COSTANZA DI FRANCESCO MAESA

IL SISTEMA DI SORVEGLIANZA BIOMETRICA ALLE FRONTIERE DELL'UE[1]

Introduzione

La presidente della Commissione Ursula Von der Leyen ha affermato che sono stati stanziati 170 milioni di finanziamenti per «aggiornare i sistemi di sorveglianza elettronici, migliorare le reti di telecomunicazione [e] installare apparecchiature mobili di rilevamento» al fine di «contrastare le minacce ibride derivanti dall'inaccettabile uso della migrazione come arma» (2024, https://ec.europa.eu/commission/presscorner/detail/it/ip_24_6251). L'obiettivo è quello di «garantire la sicurezza dell'Unione e l'integrità territoriale degli Stati membri» (COM 2024/570: 2) e l'accento è posto sulla necessità di garantire la sicurezza interna e combattere l'immigrazione irregolare.

Queste dichiarazioni trovano riscontro nei documenti programmatici e nella le-

1 Marie Sklodowska-Curie Postdoctoral Fellow, Università di Siena, Italia, e Universidade de São Paulo, Brasile. Finanziato dall'Unione Europea. Il punto di vista e le opinioni espresse sono tuttavia esclusivamente dell'autore e non riflettono necessariamente quelli dell'Unione Europea o dell'autorità che ha stipulato il Grant Agreement, ovvero l'Agenzia esecutiva europea per la ricerca (REA), che lo ha stipulato grazie alla delega da parte della Commissione Europea. Né l'Unione Europea né REA o la Commissione europea possono essere ritenuti responsabili per essi. Nome del Progetto: "EcoAI - A New EU Framework for an Ecological AI", HORIZON-MSCA-PF-2023, Marie Sklodowska Curie Actions, Post doctoral Fellowships, Global Fellowships, GA 101155739.

gislazione adottata negli ultimi anni, che ha ulteriormente rafforzato i controlli alle frontiere esterne dell'UE e ha previsto l'installazione di sistemi di sorveglianza, e in particolare di sorveglianza biometrica. L'uso di questi ultimi, tuttavia, mette seriamente a rischio alcuni diritti fondamentali dei cittadini dei Paesi terzi che intendono attraversare le frontiere esterne dell'UE, quali il diritto alla protezione dei dati personali, il diritto alla privacy e in alcuni casi anche il diritto ad un equo processo o il diritto all'inviolabilità della libertà personale.

Questo contributo intende esplorare questo importante tema soffermandosi in particolare sull'analisi delle conseguenze che derivano dall'uso crescente di sistemi di Intelligenza Artificiale (d'ora innanzi IA) per gestire i flussi di cittadini di Stati terzi alle frontiere esterne dell'UE. Sebbene la dottrina abbia esaminato il fenomeno da diversi punti di vista, sia studiando il fenomeno della cosiddetta *securisation*, che quello della criminalizzazione dei migranti irregolari (Mitsilegas 2011), sia esaminando l'impatto sui diritti fondamentali derivante dall'inserimento e il trattamento dei dati di questi ultimi nelle banche dati europee su larga scala (Vavoula 2022), non è, infatti, ancora stato studiato in modo approfondito in che modo e fino a che punto l'uso dei sistemi di IA per effettuare la sorveglianza biometrica alle frontiere esterne dell'UE rischi di violare i diritti fondamentali dei cittadini di Paesi terzi (ma cfr. Vavoula 2021).

A tal fine, il contributo, in primo luogo, indaga in che modo si esplica la sorveglianza biometrica digitale con sistemi di IA, soffermandosi sul ruolo svolto dalle banche dati europee su larga scala (1.1.) e sul duplice uso dei sistemi di IA per sorvegliare le frontiere esterne (1.2.) e per prendere decisioni nel settore dell'immigrazione (1.3.). Nel secondo e terzo paragrafo si esamina poi la disciplina prevista nel Regolamento sull'IA nel settore dell'immigrazione e l'asilo (2.) e si approfondisce la disciplina e le conseguenze derivanti dall'utilizzo di sistemi di riconoscimento facciale (3.). Nel quarto paragrafo, infine, si esaminano le conseguenze che l'uso di questi sistemi comporta per i diritti fondamentali dei cittadini di Paesi terzi, approfondendo, in particolare, in che modo rischino di essere violati gli articoli 7 e 8 della Carta (4.1.), il diritto di accesso, di rettifica, di cancellazione e il diritto ad un rimedio effettivo (4.2.), così come il principio di non discriminazione (4.3.). Infine, nelle conclusioni si traggono le somme dell'analisi previamente svolta, soffermandosi sugli aspetti più problematici che l'attuale situazione legislativa comporta.

1. Sorveglianza biometrica digitale con sistemi di IA

Qualunque cittadino di un Paese terzo che intenda attraversare i confini dell'UE è soggetto a controlli effettuati con tecnologie digitali e in particolare con sistemi di IA. La tendenza a privilegiare ragioni di sicurezza è, infatti, strettamente correlata all'uso di nuove tecnologie (Brouwer 2024), quali droni, strumenti di rilevazione della temperatura corporea, sistemi di IA per effettuare il confronto dei dati biometrici,

e sistemi di riconoscimento facciale, senza i quali gli Stati membri non avrebbero la possibilità di individuare e identificare un numero così elevato di persone in tempi rapidi. I dati dei cittadini dei Paesi terzi, dopo esser stati raccolti sono ulteriormente processati e controllati mediante l'inserimento in banche dati nazionali ed europee su larga scala, in cui sono processati tramite sistemi di IA; è per questo motivo che alcuni autori hanno parlato di «digitalizzazione della politica migratoria europea» (Besters/Brom 2010).[2]

1.1. Banche dati europee su larga scala ed EUROSUR

Per quanto riguarda la sorveglianza delle frontiere esterne dell'UE, assumono un ruolo fondamentale EUROSUR e le sei banche dati europee su larga scala. Grazie ad EUROSUR (Regolamento 2019/1896, art. 18), i Centri nazionali di coordinamento sono connessi ad un sistema centrale gestito da Frontex (Regolamento 2019/1896, artt. 20-21) e sono collegati tutti i sistemi di controllo utilizzati a livello europeo e nazionale, tra cui droni, telecamere, sensori e altri tipi di tecnologie volte a raccogliere dati. Tali sistemi sono utilizzati per effettuare le verifiche ai valichi di frontiera autorizzati e per effettuare una sorveglianza preventiva, al fine di evitare che cittadini irregolari si avvicinino ai confini dell'UE (Regolamento 2019/1896, art. 19). A tal fine, sono monitorati anche i *social media* e *internet* per individuare i trafficanti di esseri umani e le rotte che questi utilizzano per trasportare le persone sul territorio dell'UE. A tal proposito, di recente Frontex si è interessato alla possibilità di controllare i *media* mediante l'utilizzo di strumenti di IA (Frontex 2021a). Accanto ad EUROSUR, assumono fondamentale importanza le banche dati europee su larga scala. Queste ultime si sono moltiplicate negli ultimi anni; ne sono, infatti, state create delle nuove e si è ampliato l'ambito di applicazione di quelle preesistenti.

L'efficacia del sistema di sorveglianza biometrica alle frontiere esterne dell'UE si basa, in particolare, sull'operatività, e l'interoperabilità dal 2019 (Regolamento 2019/817; Regolamento 2019/818), di sei banche dati europee su larga scala, ossia lo *Schengen Information System* (d'ora innanzi SIS) (Regolamento (UE) 2018/1860; Regolamento (UE) 2018/1861; Regolamento (UE) 2018/1862), il Visa Information System (d'ora innanzi VIS) (Regolamento 767/2008; Regolamento 2021/1134), Eurodac (Regolamento 603/2013; Regolamento 2024/1358), l'*Entry/Exit System* (d'ora innanzi EES) (Regolamento 2017/2226), che dovrebbe entrare in vigore a novembre 2025, l'*European Travel Information and Authorisation System* (d'ora innanzi ETIAS) (Regolamento 2018/1240), che dovrebbe essere operativo a partire dalla fine del 2026, e l'*European Criminal Record Information System for third-country nationals* (d'ora innanzi ECRIS-TCN) (Regolamento 2019/816). Dal 2019, inoltre, come accennato, è prevista l'interoperabilità delle stesse, ossia la creazione di una serie di strumenti

2 In originale: *digitalisation of the European migration policy.*

utili a permettere di svolgere ricerche contemporaneamente su tutte le banche dati europee su larga scala. A tal fine è stato creato: un portale di ricerca europeo (ESP con acronimo inglese) che permetterà di effettuare la ricerca di un determinato soggetto simultaneamente su tutti i database su larga scala; la creazione di un *Biometric Matching Service*, che genererà template specifici sulla base di tutti i dati biometrici contenuti in SIS II, VIS, Eurodac, EES e ECRIS-TCN; un *Common Identity Repository* in cui saranno depositate le schede personali di ogni individuo. In tali schede sono contenuti sia i dati biometrici che biografici, così come una nota indicante da quale sistema sono state prese le informazioni, al fine di facilitare i controlli sui cittadini di Paesi terzi e individuare soggetti con plurime identità. È stata anche prevista l'adozione di un *Common Repository for Reporting and Statistics* (CRRS) e di un *Multiple Identity Detector* (MID con acronimo inglese) tramite cui creare collegamenti tra dati identici per capire se lo stesso individuo è registrato legittimamente in diverse banche dati o se vi è un sospetto di frode sull'identità (Regolamento 2019/817; Regolamento 2019/818).

Oltre a ciò, con il Nuovo Patto sulla Migrazione e l'Asilo è stato adottato anche un nuovo Regolamento istitutivo di Eurodac (Regolamento 2024/1358), in base al quale è prevista la raccolta sistematica dei dati biometrici dei migranti, ossia il rilevamento delle impronte digitali e delle immagini del volto, che saranno conservati nei database europei fino a dieci anni a decorrere dalla data di trasmissione dei dati biometrici (Regolamento 2024/1358, art. 29, considerando 55). I dati conservati in Eurodac possono essere consultati in ogni fase della procedura di frontiera e sono accessibili alle forze di polizia di tutti gli Stati membri al fine di identificare o controllare l'identità di chi intende attraversare la frontiera in modo irregolare (Regolamento 2024/1358, artt. 5, 10, 32, 34, 40). L'età minima di rilevamento dei dati è stata abbassata da quattordici a sei anni di età (Regolamento 2024/1358, art. 14, considerando 38). Nella norma a ciò espressamente dedicata si legge altresì che, sebbene non debba essere utilizzata alcuna forma di forza nei confronti dei minori, tuttavia, «può essere utilizzato un grado proporzionato di coercizione nei [loro] confronti per garantire il rispetto di tale obbligo» (Regolamento 2024/1358, art. 14, par. 1, 4).

Queste modifiche sollevano molte perplessità per quanto riguarda la compatibilità di tale normativa con il principio di limitazione delle finalità, in base al quale il trattamento dei dati personali deve essere effettuato con riguardo ad un obiettivo determinato, esplicito e legittimo (Regolamento 2016/679, art. 5, par. 1, lett. b; Brouwer 2011; Art. 29 WP 2013). Dal momento che Eurodac è stato inserito nel novero delle banche dati che sono interoperabili tra loro, infatti, i dati possono essere utilizzati per finalità del tutto diverse da quelle per cui sono stati raccolti e registrati in Eurodac (EDPS Opinion 2016). Per motivi di spazio e di attinenza al tema trattato non ci soffermeremo, tuttavia, in questa sede sulla descrizione del funzionamento delle sei banche dati europee su larga scala, né sull'interoperabilità delle stesse (cfr. Vavoula 2022), limitandoci ad analizzare in che modo l'analisi di dati nelle banche dati euro-

pee tramite sistemi di IA rischi di ledere i diritti fondamentali dei cittadini di Paesi terzi.

1.2. Uso di nuove tecnologie e sistemi di IA

Per quanto riguarda l'uso di nuove tecnologie e sistemi di IA per controllare in modo più efficace le frontiere dell'UE, le ultime riforme adottate a livello europeo hanno contribuito a rafforzare i controlli biometrici alle frontiere esterne dell'UE e hanno portato a "sperimentare" alcune nuove soluzioni tecnologiche e giuridiche nei confronti dei migranti (Vavoula 2021; Hayes 2009). Sono stati, per esempio, "testati" sistemi di riconoscimento facciale e vocale e sono aumentate le perquisizioni sugli oggetti personali, come gli smartphone, consentendo in tal modo, tramite sequestro e analisi di dispositivi personali, di estrarre dati utili a comprovare la veridicità delle dichiarazioni rilasciate o verificare l'identità, l'età e il Paese di origine dei cittadini di Paesi terzi (Regolamento 2024/1348, art. 9, par. 5). Tali pratiche sono state contestate in tribunale in alcuni Stati membri, tra cui la Germania (Palmiotto/Ozkul 2023), ma continuano ad essere utilizzate in altri (Ozkul 2023). Non esistendo regole europee uniformi in materia di modalità di raccolta dei dati utilizzati per identificare i cittadini di Paesi terzi, ogni Stato potrà infatti ricorrere alle tecniche che ritiene più idonee. Inoltre, il *Research Center* del Parlamento europeo ha individuato altre applicazioni degli algoritmi di IA nel campo della migrazione e l'asilo, prendendo in considerazione, per esempio, la possibilità di usare in futuro strumenti per identificare le emozioni e capire quando i migranti mentono, nonostante le forti preoccupazioni che l'uso di questi sistemi comporta (Dumbrava 2021).

L'uso di questi strumenti solleva dubbi quanto alla proporzionalità e necessità rispetto all'obiettivo da raggiungere (Marinai 2020). La Corte di Giustizia ha infatti precisato che nel caso di dati sensibili, il controllo di «stretta necessità» deve essere condotto con particolare rigore e deve essere sempre rigorosamente applicato il principio di limitazione delle finalità e il principio di minimizzazione dei dati (Regolamento 2016/679, art. 5, par. 1, lett. c; CGUE C-205/21, parr. 117, 118, 125).

Inoltre, la Corte ha ribadito che la «conservazione generalizzata e indifferenziata dei dati» di un numero indeterminato di individui comporta un'ingerenza grave nei diritti fondamentali di cui agli articoli 7 e 8 della Carta (CGUE *La Quadrature du Net*, par. 174), per cui la loro analisi automatizzata può soddisfare il requisito di proporzionalità «solo in situazioni nelle quali uno Stato membro si trovi di fronte ad una minaccia grave per la sicurezza nazionale che risulti reale e attuale o prevedibile, e a condizione che la durata di tale conservazione sia limitata allo stretto necessario» (CGUE *La Quadrature du Net*, par. 177). Rischia, pertanto, di risultare incompatibile con il diritto UE l'analisi indiscriminata dei dati di tutti i cittadini di Paesi di terzi che intendano attraversare le frontiere esterne dell'UE in assenza di alcun sospetto o comportamento che possa presentare un nesso, pur se indiretto o remoto, con attività terroristiche.

Dubbi di compatibilità con il diritto europeo dei nuovi sistemi di IA utilizzati nel campo della migrazione e l'asilo sorgono anche in riferimento al caso in cui questi vengano utilizzati per prendere decisioni in merito alle richieste presentate dai cittadini di Paesi terzi.

1.3. Sorveglianza biometrica digitale con sistemi di IA per prendere decisioni

Oltre ad essere utilizzati per verificare l'identità dei migranti, i sistemi di IA sono utilizzati anche per decidere sulle richieste presentate dai cittadini di Paesi terzi. L'art. 29 Working Party, ora Gruppo di Protezione Dati europeo, ha definito il "processo decisionale automatizzato" come la «capacità di prendere decisioni con mezzi tecnologici senza il coinvolgimento umano» (Art. 29 WP 2018) e negli ultimi anni si è fatto ricorso sempre più spesso a sistemi di IA per prendere decisioni in materia di richieste di immigrazione e asilo. Sulla base dei dati raccolti e inseriti nei database su larga scala europea, infatti, i sistemi di IA valutano tramite algoritmi il rischio per la sicurezza pubblica e per la salute pubblica o il pericolo di commissione di reati che un cittadino di un Paese terzo comporta (Molnar 2019), con conseguenze rilevanti circa la durata della detenzione amministrativa dei cittadini di Paesi terzi in attesa di accertamento. Tuttavia, nonostante le gravi ripercussioni sui diritti fondamentali che derivano dalle decisioni automatizzate prese per mezzo di sistemi di IA, la disciplina attuale, e in particolare quanto previsto nel Regolamento sull'IA, non sembra adeguata a tutelare i diritti fondamentali dei cittadini dei Paesi terzi.

2. Disciplina prevista nel Regolamento sull'IA nel settore dell'immigrazione e l'asilo

La disciplina prevista nel Regolamento sull'IA in materia di immigrazione e asilo risulta carente per una serie di motivi. In primo luogo, essa non si applica fino al 31 dicembre 2030 ai sistemi di IA che sono componenti di sistemi di IT su larga scala (Regolamento 2024/1689, art. 111, par. 1), ivi inclusi SIS, Eurodac, VIS, ETIAS, EES e ECRIS-TCN, nonché ai Regolamenti che prevedono l'interoperabilità degli stessi (Regolamento 2024/1689, Allegato X).

In secondo luogo, sono specificamente previste delle eccezioni nel settore della migrazione rispetto a quanto previsto in generale per i sistemi di IA ad alto rischio (Regolamento 2024/1689, art. 6). Un'eccezione importante in tal senso è rappresentata dall'esclusione di una necessaria «verifica separata da parte di almeno due persone fisiche» ai sistemi di IA ad alto rischio che sono utilizzati nel settore della migrazione, «qualora il diritto dell'Unione o nazionale ritenga sproporzionata l'applicazione del requisito» (Regolamento 2024/1689, art. 4, par. 5). Sarà, pertanto, la legislazione nazionale a stabilire se escludere o meno l'obbligo della verifica da parte di almeno due persone fisiche, dato che il Regolamento sull'IA non chiarisce in che situazioni questo requisito possa considerarsi sproporzionato o quali interessi debbano essere bilanciati (Brouwer 2024: 5).

Tuttavia, in assenza di controllo umano, i diritti fondamentali dei cittadini di Paesi terzi sono a rischio, considerato l'elevato tasso di errore rilevato nelle decisioni prese dagli algoritmi, spesso viziati, dei sistemi di IA. Sul punto, sebbene in altro ambito, la Corte ha affermato che, dato che le analisi automatizzate sono effettuate «a partire da dati personali non verificati e si fondano su modelli e criteri prestabiliti, le stesse presentano necessariamente un certo tasso d'errore» (Corte Parere 1/15, par. 169). Pertanto, qualsiasi risultato positivo che sia stato ottenuto grazie ad un trattamento automatizzato di tali dati, «deve essere sottoposto a un riesame individuale con strumenti non automatizzati prima dell'adozione di una misura individuale che produca effetti pregiudizievoli nei confronti dei [soggetti] interessati» (Corte Parere 1/15, par. 173). Del pari, il Regolamento Generale Protezione Dati (da ora innanzi RGPD) prevede che il titolare del trattamento dei dati abbia il diritto di non essere soggetto ad una decisione che si basi esclusivamente sul trattamento automatizzato dei dati, ivi inclusa la profilazione, nel caso questa produca effetti giuridici che lo riguardano o incidano in modo significativo sulla sua persona (Regolamento 2016/679, art. 22). L'eccezione prevista dal Regolamento sull'IA per cui non è necessario il controllo da parte di almeno due persone nel settore dell'immigrazione rischia, pertanto, di essere incompatibile con il diritto UE.

Inoltre, in base ad un'altra eccezione, i sistemi di IA ad alto rischio nel settore della migrazione e asilo sono registrati in una «sezione sicura non pubblica» della banca dati dell'UE accessibile solo da parte della Commissione e delle autorità nazionali competenti (Regolamento 2024/1689, art. 49, par. 4) e all'atto della registrazione non devono essere fornite e presentate certe informazioni importanti, quali il set di dati utilizzato per l'addestramento di sistemi di IA o un riassunto della valutazione dell'impatto sui diritti umani (Regolamento 2024/1689, art. 49, par. 4; Allegato VIII).

Queste eccezioni sanciscono l'assenza di trasparenza nell'uso dei sistemi di IA nel settore della migrazione e dell'asilo (Vavoula 2024: 1235). Inoltre, in base al Regolamento sull'IA, alcuni sistemi di IA ad alto rischio possono essere "declassati" a certe condizioni a meno che non siano sistemi che svolgono un'attività di profilazione (Regolamento 2024/1689, art. 6, par. 3).

A ciò si aggiunga che alcuni sistemi di IA utilizzati nel settore della migrazione e il controllo alle frontiere non sono inclusi nell'elenco dei sistemi di IA ad alto rischio. Tra questi vi sono i sistemi di IA che vengono utilizzati per monitorare, analizzare e prevedere tendenze migratorie e minacce per la sicurezza, che sono stati auspicati da Frontex per supportare operazioni coordinate alle frontiere esterne (Frontex 2021b), e che, come sottolineato dal Garante europeo per la protezione dei dati (EDPS 2019), possono creare rischi gravi per il diritto alla protezione dei dati personali e alla libertà di espressione dei soggetti interessati. Del pari, nonostante le gravi implicazioni per la privacy e le preoccupazioni circa la loro affidabilità, non sono definiti ad alto rischio i sistemi di IA utilizzati per estrarre dati dai cellulati e i sistemi di riconoscimento della lingua e del dialetto.

Al contrario, sono inseriti nell'elenco sistemi "come poligrafi o strumenti analoghi", già testati in progetti finanziati dall'UE quali *iBorderCtrl* e *Tresspass*, nonostante numerosi attori, tra cui l'EDPS e l'EDPB ritengano necessario vietare l'uso di detettori della verità in generale (EDPB-EDPS Joint Opinion 2021, par. 33).

Sono altresì ricompresi nella categoria dei sistemi ad alto rischio gli strumenti di IA utilizzati dalle autorità nazionali per verificare l'affidabilità delle richieste di asilo, come i sistemi di riconoscimento della lingua (Regolamento 2024/1689, Allegato III, par. 7, lett. c).

Nel Regolamento sull'IA sono inoltre previste delle pratiche di IA che devono essere vietate del tutto (Regolamento 2024/1689, art. 5). Tra di esse ce ne sono alcune che rilevano nel contesto della migrazione, tra cui, per esempio, il divieto di usare sistemi di IA per «valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione [di essa] o della valutazione dei tratti e delle caratteristiche della personalità» (Regolamento 2024/1689, art. 5, par. 1, lett. d), che è pertinente al caso di SIS o di VIS, in cui è permesso negare l'ingresso o il visto al cittadino di un Paese terzo se questo individuo è considerato una minaccia per la sicurezza interna. Secondo quanto previsto dal Regolamento sull'IA, tuttavia, tale decisione non potrebbe basarsi su una valutazione del rischio effettuata da sistemi di IA, a meno che la persona interessata sia già sospettata di voler commettere o aver commesso specifici reati sulla base di fatti oggettivi e verificabili (Regolamento 2024/1689, art. 5, par. 1, lett. d).

Una seconda pratica vietata riguarda i sistemi di IA che «creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso» (Regolamento 2024/1689, art. 5, par. 1, lett. e). In base a tale disposizione, pertanto, è vietato espandere le banche dati dei sistemi su larga scala esistenti mediante lo *scraping* non mirato di immagini facciali. È altresì vietato l'uso di sistemi di «categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale» (Regolamento 2024/1689, art. 5, par. 1, lett. g). Questa disposizione riprende la giurisprudenza della Corte di Giustizia, la quale ha stabilito che i modelli e criteri prestabiliti ai fini di un'analisi automatizzata volta a prevenire attività di terrorismo non possono essere fondati solo su dati sensibili, in quanto qualsiasi analisi automatizzata effettuata in funzione di modelli e criteri basati sul presupposto che l'origine etnica o un'altra delle caratteristiche sopra elencate potrebbero «di per se stesse e indipendentemente dal comportamento individuale di tale persona, essere rilevanti rispetto alla prevenzione del terrorismo» violerebbe gli articoli 7 e 8 della Carta (CGUE *La Quadrature du Net*, par. 181).

Infine, è vietato l'uso di «sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto», a meno che ciò sia

necessario per ricercare vittime specifiche di gravi reati o per prevenire «una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico» o a localizzare e identificare una persona sospettata di aver commesso un reato (Regolamento 2024/1689, art. 5, par. 1, lett. h). Questa disposizione riprende quanto affermato dalla Corte di Giustizia (CGUE *La Quadrature du Net*, par. 188), la quale aveva altresì ribadito che la raccolta in tempo reale dei dati risulta particolarmente grave in quanto comporta una «sorveglianza quasi totale degli utenti», fornendo alle «autorità nazionali competenti uno strumento di controllo preciso e permanente degli spostamenti degli utenti dei telefoni mobili» (CGUE *La Quadrature du Net*, par. 187).

È alla luce di tale disciplina e della giurisprudenza della Corte che occorre verificare la compatibilità con il diritto europeo, e in particolare con i diritti contenuti nella Carta, di uno degli strumenti di controllo mediante sistemi di IA più diffusi, ossia il sistema di riconoscimento facciale.

3. Riconoscimento facciale: aspetti problematici

Tra gli strumenti di controllo mediante sistemi di IA più diffusi alle frontiere esterne dell'UE vi è il sistema di riconoscimento facciale. Tramite quest'ultimo, nei punti di varco automatico alle frontiere è possibile riconoscere automaticamente, mediante la comparazione dell'immagine con altre prese come riferimento, se un determinato soggetto appartiene ad un determinato gruppo sulla base di specifiche caratteristiche del viso (FRA 2019:7-8).

La disciplina applicabile è quella dei dati biometrici, che sono considerati una categoria speciale di dati personali (Regolamento 2016/679, art. 9; Direttiva 2016/680, art. 10) e sono definiti come «i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici» (Regolamento 2016/679, art. 4, par. 14). Il riconoscimento facciale è altresì compreso nell'ambito di applicazione dell'art. 8 CEDU ed è il tipo di dato biometrico che viene raccolto più facilmente: a differenza delle impronte digitali, esso può infatti essere estratto da video effettuati da telecamere anche all'insaputa dei soggetti interessati.

Per quanto riguarda il diritto UE, la prima volta che si è menzionata la possibilità di ricorrere al riconoscimento facciale per verificare l'identità dei cittadini di Paesi terzi alle frontiere è stato con la banca dati EES (Regolamento 2017/2226, artt. 23, par. 2; 26), che si avvarrà anche di tecniche di *machine learning*/IA per il *biometric matching* (Eu-LISA 2020). Del pari, nell'ambito del SIS si prevede l'utilizzo del riconoscimento facciale per confermare l'identità di una persona, ma anche per identificare una persona quando attraversa regolarmente le frontiere dell'UE (Regolamento

2018/1861, art. 33, par. 4; Galbally Herrero *et al*. 2019), così come è possibile confermare l'identità di un cittadino di un Paese terzo nell'ambito di ECRIS-TCN (Regolamento 2019/816, art. 6). Per quanto riguarda Eurodac, il riconoscimento facciale è incluso per consentire comparazioni (Regolamento 2024/1358, art. 12, par. 1, lett. q). Infine, il Regolamento recentemente emendato di VIS prevede che sia possibile utilizzare i sistemi di riconoscimento facciale al momento della domanda di visto per verificare l'identità e consentire una comparazione (Regolamento 2021/1134, art. 22bis, par. 1, lett. j), benché questo non possa essere il solo criterio preso in considerazione (Regolamento 2021/1134, art. 20).

Al riguardo occorre notare che, nonostante i progressi occorsi negli ultimi anni, i sistemi di riconoscimento facciale, sono tuttora soggetti a molti errori e inaccuratezze (Israel 2020). Una conseguenza inevitabile è l'alto numero di falsi positivi o falsi negativi, ossia il numero elevato di associazioni non corrette tra immagini individuate dall'algoritmo. Questa rappresenta una grave violazione dei diritti di centinaia di persone, considerato che anche una percentuale bassa di errore come lo 0,01% assume una rilevanza importante se si considerano i grandi numeri e il fatto che sono utilizzati in spazi pubblici (Dumbrava 2021). Le conseguenze sono gravissime in quanto in caso di falsi positivi certe persone saranno segnalate per errore nel SIS, saranno soggette a controlli ulteriori e saranno considerate un potenziale pericolo per la sicurezza pubblica (Vavoula 2021).

Il tasso di errore dipende dall'inaccuratezza del riconoscimento, che a sua volta dipende dalla scarsa qualità delle immagini raccolte, che è un fattore che potrebbe ulteriormente aggravarsi a causa dell'interoperabilità delle banche dati poiché la quantità di dati di scarsa qualità raccolti in ognuna delle sei banche dati aumenterà esponenzialmente nel momento in cui esse saranno rese interoperabili (Vavoula 2021: 21). Al riguardo, non sembra sufficiente a tutelare i diritti dei cittadini di Paesi terzi il fatto di consentire ad eu-LISA di condurre controlli automatici sulla qualità dei dati, a meno che questa misura non sia affiancata all'obbligo da parte degli Stati membri di adeguarsi e rettificare o cancellare i dati che risultano errati entro specifici termini di scadenza (Regolamento 2018/1726, art. 12; Vavoula 2021: 21), o alla comminazione di sanzioni nel caso di violazioni persistenti (Vavoula 2021: 21).

Al fine di migliorare la qualità dei dati sarebbe altresì auspicabile imporre di utilizzare solo immagini del viso prese in certe specifiche condizioni piuttosto che utilizzare anche le immagini riprese dalle telecamere o ai *gate* elettronici in condizioni ambientali e di luce scarse. Sarebbe altresì necessario specificare in che momento deve essere scattata la fotografia e inserita nella banca dati. Nel caso di bambini, per esempio, l'apparenza fisica e i lineamenti del volto cambiano molto con il passare degli anni. È per questo motivo che è stato riscontrato un notevole peggioramento delle prestazioni di riconoscimento facciale nei confronti di bambini rispetto agli adulti. Tuttavia, considerato che le nuove regole previste per Eurodac e VIS prevedono di abbassare l'età in cui prelevare i campioni biometrici a sei anni, queste preoccupazio-

ni aumentano.

Un altro aspetto da considerare è che, anche se queste tecnologie fossero perfettamente accurate e affidabili, esse rappresenterebbero comunque uno strumento per registrare le immagini di un numero elevatissimo di persone all'interno delle banche dati europee su larga scala ed effettuare un controllo generalizzato di massa (Israel 2020). I cittadini di Paesi terzi e in generale tutti coloro che viaggiano corrono, infatti, il rischio di essere classificati e identificati quali possibili sospetti di attività terroristiche o altri gravi crimini transnazionali (Statewatch 2020). I dati raccolti nelle banche dati europee potrebbero, inoltre, essere utilizzati in altri contesti a fini di sorveglianza. Questo rappresenta una deriva inammissibile dato che è stato più volte ribadito che una legislazione che consenta la raccolta indiscriminata di dati di individui verso cui non esiste alcun indizio di colpevolezza è incompatibile con il diritto europeo (CGUE *La Quadrature du Net*, par. 174; EDPS Opinion 2024).

3.1. Violazione degli articoli 7 e 8 della Carta

Secondo quanto previsto dal diritto europeo, il trattamento dei dati personali, e in particolare dei dati biometrici, è consentito solo ove strettamente necessario e proporzionato agli obiettivi perseguiti, come è stato precisato anche dal Garante europeo della protezione dei dati personali in un Parere del 2024 (EDPS Opinion 2024), in cui ha precisato che il nuovo sistema di identificazione automatizzato tramite impronte digitali e le nuove funzionalità per ricercare dati biometrici nelle banche dati europee richiedono un controllo rafforzato circa la stretta necessità e la proporzionalità delle misure attuate (EDPS Opinion 2024, parr. 14-18).

Sul punto anche la giurisprudenza della Corte ha ribadito la necessità di un controllo rafforzato, che deve affiancarsi ad una valutazione dei «modelli» e dei «criteri prestabiliti», nonché delle banche dati, su cui si basano le «analisi automatizzate dei dati» (Corte, Parere 1/15, par. 172). In particolare, affinché sia rispettato il diritto UE, e in particolare gli articoli 7 e 8 della Carta, il controllo automatizzato dei dati può, ad avviso della Corte, essere considerato proporzionato solo se i modelli e i criteri prestabiliti sono «specifici e affidabili» in relazione a individui «sui quali potrebbe gravare un sospetto ragionevole di partecipazione a reati di terrorismo o a reati gravi di natura transnazionale», e solo se non sono discriminatori. Del pari, nel caso in cui si effettuino controlli incrociati di dati, le banche dati devono essere affidabili e aggiornate, tenuto conto dei dati statistici e delle ricerche compiute a livello internazionale (Corte, Parere 1/15, par. 174). Inoltre, è necessario il riesame individuale da parte di un essere umano prima dell'adozione di una misura individuale (CGUE *La Quadrature du Net*, par. 182) ed è necessario che «il provvedimento che autorizza l'analisi automatizzata [possa] 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» (CGUE *La Quadrature du Net*, par. 179).

I principi enunciati dalla Corte si applicano anche in un caso in cui il rischio di violazione dei diritti fondamentali di cui agli articoli 7 e 8 della Carta risulta ancora più accentuato, ossia l'interoperabilità dei database europei. Se ogni singolo dato immesso in un determinato sistema non rivela, infatti, molto dell'individuo a cui si riferisce il dato, al contrario, i dati raccolti in tutti i database comparati e combinati tra loro possono rivelare o far dedurre i percorsi scelti per viaggiare, le abitudini di viaggio, le relazioni sentimentali tra soggetti, la situazione finanziaria e le condizioni di salute dei viaggiatori (EDPS Opinion 2017; Corte, Parere 1/15, par. 128). Ciononostante, al momento l'individuazione di identità multiple da parte del MID e la valutazione del rischio di una certa persona compiuta da ETIAS sono eseguite sistematicamente nei confronti di tutti coloro i cui dati sono inseriti nei database pur in assenza di alcun valido motivo per sospettare che una certa persona rappresenti un rischio per la sicurezza pubblica o utilizzi una falsa identità.

La disciplina attuale si configura, pertanto, come un controllo indiscriminato verso tutti i viaggiatori, in quanto tale incompatibile con il diritto UE, e in particolare con gli articoli 7 e 8 della Carta, così come interpretati dalla Corte di Giustizia nella sua costante giurisprudenza (CGUE *Ligue des droits humains*, parr. 98, 102).

3.2. Diritto di accesso, di rettifica, di cancellazione e diritto ad un rimedio giurisdizionale effettivo

L'articolo 8 della Carta prevede altresì che «ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica» (Carta, art. 8, par. 2) e ha il diritto al controllo da parte di un'autorità indipendente (Carta, art. 8, par. 3; Ward 2021). Del pari, il soggetto interessato ha diritto ad una buona amministrazione (Carta, art. 41) e a un rimedio giurisdizionale effettivo (Carta, art. 47). Ogni individuo ha, dunque, il diritto di impugnare le decisioni prese nei suoi riguardi, così come quello di ottenere le informazioni e i dati sulla cui base le decisioni sono state adottate (CGUE, *ZZ*, par. 53).

La trasparenza delle informazioni concernenti i soggetti interessati e il diritto di accesso di questi ultimi ai dati raccolti sono requisiti essenziali per l'esercizio del diritto ad un rimedio giurisdizionale effettivo (CGUE *Ligue des droits humains,* par. 210; EDPS Opinion 2017, par. 79; CGUE *Maximilian Schrems*, par. 95). Tuttavia, nel caso delle decisioni prese sulla base dei dati conservati nei database europei, il problema maggiore consiste proprio nella mancanza di trasparenza delle decisioni, così come delle informazioni che i soggetti interessati possono ottenere esercitando il proprio diritto di accesso, rettifica e cancellazione dei dati (Regolamento 2016/679, art. 13, par. 2, lett. b; Regolamento 2019/817, artt. 48-49; Regolamento 2019/818, artt. 48-49). Le informazioni che i soggetti interessati possono ottenere esercitando questi diritti non riflettono infatti la situazione registrata nei database, dato che i criteri utilizzati per prendere le decisioni non sono trasparenti a causa dei complicati meccanismi che li sottendono (Pesch/Boehm 2024: 178). Questo rischia di ledere il

diritto degli individui interessati ad esercitare i propri diritti.

Sia nel caso in cui una persona fisica sia oggetto di un "collegamento rosso" in base a quanto stabilito nel Regolamento sull'interoperabilità (Regolamento 2019/817 artt. 32, par. 1), che nel caso di rifiuto, revoca o annullamento di un'autorizzazione di viaggio nel sistema ETIAS, il soggetto interessato potrà, infatti, conoscere il contenuto della decisione finale, ma non i motivi che hanno portato l'autorità competente a prendere questa decisione (EDPS Opinion 2017, par. 78). Lo stesso accade nella procedura di pre-ingresso istituita in forza del nuovo Patto sulla Migrazione e l'Asilo, in cui si prevede che in seguito agli accertamenti debba essere compilato da parte delle autorità competenti un modulo consuntivo, che sarà poi trasmesso alle autorità competenti a seconda della procedura a cui è indirizzato il cittadino di Paese terzo (Regolamento 2024/1356, artt. 17-18). Il modulo consuntivo rappresenta il documento essenziale sulla cui base sarà successivamente deciso se un determinato individuo sarà sottoposto ad una procedura di frontiera di protezione internazionale o di rimpatrio nel paese di origine (Regolamento 2024/1356, artt. 17-18). Tuttavia, benché le informazioni contenute nel modulo siano messe a disposizione della persona interessata, non è comunicato al soggetto interessato se la «consultazione delle banche dati pertinenti […] abbia dato riscontro positivo» (Regolamento 2024/1356, art. 17, par. 3). Non si ravvisa, pertanto, trasparenza nel trattamento dei dati conservati e processati nelle banche dati europee.

La motivazione che viene addotta è l'interesse alla segretezza, che, tuttavia, dovrebbe essere bilanciato con il diritto individuale alla trasparenza (CGUE *Ligue des droits humains*, par. 195; Corte, Parere 1/15, par. 220) e con i diritti sopra menzionati, che devono essere interpretati alla luce delle disposizioni della Carta e della giurisprudenza della Corte. Nel GDPR e nell'EUDPR è previsto che i soggetti interessati devono essere informati se sono stati oggetto di una decisione automatizzata, inclusa la profilazione, e almeno in tal caso devono essere fornite informazioni rilevanti per quanto riguarda la logica seguita per prendere la decisione e le conseguenze per il soggetto interessato. Il fatto che la logica sottesa alle decisioni debba essere spiegata "almeno in quei casi" evidenzia che essa possa essere spiegata anche in altri casi (Barros Vale/Zanfir-Fortuna 2022: 18; Malgieri/Comandé 2017), come nel caso dei database europei, in cui sarebbe auspicabile, date le interferenze gravi con i diritti di cui agli articoli 7 e 8 della Carta (Pesch/Boehm 2024: 180).

Le regole vigenti a livello generale dovrebbero, pertanto, applicarsi anche nel settore della migrazione per garantire che i diritti fondamentali dei cittadini di Paesi terzi riconosciuti dalla Carta, così come interpretati dalla Corte di Giustizia, siano tutelati.

3.3. Violazione del principio di non discriminazione e profilazione etnica

Gli algoritmi utilizzati dai sistemi di IA per il riconoscimento facciale, in base a studi recenti, inoltre, sono discriminatori nei confronti di specifici gruppi demografici (Drozdowski *et al*. 2020) e producono un numero più elevato di corrispondenze errate positive nei confronti di persone di colore, e soprattutto nei confronti di donne di colore (NIST 2019). Questo comporta una grave violazione del principio di non discriminazione.

Nel caso in cui vengano utilizzati questi sistemi alle frontiere esterne dell'UE è, infatti, più elevato il rischio che siano segnalate erroneamente e discriminate certe categorie di soggetti, con la conseguenza che saranno soggette a controlli più invasivi e a pratiche discriminatorie sul territorio nazionale, oltre a rischiare di vedersi rigettata la richiesta di ingresso sul territorio nazionale a causa di errori commessi dagli algoritmi dei sistemi di riconoscimento facciale. I sistemi di IA sono, infatti, addestrati con dati discriminatori da parte di società esterne, che oltretutto tengono segreti sia il modello di addestramento che i set di dati su cui sono addestrati i modelli (Pesch/Dimitrova/Boehm 2022: 64). Il perpetuarsi delle discriminazioni comporta, inoltre, il rischio che previe decisioni discriminatorie influenzino gli indicatori di rischio e in tal modo perpetuino le discriminazioni in un ciclo destinato a ripetersi (FRA 2022). Al riguardo, eu-LISA ha proposto due diverse soluzioni: o l'uso di set di dati rappresentativi di quella parte della popolazione per addestrare gli algoritmi o la creazione di un set di dati artificiali che riproducano le caratteristiche rappresentative di quella parte della popolazione (eu-LISA 2020). Nessuna delle due alternative proposte sembra, tuttavia, soddisfacente. La prima, infatti, è preoccupante per quanto riguarda la tutela del principio di finalità del trattamento dei dati e il principio di "minimizzazione dei dati", a seconda della dimensione dei set di dati utilizzati per addestrare gli algoritmi. La seconda soluzione potrebbe comportare soglie di errore ancora maggiori a causa dell'utilizzo di dati artificiali (Regolamento 2024/1689, Considerando 133; Dumbrava 2021).

Un accorgimento assolutamente necessario consiste, invece, nel monitorare previamente il funzionamento dei sistemi di IA al fine di evitare pregiudizi e discriminazioni, nonché la violazione dei diritti fondamentali dei soggetti coinvolti. Sarebbe altresì opportuno garantire l'accuratezza dei dati che sono comparati (Corte, Parere 1/15, parr. 169, 172; CGUE *La Quadrature du Net*, par. 180). Molti errori derivano, infatti, dalla scarsa qualità dei dati nei database (FRA 2018: 83ss.).

Affinché le decisioni su ogni caso di specie siano prese in modo oggettivo e non discriminatorio senza fare affidamento sul risultato ottenuto tramite gli algoritmi di IA (Goddard/Roudsari/Wyatt 2012), occorre, inoltre, garantire il controllo di ogni singolo caso da parte di un essere umano (Regolamento 2016/679, art. 22, par. 1; EUDPR, art. 24, par. 1; LED, art. 11, par. 1; CGUE *Ligue des droits humains*, par. 179; CGUE *La Quadrature du Net*, par. 182) e prevedere che gli individui che andranno a controllare le decisioni automatizzate abbiano seguito un addestramento specifico

(EDPB-EDPS Joint Opinion 2021, par. 59). Come è stato sottolineato dalla Corte, infatti, è necessario che la persona fisica che controlla la decisione sia stata specificamente addestrata e sia, quindi, in grado di capire il ragionamento di modelli spesso non trasparenti che danno luogo a risultati non facilmente interpretabili o spiegabili (CGUE *Ligue des droits humains*, par. 194).

L'uso di sistemi di IA nel settore della migrazione richiederebbe pertanto una base giuridica specifica che preveda ulteriori specifiche misure di salvaguardia (Pesch/Boehm 2024: 174). Inoltre, nel caso in cui siano utilizzati sistemi di AI, il Regolamento sull'IA dovrebbe applicarsi senza eccezioni al fine di garantire il controllo umano e una trasparenza sufficiente agli utilizzatori finali (Statewatch 2022). Tuttavia, garanzie di tal genere non sono previste né nella legislazione esistente concernente le banche dati né nella disciplina prevista nel Nuovo Patto sulla Migrazione e l'Asilo, che prevede l'obbligo di svolgere i controlli e gli accertamenti in soli sette giorni (Regolamento 2024/1356, art. 8, par. 3). Questa riduzione dei tempi, considerato il lasso temporale che viene impiegato attualmente per effettuare gli accertamenti (Lücke *et al.* 2021), potrebbe, tuttavia, portare gli Stati membri a diminuire ulteriormente la qualità degli accertamenti e a indurre le autorità competenti ad effettuare accertamenti sulla base di pregiudizi (cosiddetto *racial profiling*). Inoltre, aumenta il rischio che non vengano fornite in modo esauriente ai richiedenti protezione internazionale tutte le informazioni necessarie per preparare adeguatamente i loro fascicoli, con quello che ne consegue in termini di buona riuscita della procedura (Tsourdi 2024: 9).

4. Conclusioni

Dall'analisi che precede si desume che sia le dichiarazioni politiche che gli atti legislativi adottati dall'UE hanno l'obiettivo di tutelare la sicurezza dell'UE, più che quello di garantire un sistema di protezione dei cittadini di Paesi terzi. La prevenzione del terrorismo e di altri gravi reati transnazionali è diventato l'obiettivo principale da raggiungere e le nuove tecnologie e i sistemi di IA sono stati considerati uno strumento fondamentale per raggiungere tale obiettivo. In tale ottica, l'ambito di applicazione delle banche dati europee su larga scala già esistenti è stato ampliato, ne sono state create delle nuove ed è stata prevista l'interoperabilità delle stesse.

Il sempre maggiore utilizzo di sistemi di IA quali i sistemi di riconoscimento facciale e gli altri sistemi di sorveglianza biometrica non è stato, tuttavia, accompagnato da una disciplina idonea a tutelare i diritti dei cittadini di Paesi terzi che intendano attraversano le frontiere esterne dell'UE. Al contrario, i diritti di questi ultimi rischiano di essere violati in maniera ancora più grave, nonostante la costante giurisprudenza della Corte di Giustizia riguardo agli articoli 7 e 8 della Carta.

L'uso di questi sistemi, infatti, in primo luogo, comporta il rischio di un alto tasso di errore, ossia di un alto numero di falsi positivi o falsi negativi, con gravi con-

seguenze per i migranti. Alcune persone potrebbero, infatti, essere erroneamente trattenute per più tempo del dovuto in stato di detenzione amministrativa ed essere soggette a controlli serrati, mentre altre potrebbero essere rimpatriate nel Paese di origine. L'eccezione prevista nel Regolamento sull'IA per cui in alcuni casi è possibile omettere il controllo delle decisioni automatizzate da parte di almeno due persone fisiche in ambito di migrazione rende ancora più grave la situazione e più alto il rischio che i diritti dei cittadini di Paesi terzi vengano violati.

In secondo luogo, l'uso di modelli non trasparenti che danno luogo a risultati non facilmente interpretabili o spiegabili rischia di violare il diritto a proporre un ricorso avverso la decisione che li riguarda, di cui agli articoli 8 e 47 della Carta, in quanto l'assenza di trasparenza in merito ai criteri e ai motivi che hanno portato le autorità competenti a prendere le proprie decisioni sulla base degli output dei sistemi di IA in materia di immigrazione rende difficile se non impossibile per i soggetti interessati proporre ricorso avverso la decisione che li riguarda.

Per quanto riguarda il principio di non discriminazione, inoltre, l'uso di sistemi di IA di riconoscimento facciale configura il rischio di profilazione etnica, ossia il rischio che certe categorie di soggetti, e in particolare donne di colore, siano discriminate. A ciò si aggiunga, infine, che, pur in assenza di errori da parte degli algoritmi dei sistemi di IA, l'uso di questi sistemi di sorveglianza sottopone tutti i viaggiatori che intendano entrare nel territorio dell'UE ad una forma molto invasiva di controllo assimilabile ad una forma di sorveglianza di massa incompatibile con il diritto UE in base alla giurisprudenza della Corte di Giustizia.

In conclusione, quindi, l'uso dei sistemi di IA non solo non ha contribuito a migliorare la tutela dei diritti dei cittadini di Paesi terzi, ma, al contrario, rischia di comportare una violazione grave dei diritti di tutti i viaggiatori che intendano attraversare le frontiere esterne dell'UE con indebite ingerenze nella sfera della *privacy* dei singoli individui, mancata protezione dei dati personali di questi ultimi e della libertà di movimento di tutti. A nostro avviso, bisogna, pertanto, chiederci in che società desideriamo vivere e porci le seguenti domande: fino a che punto è giustificata un'analisi basata su fattori sconosciuti (*black box*) in cui non sono previste tutele adeguate per i cittadini di Paesi terzi, specialmente in assenza di controllo umano e nel caso in cui si utilizzino strumenti che non ricadono nella disciplina del Regolamento sull'IA? Fino a che punto le esigenze di sicurezza possono giustificare una tale compressione e violazione dei diritti fondamentali dei cittadini dei Paesi terzi e di tutti i viaggiatori? In che modo è giustificabile in un'"Unione di diritto"?

BIBLIOGRAFIA

Art. 29 WP 2013= Article 29 Data Protection Working Party 2013, *Opinion 03/2013 on purpose limitation*, Doc. 00569/13/EN, WP 203, del 2 aprile 2013.

Art. 29 WP 2018= Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251, 6 febbraio 2018.

Barros Vale/Zanfir-Fortuna 2022 = Sebastião Barros Vale/Gabriela Zanfir-Fortuna, *Automated Decision- Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities*, consultabile all'indirizzo https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf.

Besters/Brom 2010= Michiel Besters/Frans W.A. Brom, *"Greedy" Information Technology: the Digitalization of the European Migration Policy*, in «European Journal of Migration and Law», 4, 12.

Brouwer 2011 = Evelien Brouwer, *Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation*, in Leonard Besselink/Frans Pennings/Sacha Prechal (a cura di), *The Eclipse of the Legality Principle in the European Union*, Alpen aan den Rijn, Kluwer Law International, pp. 273-294.

Brouwer 2024 = Evelien Brouwer, *EU's AI Act and Migration Control. Shortcomings in Safeguarding Fundamental Rights*, 12 dicembre 2024, «verfassungsblog.de».

CGUE causa C-518/07 = Corte di Giustizia, del 9 marzo 2010, *European Commission v Federal Republic of Germany*, causa C- 518/07.

CGUE causa C-614/10 = Corte di Giustizia, del 16 ottobre 2012, *European Commission v Republic of Austria*, causa C-614/10.

CGUE *ZZ* = Corte di Giustizia, del 4 giugno 2013, *ZZ v Secretary of State for the Home Department,* causa C-300/11.

CGUE *Maximilian Schrems* = Corte di Giustizia, del 6 ottobre 2015, *Maximillian Schrems v Data Protection Commissioner*, causa C- 362/14.

CGUE *La Quadrature du Net* = Corte di Giustizia, del 6 ottobre 2020, *La Quadrature du Net e a. contro Premier ministre e a.*, cause riunite C-511/18, C-512/18 e C-520/18.

CGUE *Ligue des droits humains* = Corte di Giustizia, del 21 giugno 2022, *Ligue des droits humains ASBL v Conseil des ministers*, causa C-817/19.

CGUE C-205/21= Corte di Giustizia, del 26 gennaio 2023, *Ministerstvo na vatreshnite raboti (Biometric and genetic data registration by the police*), causa C-205/21.

Commissione 2005= Commissione europea, *Biometrics at the frontiers: Assessing the impact on society*, consultabile all'indirizzo https://op.europa.eu/en/publication-detail/-/publication/cd472dc6-4298-441c-92ec-7307811bb479/language-en.

COM 2024/570 = Commissione, Comunicazione dell'11 dicembre 2024, sul contrasto alle minacce ibride causate dall'uso della migrazione come arma e sul rafforzamento della sicurezza alle frontiere esterne dell'UE, COM/2024/570 final.

Drozdowski *et al*. 2020 = Pawel Drozdowski, Christian Rathgeb, Antitza Dantcheva, Naser Damer, Christoph Busch, *Demographic Bias in Biometrics: A Survey on an Emerging Challenge*, in «IEEE Transactions on Technology and Society», 1, 2.

Dumbrava 2021= Costica Dumbrava, *Artificial Intelligence at EU borders, Overview of applications and key issues*, «European Parliament Research Service», luglio 2021.

EDPS Opinion 2016 = European Data Protection Supervisor, *Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)*, Opinion 07/2016, del 21 settembre 2016.

EDPS Opinion 2017 = European Data Protection Supervisor, *Opinion 3/2017 on the Proposal for a European Travel Information and Authorisation System (ETIAS)*, Opinion 3/2017.

EDPS 2019 = European Data Protection Supervisor, *Formal consultation on EASO's social media monitoring reports (case 2018-1083)* consultabile online all'indirizzo https://www.edps.europa.eu/sites/default/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf.

EDPB-EDPS Joint Opinion 2021 = European Data Protection Board (EDPB) - European Data Protection Supervisor (EDPS) Joint Opinion 5/ 2021 *on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 giugno 2021.

EDPS Opinion 2024 = European Data Protection Supervisor, *Opinion on the Proposal for a Regulation on enhancing police cooperation in relation to the prevention, detection and investigation of migrant smuggling and trafficking in human beings, and on enhancing Europol's support to preventing and combating such crimes and amending Regulation (EU) 2016/794*, Opinion 4/2024, 23 gennaio 2024.

EUDPR = Regolamento (UE) 2018/1725, del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati.

Eu-LISA 2020 = Eu-LISA, *Artificial Intelligence in the Operational Management of Large-scale IT Systems,* https://op.europa.eu/en/publication-detail/-/publication/6173f7a8-d78a-11ea-adf7-01aa75ed71a1.

FRA 2018 = European Union Agency For Fundamental Rights, *Under Watchful Eyes: Biometrics, EU IT systems and Fundamental Rights*, «Publications Office of the European Union».

FRA 2019= European Union Agency For Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, «Publications Office of the European Union».

FRA 2022 = European Union Agency for Fundamental Rights (FRA), *Bias in Algorithms, Artificial Intelligence and Discrimination - Report,* «Publications Office of the European Union», file:///Users/costanzadfm/Downloads/fra-2022-bias-in-algorithms_en.pdf.

Frontex 2021a = Frontex, *Single Programming Document 2022-2024*, consultabile online https://www.frontex.europa.eu/assets/Key_Documents/Programming_Document/2022/Single_Programming_Document_2022_2024.pdf.

Frontex 2021b = Frontex, Artificial Intelligence - Based Capabilities for the European Border and Coast Guard, Final Report consultabile online all'indirizzo: https://www.frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf.

Galbally Herrero *et al.* 2019= Javier Galbally Herrero, Pasquale Ferrara, Rudolf Haraksim, Apostolos Psyllos, *Study on Face Identification Technology for its Implementation in the Schengen Information System*, «Publications Office of the European Union», file:///Users/costanzadfm/Downloads/sis_face-jrc_science_for_policy_report_22.07.2019_final.pdf.

Goddard/Roudsari/Wyatt 2012 = Kate Goddard/Abdul Roudsari/Jeremy C Wyatt, *Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators*, in «Journal of the American Medical Informatics Association», 19, 1.

Israel 2020 = Tamir Israel, *Facial Recognition at a Crossroads: Transformation at our Borders and Beyond*, «Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)».

Hayes 2009 = Ben Hayes, *NeoConOpticon: The EU Security-Industrial Complex*, in «Transnational Institute/Statewatch», https://www.statewatch.org/media/documents/analyses/neoconopticon-report.pdf.

LED = Direttiva (UE) 2016/680 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.

Lücke *et al.* 2021 = Matthias Lücke/ Alberto-Horst Neidhardt/ Martin Ruhs/ Saime Özçürümez/ Olivia Sundberg Diez, *2021 MEDAM Assessment Report on Asylum and Migration Policies in*

Europe. The EU and Turkey: Toward sustainable cooperation in migration management and refugee protection, https://www.econstor.eu/bitstream/10419/243291/1/1762498014.pdf.

Malgieri/Comandé 2017 = Gianclaudio Malgieri/Giovanni Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in «International Data Privacy Law», 7, 4, p. 250 ss.

Marinai 2020= Simone Marinai, *Il rafforzamento del controllo digitale nel nuovo Patto sulla migrazione e l'asilo*, in «i Post di AISDUE, Focus, La proposta di Patto su immigrazione e asilo», 8.

Mitsilegas 2007 = Valsamis Mitsilegas, *Border Security in the European Union. Towards Centralised Controls and Maximum Surveillance*, in Elspeth Guild/Helen Toner / Anneliese Baldaccini (a cura di), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, Hart Publishing, pp. 359-394.

Mitsilegas 2011 = Valsamis Mitsilegas, *Human Rights, Terrorism and the Quest for "Border Security"*, in Marco Pedrazzi/Ilaria Viarengo / Alessandra Lang (a cura di), *Individual Guarantees in the European Judicial Area in Criminal Matters*, Bruylant.

Mitsilegas 2024 = Valsamis Mitsilegas, *Reconceptualising Security in the Law of the European Union*, in «European Papers», 9, 3, pp. 1438-1473.

Molnar 2019 = Petra Molnar, *Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective*, in «Cambridge International Law Journal», 8, 2.

NIST 2019 = National Institute for Standards and Technology (NIST), Patrick Grother/Mei Ngan/Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf.

Ozkul 2023= Derya Ozkul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*, «Refugee Studies Centre», University of Oxford, Oxford, consultabile all'indirizzo https://www.hertie-school.org/fileadmin/2_Research/1_About_our_research/2_Research_centres/Centre_for_Fundamental_Rights/AFAR/Automating-immigration-and-asylum_Ozkul.pdf.

Pesch/Dimitrova/Boehm 2022 = Paulina Jo Pesch/Diana Dimitrova/Franziska Boehm, *Data Protection and Machine- Learning- Supported Decision- Making at the EU Border - ETIAS Profiling Under Scrutiny*, in «Proceedings of the 10th Annual Privacy Forum» (APF 2022).

Pesch, Boehm 2024 = Paulina Jo Pesch/Franziska Boehm, *Smart Border is Watching You!*, in Herwig C.H. Hofmann/Felix Pflücke (a cura di), *Governance of Automated Decision- Making and EU Law*, Oxford, Oxford University Press.

Regolamento 767/2008= Regolamento (CE) 767/2008, 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 (Regolamento VIS), modificato da Regolamento 2021/1134, del 7 luglio 2021, da Regolamento 2021/1152, del 7 luglio 2021 e da Regolamento 2023/2667, del 22 novembre 2023.

Regolamento 603/2013 = Regolamento (UE) n. 603/2013, del 26 giugno 2013, che istituisce l'«Eurodac» per il confronto delle impronte digitali.

Regolamento 2016/679= Regolamento (UE) 2016/679, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Generale sulla Protezione dei Dati, o RGPD).

Regolamento 2017/2226= Regolamento (UE) 2017/2226, 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.

Regolamento 2018/1240 = Regolamento (UE) 2018/1240 del 12 settembre 2018 che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (Regolamento ETIAS).

Regolamento 2018/1726 = Regolamento (UE) 2018/1726 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).
Regolamento (UE) 2018/1860 = Regolamento (UE) 2018/1860, 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 = Regolamento (UE) 2018/1861, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera.
Regolamento (UE) 2018/1862 = Regolamento (UE) 2018/1862, 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.
Regolamento 2019/816 = Regolamento (UE) 2019/816 del 17 aprile 2019 che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, da ultimo modificato dal Regolamento (UE) 2021/1151, del 7 luglio 2021.
Regolamento 2019/817 = Regolamento (EU) 2019/817, del 20 maggio 2019, che istituisce in quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti (*EIF Border Regulation*).
Regolamento 2019/818 = Regolamento (EU) 2019/818 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 (*EIF LE Regulation*).
Regolamento 2019/1896= Regolamento (UE) 2019/1896, del 13 novembre 2019, relativo alla guardia di frontiera e costiera europea.
Regolamento 2021/1134= Regolamento (UE) 2021/1134, del 7 luglio 2021, ai fini della riforma del sistema di informazione visti.
Regolamento 2024/1356 = Regolamento (UE) 2024/1356, del 14 maggio 2024, che introduce accertamenti nei confronti dei cittadini di paesi terzi alle frontiere esterne.
Regolamento 2024/1358 = Regolamento (UE) 2024/1358, del 14 maggio 2024, che istituisce l'«Eurodac» per il confronto dei dati biometrici 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.
Regolamento 2024/1689= Regolamento (UE) 2024/1689, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (Regolamento sull'Intelligenza Artificiale).
Statewatch 2020 = Statewatch, *Automated suspicion: The EU's new travel surveillance initiatives*, consultabile all'indirizzo https://www.statewatch.org/media/1235/sw-automated-suspicion-full.pdf.
Statewatch 2022 = Statewatch, *Joint Statement: The EU Artificial Intelligence Act Must Protect People on the Move*', consultabile all'indirizzo: https://www.statewatch.org/news/2022/december/joint-statement-the-eu-artifical-intelligence-act-must-protect-people-on-the-move/
Tsourdi 2024 = Evangelia Lilian Tsourdi, *The New Screening and Border procedures: towards a seamless migration process?*, in «Policy Study», giugno 2024, consultabile all'indirizzo https://epc-web-s3.s3.amazonaws.com/content/FEPS-Policy_Study_-_The_New_Screening_and_Border_Procedure_-_DP_66__9_.pdf.
Vavoula 2021 = Niovi Vavoula, *Artificial Intelligence (AI) at EU Borders: From Automated Processing to Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism*, in «European Journal of Migration Law», consultabile all'indirizzo: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3950389.
Vavoula 2022 = Niovi Vavoula, *Immigration and Privacy in the Law of the European Union – The Case of Information Systems*, Brill Nijhoff.
Vavoula 2024 = Niovi 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», 9, 3, pp. 1228-1249.
Palmiotto/Ozkul 2023 = Francesca Palmiotto/Derya Ozkul, *"Like Handing My Whole Life Over" The German Federal Administrative Court's Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures*, in «Verfassungsblog», 28 febbraio 2023, consultabile all'indirizzo: https://verfassungsblog.de/like-handing-my-whole-life-over/.
Ward 2021 = Angela Ward, *Article 8*, in Steve Peers *et al.* (a cura di), *The EU Charter of Fundamental Rights - A Commentary,* seconda edizione, Bloomsbury.