G. Mobilio, *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso Glukhin c. Russia*, in *DPCE Online*, 1/2024, p. 695 ss.

<sup>61</sup> Corte giust., sentenza *A e a.*, punto 55 e giurisprudenza ivi citata. Si veda anche documento di lavoro dei servizi della Commissione – Valutazione dell'impatto, Proposta di regolamento del Parlamento europeo e del Consiglio sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione, Strasburgo, 17 aprile 2018, COM(2018) 212 definitivo, punto 6.1, in cui si sottolinea che i dati biometrici devono essere crittografati e che, a tal fine, è necessario scambiare le chiavi crittografiche con i servizi specifici, vale a dire le guardie di frontiera e la polizia.

<sup>62</sup> Corte giust., sentenza *Schwarz*, punto 29.

<sup>63</sup> *Ivi*, punti 36-38.

autorità pubbliche, sempre in conformità dell'art. 7 della Carta dei diritti fondamentali UE, non sono obbligate a garantire nelle legislazioni nazionali che i dati biometrici rilevati e conservati non saranno trattati e utilizzati per fini diversi dal rilascio del passaporto<sup>64</sup>.

Inoltre, il diritto UE impedisce, secondo la Corte di giustizia<sup>65</sup>, una conservazione generalizzata e indifferenziata dei dati sul traffico e sull'ubicazione degli individui a fini di contrasto, consentendosi di conseguenza solo una sorveglianza biometrica mirata in forza dell'art. 52, par. 1, della Carta. Questo tipo di sorveglianza si distingue dalla sorveglianza di massa in quanto è rivolta a una persona o a un gruppo di persone sulla base di un presunto coinvolgimento in attività criminali. La stessa Corte ha poi evidenziato che l'ambito di applicazione di una misura che prevede la conservazione dei dati relativi al traffico e all'ubicazione può essere fondata anche su un criterio geografico qualora le autorità nazionali competenti considerino, in forza di elementi oggettivi e non discriminatori, che esiste, in una o più zone geografiche, una situazione caratterizzata da un rischio elevato di preparazione o di commissione di atti di criminalità grave<sup>66</sup>. Siffatte zone possono essere, in particolare, luoghi caratterizzati da un numero elevato di atti di criminalità grave, luoghi particolarmente esposti alla commissione di tali atti, quali luoghi o infrastrutture frequentati regolarmente da un numero molto elevato di persone, o ancora luoghi strategici, quali aeroporti, stazioni o aree di pedaggio; tuttavia, nel contesto della sorveglianza biometrica negli spazi pubblici, questo criterio potrebbe non rappresentare una limitazione sufficiente poiché essa finirebbe col monitorare indiscriminatamente qualunque individuo si venisse a trovare in quello spazio.

Laddove la sorveglianza biometrica venga condotta in modo mirato, la sua liceità dipende dalla finalità legittima perseguita e da una valutazione della sua proporzionalità alla luce di tale obiettivo<sup>67</sup>. Dunque, in una zona di frontiera, ad esempio, la sorveglianza biometrica mirata è consentita solo se strettamente necessaria ai fini della lotta al terrorismo o alla criminalità grave, dovendosi altresì predisporre rimedi giurisdizionali effettivi per gli

---

<sup>64</sup> Corte giust., 16 aprile 2015, cause riunite C-446/12-C-449/12, *Willems e a.*

<sup>65</sup> Corte giust., sentenza *Digital Rights Ireland e Seitlinger e a.*, punto 37; nonché Corte giust., GS, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige*, punto 100. Si veda F. Rossi Dal Pozzo, *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, in *I Post di AISDUE*, 2019, p. 127 ss.

<sup>66</sup> Corte giust., GS, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, punto 150. Così anche sentenza *Tele2 Sverige*, punto 111.

<sup>67</sup> V., in tal senso, sentenza *Tele2 Sverige*, punto 102.

individui coinvolti. Secondo la Corte di giustizia, infatti, il provvedimento che autorizza la sorveglianza biometrica mirata deve essere oggetto di un controllo effettivo da parte di un giudice o di un organo amministrativo indipendente, la cui decisione sia dotata di effetto vincolante, diretto a verificare l'esistenza di una situazione che giustifichi il provvedimento<sup>68</sup>.

Come si è già accennato, nell'applicazione della sorveglianza biometrica, oltre alla tutela della vita privata e familiare e alla protezione dei dati, rilevano anche altri diritti fondamentali, come la dignità umana, che può essere compromessa dal modo in cui funziona una tecnologia biometrica o dai dati che essa elabora ad esempio, nel caso del rilevamento forzato delle impronte digitali, qualora un individuo non comprenda appieno la procedura e i propri diritti<sup>69</sup>. Nella ipotesi del rilevamento delle impronte digitali, in particolare, la dignità umana può essere lesa dalla natura coercitiva della procedura, se determinate categorie di individui, quali i migranti irregolari o i richiedenti asilo, siano costretti a scegliere tra il rilevamento delle impronte digitali o la possibile detenzione con conseguente perdita dell'accesso all'asilo<sup>70</sup>.

---

<sup>68</sup> Corte giust., sentenza *La Quadrature du Net e a.*, punto 179.

<sup>69</sup> FRA Focus, *Le ripercussioni sui diritti fondamentali dell'obbligo di fornire le impronte digitali per Eurodac*, in fra.europa.eu, 05/2015. Con riferimento all'uso della coercizione sui minori si veda R. Bendinelli, *Le norme sul trattamento dei dati personali dei richiedenti asilo nell'Unione europea: talune criticità rispetto al caso dell'interessato minorenne*, in *Diritto, Immigrazione e Cittadinanza*, 2024, p. 19 ss.

<sup>70</sup> Diversi Stati membri hanno adottato pratiche quali la segnalazione telefonica, che presuppone l'uso di *software* di riconoscimento vocale o facciale, alle autorità e forme di controllo tramite dispositivi gps con l'obiettivo dichiarato di ridurre il numero di persone trattenute nei centri di detenzione amministrativa. Le misure alternative alla detenzione spesso vengono strumentalizzate e rese funzionali a scopi di controllo e sorveglianza tali da renderle vere e proprie detenzioni alternative. Diverse ricerche hanno dimostrato le difficoltà affrontate da coloro che sono soggetti a questi controlli tra cui l'accesso al lavoro, i rischi di stigmatizzazione, l'aggravamento dei problemi di salute mentale, nonché il dolore o il disagio fisico associati all'uso di tecnologie di tracciamento. Inoltre, molti dei migranti soggetti a siffatte misure appartengono a gruppi vulnerabili. In più occasioni, le istituzioni internazionali per i diritti umani hanno segnalato le probabili violazioni derivanti dall'uso del monitoraggio elettronico come alternativa alla detenzione. Si veda sul punto il report *Technologies, migration and human rights: the role of European NHRIs*, ENNHRI scoping paper, Saint-Gilles, 2024, p. 19, nonché L. Nalbandian, *An eye for an "I": a critical assessment of artificial intelligence tools in migration and asylum management*, in <https://comparativemigrationstudies.springeropen.com/>, 03 August 2022.

La dignità umana può altresì essere compromessa dalla tecnologia di riconoscimento facciale<sup>71</sup> la quale rileva anche ai fini della non discriminazione poiché siffatta tecnologia, come si è detto<sup>72</sup>, potrebbe non identificare con altrettanta efficacia i volti neri rispetto a quelli bianchi, e i volti femminili rispetto a quelli maschili.

#### 8. *Considerazioni conclusive*

L'analisi che si è compiuta ha evidenziato, tra l'altro, che le rotte intraprese dai migranti, governate dalle politiche di sicurezza, sono dominate dai meccanismi di sorveglianza biometrica esaminati, i quali, se offrono molti vantaggi nella gestione delle migrazioni in termini di sicurezza, sollevano gravi preoccupazioni in termini di diritti umani trasformando le frontiere in zone in cui sono più evidenti le massicce violazioni dei diritti umani<sup>73</sup>. Tali politiche influenzano le rotte che i migranti possono intraprendere, costringendoli ad affidarsi a percorsi più difficili e pericolosi e minacciando il loro diritto di asilo. I programmi di scambio di informazioni tra Stati membri<sup>74</sup> consentono la raccolta e la condivisione di grandi quantità di dati personali sulle persone in movimento. Questi sistemi possono portare a discriminazioni e identificazioni errate (ad esempio, attraverso strumenti di riconoscimento facciale) a causa di distorsioni nei dati biometrici.

Le misure presenti nel regolamento sull'intelligenza artificiale possono essere certamente qualificate come una importante risposta alle complicate questioni delineate, sebbene esse entreranno in vigore, con riguardo ai sistemi informativi su larga scala, "solo" tra un quinquennio,

---

<sup>71</sup> V. EDPB, linee guida 05/2022, punto 39: «in molti casi l'utilizzo dei dati biometrici e della FRT in particolare incide anche sul diritto alla dignità umana, garantito dall'articolo 1 della Carta. La dignità umana richiede che gli individui non siano trattati come semplici oggetti. La FRT calcola caratteristiche esistenziali ed estremamente personali (i tratti del viso) tramite lettura elettronica, al fine di utilizzarle come una targa umana o una carta d'identità, oggettivando così il volto».

<sup>72</sup> V. *supra* par. 3.

<sup>73</sup> Per una approfondita riflessione sulle ricadute della cooperazione alle frontiere europee sulla tutela dell'individuo, D. Vitiello, *Le frontiere esterne dell'Unione europea*, Bari, 2020, p. 201 ss.; I. Ingravallo, *Il rispetto dei diritti fondamentali nell'azione dell'Agenzia europea della guardia di frontiera e costiera*, in I. Caracciolo - G. Cellamare - A. Di Stasi - P. Gargiulo (a cura di), *Migrazioni internazionali. Questioni giuridiche aperte*, Napoli, 2022, p. 111 ss.

<sup>74</sup> V., solo per alcuni riferimenti, [www.consilium.europa.eu/it/policies/it-systems-security-justice/](http://www.consilium.europa.eu/it/policies/it-systems-security-justice/).

probabilmente a causa della interoperabilità che è ancora *in fieri*. I complessi meccanismi di interoperabilità dei dati serviranno, tra l'altro, ad esternalizzare i controlli di frontiera con maggiore accuratezza, consentendo di monitorare le rotte dei migranti nei Paesi terzi molto prima che essi raggiungano i confini dell'UE e di categorizzare i migranti e i loro percorsi di movimento utilizzando valutazioni di sicurezza automatizzate.

L'allineamento tra le politiche di frontiera dell'UE e le tecnologie di sorveglianza biometrica evidenzia che queste ultime non sono più strumenti isolati da sguinzagliare agli ingressi ma si estendono attraverso lo spazio e il tempo oltre il luogo di ingresso<sup>75</sup>. Così l'elenco dei sistemi ad alto rischio avrebbe dovuto inglobare i sistemi di intelligenza artificiale volti a prevedere le tendenze migratorie e gli attraversamenti delle frontiere poiché, se per un verso, questi modelli, attraverso tecniche predittive, possono garantire risposte efficienti alle crisi migratorie, per altro verso, rischiano di diventare l'ennesimo desolante strumento volto ad impedire ai richiedenti asilo di raggiungere le proprie mete. Pertanto, in forza degli articoli 7, 97 e 112 del regolamento sull'intelligenza artificiale che, in linea con gli sviluppi tecnologici e le esigenze sociali, consentono alla Commissione di aggiornare gli elenchi, dovrebbero essere modificati sia l'elenco dei sistemi di IA vietati sia l'allegato III del regolamento.

Allo stesso modo, sebbene il regolamento generale sulla protezione dei dati offra determinate garanzie in merito all'uso di processi decisionali individuali automatizzati e alla protezione dei dati personali, e rappresenti un punto di partenza per standard globali più ampi, pure tracciati attraverso il regolamento sull'intelligenza artificiale, il quadro che ne deriva non appare sufficiente a proteggere i diritti fondamentali dei migranti.

In particolare, con riguardo ai processi decisionali automatizzati, il regolamento generale sulla protezione dei dati dovrebbe meglio chiarire il ruolo dell'intervento umano rispetto al funzionamento delle tecnologie sottostanti alla gestione delle migrazioni. Tale interpretazione è in linea con l'approccio antropocentrico accolto nel regolamento sull'intelligenza artificiale in forza del quale viene imposto ai fornitori di IA l'obbligo di informare gli utenti dei loro sistemi su elementi essenziali, come le misure tecniche adottate per facilitare l'interpretazione dei risultati dei sistemi di IA. Il regolamento, tuttavia, non si applicherà immediatamente alla materia delle

---

<sup>75</sup> Sulla definizione di confine e di frontiera esterna si veda G. Caggiano, *Recenti sviluppi del regime delle frontiere esterne nello Spazio di libertà, sicurezza e giustizia*, in A. Di Stasi - L.S. Rossi (a cura di), *Lo Spazio di libertà, sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere*, Napoli, 2020, p. 383 ss.

migrazioni e, alla luce dell'art. 6, paragrafi 4-8, potrebbe in futuro escludere dal proprio ambito di applicazione i sistemi di IA impiegati nei *database* di controllo delle frontiere dell'UE.

Si tratta di suggestioni e riflessioni volte, tra l'altro, ad accrescere la fiducia rispetto alla politica UE in materia di migrazione, asilo e controllo delle frontiere, mostrandoci che il coinvolgimento "sostanziale" degli esseri umani nel processo decisionale serve a garantire che i meccanismi biometrici vengano accuratamente esaminati in tutte le fasi del processo assicurando nel contempo una concreta possibilità di contestare un *output*. Dunque, oltre all'ampliamento dell'ambito di applicazione delle categorie ad alto rischio, è necessario irrobustire la garanzia della supervisione umana e della trasparenza.

L'equilibrio tra sicurezza, innovazione tecnologica e diritti fondamentali non è mai stato così delicato, specie nelle regioni di confine. La costruzione di un sistema migratorio europeo moderno, equo, inclusivo ed in cui la sorveglianza biometrica sia funzionale al raggiungimento dei più nobili traguardi di cooperazione e libera circolazione, richiede che l'uso dei sistemi di IA, in caso di conflitto tra valori, propenda per la salvaguardia dei diritti fondamentali dei migranti.

\*\*\*

**ABSTRACT:** The use of biometric surveillance in migration, asylum, and border control processes is becoming increasingly prevalent in European Member States in order to monitor borders and identify individuals transiting through their territories. Another significant application of biometrics pertains to various large-scale IT systems. This Article aims to reconstruct the European legal framework surrounding biometric surveillance, demonstrating that human rights violations are most evident at borders. The measures outlined in the AI Act can certainly be regarded as an important, yet still insufficient, response to the complex issues outlined.

**KEYWORDS:** biometric surveillance - border control - human rights – EU AI Act - large-scale IT Systems

\*\*\*

**Giuseppina Pizzolante** - Professore associato di Diritto dell'Unione europea, Università degli studi di Bari Aldo Moro ([giuseppina.pizzolante@uniba.it](mailto:giuseppina.pizzolante@uniba.it))