La disciplina dei dati biometrici nella gestione dei flussi migratori: nuove prospettive alla luce del "Patto sulla migrazione e l'asilo"

di Rossella Benassai

Abstract: *The regulation of biometric data in the management of migration flows: new perspectives in light of the "New pact on migration and asylum"* – The purpose of this paper is to examine the implications for the protection of rights arising from the increasing use of new digital technologies for the regulation of migration flows entering the European Union, especially considering the adoption of the "New Pact on Migration and Asylum". The collection of biometric data is currently carried out using databases linked by the requirement of interoperability, however, there is no shortage of critical issues encountered with respect to a proper balance between data sharing and the protection of confidentiality and privacy, therefore, the securitarian logic pursued by Europe at the expense of the fundamental rights of third-country nationals subject to control is emphasized.

Keywords: Biometric data; Migratory flows; GDPR; Comparative perspectives; Securitarian logic

1. Premessa

La creazione di mezzi di riconoscimento sempre più sofisticati, oramai affidata prevalentemente a procedure biometriche precise e dettagliate, ha un'incidenza molto importante sull'individuazione e sulla raccolta dei dati personali di soggetti specifici e, di conseguenza, sul concetto stesso di identità che diviene il legame intrinseco tra le caratteristiche personali e diritti fondamentali[1].

Secondo quanto precisato all'art. 4 n. 14 del regolamento (UE) 2016/679 (GDPR)[2], i dati biometrici sono «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»[3].

[1] Corte Suprema indiana, Giudice D. Chandrachud, *Justice Puttaswamy v. Union of India*, 26-09-2018 (D.N. 35071/2012), par. 179.

[2] Reg. UE n. 679/2016 del P.E e del Cons. del 27-04-2016.

[3] Art. 9 reg. UE n. 679/2016, cit., in cui si introduce un generale divieto di trattamento di questa particolare categoria di dati, compresi i dati biometrici. Sono previste solo alcune eccezioni, tassativamente indicate quando il trattamento è necessario: «assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale; (…) motivi di interesse

DPCE online
ISSN: 2037-6677

Queste informazioni sono largamente utilizzate in diversi settori, tra cui quello della gestione dei flussi migratori, tematica di grande rilievo e di estrema attualità che ha subito recenti modifiche a seguito della adozione del nuovo "Patto sulla migrazione e l'asilo"[4].

In generale, lo scopo per cui i *data* sono richiesti ai migranti che valicano le frontiere è quello di "difendere" i confini europei (e quindi anche nazionali). In particolare, attraverso la raccolta dei dati si procede ad autorizzare o vietare l'accesso nell'Unione Europea: i) ai soggetti che richiedono la protezione internazionale (i richiedenti asilo), i quali non necessitano di un visto prima del loro arrivo in territorio comunitario, ii) a coloro che accedono alle frontiere con la qualifica di irregolari poiché non rientrano nei parametri di cui all'art. 6 del codice Schengen, iii) ai soggetti *extra* UE dotati di un visto temporaneo.

Al fine di raccogliere e conservare le informazioni personali dei migranti innanzi indicati, sono state predisposte apposite banche dati oltre a sistemi di controllo di frontiera automatizzati di natura *self-service*[5] nelle zone di confine in grado di comunicare tra di loro per rendere accessibili, alle autorità nazionali, informazioni sicure e affidabili, prevenendo molteplici rischi.

In detto contesto occorre esaminare dapprima quali sono le banche dati attualmente utilizzate a livello di Unione Europea, la loro disciplina e il loro funzionamento, per poi analizzare come il nuovo "Patto sulla migrazione e l'asilo" potrà incidere sulle stesse e sui sistemi connessi. Quest'ultimo ha, infatti, introdotto il requisito della interoperabilità tra diversi *database*, creando così un *file rouge* che lega lo scambio di informazioni.

È evidente che soprattutto nel settore migratorio, caratterizzato dalla posizione di squilibrio tra le parti che forniscono e quelle che detengono tali dati, potrebbero sorgere numerosi problemi relativi alla tutela dei diritti fondamentali, ad esempio, alla vita privata e alla *privacy*.

pubblico rilevante sulla base di norme giuridiche, prevedendo misure appropriate per tutelare i diritti dell'interessato; (…) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici».

[4] Reg. UE n. 1347/2024, reg. UE n. 1348/2024, dir. UE n. 1346/2024, reg. UE n. 1351/2024, reg. UE n. 1358/2024, reg. UE n. 1349/2024, reg. UE n. 1352/2024, reg. UE n. 1356/2024, reg. UE n. 1359/2024, reg. UE n. 1350/2024 del P.E. e del Cons. del 14-05-2024.

[5] È previsto anche il sistema EES: un sistema di ingresso-uscita automatizzato per i viaggiatori che provengono dal Regno Unito e da altri Paesi terzi che non necessitano di un visto per entrare nell'UE. I viaggiatori dovranno scansionare il proprio passaporto o un altro documento di viaggio presso un dispositivo self-service ogni volta che attraversano una frontiera esterna dell'UE, e tale sistema non si applicherà ai residenti legali o ai titolari di visti per soggiorni di lunga durata. Le barriere automatiche EES devono essere installate a tutte le frontiere internazionali terrestri, marittime e aeree dell'area Schengen. I viaggiatori potranno registrare i propri dati presso i dispositivi self-service e su applicazioni mobili in alcuni Paesi e, in seguito, le guardie di frontiera o gli e-*gates* completeranno i controlli. Non è stato definito con esattezza quando il sistema sarà introdotto. È poi previsto il sistema ETIAS: esso è utilizzato per i cittadini di Paesi terzi esenti dal visto, prima del loro arrivo nel territorio UE. I viaggiatori potranno richiedere l'ETIAS online prima del viaggio al costo di 7 euro. Una volta approvata, l'autorizzazione elettronica di viaggio sarà collegata elettronicamente al passaporto e avrà una durata di tre anni.

2. La raccolta dei dati biometrici: le preesistenti banche dati e le novità introdotte dal nuovo "Patto sulla migrazione e l'asilo"

Occorre preliminarmente chiarire che, nell'ambito dell'impiego di banche dati per il riconoscimento dei soggetti ricordati, sono attualmente attivi tre sistemi: il SIS, l'EURODAC e il VIS.

Il primo trova origine nella Convenzione di applicazione dell'Accordo di Schengen ed è stato istituito per assicurare la sicurezza pubblica e, al contempo, garantire la libera circolazione delle persone[6]. Esso convoglia le informazioni di cittadini di Paesi terzi, ricercati per arresto o estradizione, oppure sottoposti al monitoraggio straordinario[7].

La seconda banca dati, denominata EURODAC[8], invece, è operativa dal 2003 e utilizza le impronte digitali dei richiedenti asilo e dei cittadini di Paesi terzi non appartenenti allo Spazio economico europeo (SEE) per il confronto tra gli Stati membri dell'Unione[9].

In merito al VIS, introdotto per il rilascio dei visti per soggiorni di breve durata, esso consente di condividere informazioni sulle decisioni rese tra consolati, autorità centrali dei visti e autorità nazionali collocate ai valichi di frontiera esterni mediante confronti sulle impronte digitali. Segnatamente, tali controlli vengono svolti con l'obiettivo di contrastare i rischi di frode, di elusione e di individuare i soggetti che non siano più dotati dei requisiti necessari per l'ingresso nell'UE.

Più concretamente, un soggetto proveniente da uno Stato *extra* UE è sottoposto ai sistemi di controllo del SIS; un individuo che tenti irregolarmente di attraversare i confini o che richieda la protezione internazionale è tenuto a sottoporsi alla raccolta delle impronte digitali per l'inserimento nel sistema EURODAC; mentre nell'ipotesi di soggetto in

[6] Convenzione di applicazione all'Accordo di Schengen, in GUCE del 22-09-2000, n. L 239.

[7] L'originario sistema SIS è stato notevolmente ampliato nel corso degli anni prevedendosi l'estensione dell'uso del sistema di informazione Schengen per il rimpatrio di cittadini di Paesi terzi il cui soggiorno è irregolare; l'istituzione del sistema di informazione Schengen nel settore delle verifiche di frontiera, nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale si veda: reg. UE n. 1860/2018 del P.E e del Cons. del 28-11-2018; reg. UE n. 1861/2018 del P.E e del Cons. del 28-11-2018, che modifica e abroga la decisione n. 2007/533/GAI del Cons. e che abroga il reg. CE n. 1986/2006; reg. UE n. 1852/2018 del P.E e del Cons. del 28-11-2018, che modifica e abroga la decisione n. 2007/533/GAI del Cons. e che abroga il reg. CE n. 1986/2006.

[8] Reg. UE n. 603/2013 del P.E e del Cons. del 26-06-2013.

[9] I richiedenti la protezione internazionale o coloro i quali valicano le frontiere in maniera irregolare devono essere sottoposti al rilievo di dati dattiloscopici. Gli Stati membri confrontano le informazioni personali rilevate con i dati presenti in EURODAC, in modo tale da comprendere se un determinato soggetto abbia già presentato domanda di protezione internazionale o se si tratti di un irregolare. I dati sono raccolti mediante segnalazioni e l'accesso agli stessi è consentito alle autorità di controllo delle frontiere, quelle di polizia, o quelle consolari. Attraverso la raccolta di foto, impronte digitali o palmari e prelievo del DNA vengono inserite tali informazioni all'interno dei database. Nell'ipotesi di rifiuto di sottoporsi agli *scanner* di impronte digitali o di fornire i propri dati personali, sono state previste pene detentive accompagnate da un divieto di ingresso per 5 anni sul suolo europeo.

DPCE online
ISSN: 2037-6677

possesso di un visto per breve durata, i suoi dati verranno raccolti all'interno del VIS[10].

I diversi *database* fin qui descritti hanno subito significative modifiche a seguito dell'adozione da parte del Consiglio dell'UE del nuovo "Patto sulla migrazione e l'asilo"[11]. Un pacchetto formato da dieci atti legislativi che stabilisce una serie di norme volte a gestire in modo più sistematico ed efficiente i flussi migratori attraverso riforme che hanno l'ambizioso obiettivo di accrescere la solidarietà tra Stati membri e di rafforzare l'efficacia del sistema di asilo. Tale pacchetto ha posto l'accento su una migliore cooperazione tra l'Unione Europea, le sue istituzioni e gli Stati terzi, al fine di contrastare prevalentemente il fenomeno dilagante dell'immigrazione irregolare.

Per gli irregolari che accedono al suolo europeo, il nuovo Patto prevede controlli più severi, affidati ad una nuova procedura di *screening* che si concreta in una raccolta biometrica e dattiloscopica e in controlli sanitari e di sicurezza. Le informazioni ottenute verranno raccolte attraverso la piattaforma EURODAC che è stata potenziata, aggiungendo alle impronte digitali anche il riconoscimento facciale dell'individuo e le sue informazioni personali (il luogo, la data di nascita e il passaporto o documento equipollente). La categoria dei soggetti coinvolti in tale procedura è stata poi estesa, inserendo i bambini di età non inferiore ai sei anni, mentre prima dell'adozione di tale pacchetto, era previsto un limite verso i soggetti di età non inferiore a 14 anni)[12].

Con riguardo alle finalità dell'EURODAC, occorre ricordare che nonostante esso fosse stato originariamente concepito per migliorare il sistema di Dublino, a seguito della riforma del "Patto sulla migrazione e l'asilo" lo scopo si è tramutato in quello di prevenire, accertare o indagare reati di terrorismo o altri reati gravi garantendo l'interoperabilità tra banche dati[13]; ciò determina il rischio di una violazione del principio di limitazione delle finalità, poiché i dati raccolti in EURODAC prima della riforma non sono allineati ai nuovi scopi contenuti nel Patto (v. *infra*).

Con l'adozione del nuovo pacchetto si velocizzano le modalità di raccolta dei dati attraverso una fase di *screening* che si riduce a 7 giorni e una procedura di frontiera accelerata per i richiedenti asilo di massimo 12 settimane. Viene inoltre introdotto un meccanismo di redistribuzione dei richiedenti asilo fondato su un principio solidaristico.

Invero, ai fini del più equo ricollocamento dei migranti è previsto un meccanismo di solidarietà obbligatoria tra gli Stati membri che volge a diminuire la pressione sui paesi di primo approdo. È rimessa, quindi, alla

[10] S. Marinai, *Il rafforzamento del controllo digitale nel nuovo Patto sulla migrazione e l'asilo*, in *AISDUE*, II, 2020, 8, 119 ss.

[11] Reg. UE n. 1347/2024, reg. UE n. 1348/2024, dir. UE n. 1346/2024, reg. UE n. 1351/2024, reg. UE n. 1358/2024, reg. UE n. 1349/2024, reg. UE n. 1352/2024, reg. UE n. 1356/2024, reg. UE n. 1359/2024, reg. UE n. 1350/2024 del P.E. e del Cons., cit.

[12] P. De Pasquale, *Il Patto per la migrazione e l'asilo: più ombre che luci*, in *AISDUE*, II, 1, 2020, 1 ss.; D. Schilirò, *Migranti, Europa e Mediterraneo*, in *Munich Personal RePEc Archive*, 2024, 8 ss.; R. Palladino, *Patto sulla migrazione e l'asilo: verso nuove regole sui rimpatri*, in *AISDUE*, II, 2020, 5, 1 ss.

[13] Considerando 33, reg. UE n. 1358/2024 del P.E e del Cons. del 14-05-24.

discrezionalità dello Stato che ospiterà il soggetto in questione, decidere se accogliere sul proprio territorio una quota di richiedenti asilo mediante il sistema del ricollocamento oppure garantire un supporto finanziario pari a ventimila euro per ogni migrante ospitato.

La procedura prevede una fase di *screening*, la cui durata massima è di sette giorni, e una procedura di frontiera accelerata per i richiedenti asilo fino ad un totale di 12 settimane. Quest'ultima trova applicazione d'ufficio per chi proviene da paesi che hanno un tasso di ammissione delle domande d'asilo inferiore al 20 per cento, e per i soggetti che possono rappresentare una minaccia per la sicurezza nazionale o l'ordine pubblico, tra questi anche i minori non accompagnati o coloro i quali forniscono informazioni mendaci alle autorità[14].

Gli Stati membri dovranno, di conseguenza, dotarsi di strutture adeguate a ospitare i richiedenti asilo durante l'esame della richiesta e, se l'esito dovesse essere negativo, è previsto il rimpatrio entro 12 settimane. Infine, il regolamento interviene sulle procedure ordinarie, imponendo alle autorità nazionali un massimo di 6 mesi per decidere in prima istanza in merito alle richieste di protezione.

La previsione di procedure così accelerate non accompagnate da garanzie adeguate appare piuttosto critica soprattutto perché l'UE sembra agire in tal modo per ragioni securitarie. Infatti, la celerità e la speditezza previste dal nuovo Patto renderanno più difficoltoso l'esercizio del diritto di difesa da parte del migrante che avrà la possibilità di sostare sul suolo comunitario per un periodo di tempo limitato se la sua domanda dovesse essere rigettata, non potendo perciò far valere le proprie ragioni attraverso le procedure giurisdizionali. L'insieme di tali misure rischia di discriminare i migranti rendendoli, quindi, protagonisti di trattamenti differenziati.

3. Un bilanciamento tra il diritto alla *privacy* e alla riservatezza e la libera circolazione dei dati

Le criticità determinate dalla condivisione dei dati personali, relative al bilanciamento tra la libera circolazione degli stessi, per esigenze di sicurezza pubblica, la tutela della *privacy* e della riservatezza, sono state evidenziate, già da tempo, dal Garante europeo della protezione dei dati personali che, guardando all'entrata in vigore del nuovo Patto[15], ha messo in evidenza soprattutto la violazione del principio di limitazione delle finalità[16].

Infatti, il sistema EURODAC era stato originariamente pensato per supportare l'attuazione del regolamento di Dublino, mentre la disciplina novellata ne muta gli scopi, mirando a prevenire, accertare o indagare reati di terrorismo o altri reati gravi, anche grazie al meccanismo della interoperabilità. Di talché, i dati biometrici verrebbero usati per scopi divergenti da quelli specificamente dichiarati al momento della raccolta, venendo meno la trasparenza e la sicurezza degli stessi. A parere della

[14] E. Celoria, V. Ferraris, *Eurodac: dalla gestione delle domande di protezione internazionale al controllo della mobilità*, in *Quaderni AISDUE*, 2024, 4, 1 ss.
[15] EDPS, Opinion no. 9/2020, par. 31.
[16] G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i legislatori e le Corti*, in *DPCE online*, 2019, 2, 1107 ss.

DPCE online
ISSN: 2037-6677

autorità Garante, i dati biometrici non possono essere utilizzati per finalità diverse da quelle specificate senza il consenso esplicito degli interessati. Più in dettaglio, a titolo meramente esemplificativo, le impronte digitali raccolte per l'accesso ad un'area riservata non possono essere usate per il monitoraggio delle presenze senza un'adeguata informativa e consenso, oppure nel caso di un controllo ai fini identificativi, con raccolta dati e comunicazione da parte del CIR all'autorità di polizia che utilizzi tali dati per scopi differenti.

Si aggiunga poi che i rischi aumenteranno potenzialmente nella misura in cui l'interoperabilità metterà in contatto tra di loro tutte le banche dati sopra menzionate e si estenderà la legittimazione delle autorità competenti ad accedere a tali informazioni[17].

Altre questioni potranno poi sollevarsi con riguardo alla violazione del principio di proporzionalità. Invero, tale problema ha già occupato in passato le Corti costituzionali dei singoli Stati membri.

Si ricorda, ad esempio, il caso del governo francese che, nel 2012, proponeva una modifica legislativa per l'istituzione di un *database* nazionale per la raccolta di informazioni biometriche della popolazione interna, da ottenere mediante impronte digitali e conservazione di dati. La questione veniva posta al vaglio della Corte costituzionale[18] per violazione del principio di proporzionalità, soprattutto in virtù della mancanza di una limitazione temporale della conservazione dei dati. Peraltro, veniva criticata la possibilità di accesso alla stessa banca dati mediante autorizzazione del Procuratore della Repubblica, previa informazione del soggetto interessato, al fine di prevenire reati gravi come quelli di terrorismo.

La Corte ha, pertanto, stabilito che la suddetta raccolta biometrica non potesse considerarsi proporzionata rispetto allo scopo della normativa, che travalicava il mero fine identificativo. Profili critici erano da individuare dunque nell'assenza di limitazioni di ordine temporale alla conservazione e trattenimento delle informazioni nel *database* così come nella mancanza di idonee e adeguate salvaguardie e restrizioni circa l'uso della banca dati.

Di conseguenza, la proposta di legge francese veniva modificata mediante la semplice introduzione delle impronte digitali all'interno del *chip* della carta di identità, non includendo l'esistenza di un *database*, al fine di eliminare le illegittimità riscontrate[19].

---

[17] S. Marinai, *Il rafforzamento del controllo digitale nel nuovo Patto sulla migrazione e l'asilo*, op. cit., 119 ss.; M. Forti, *Il Regolamento (UE) 2016/679 alla prova dei flussi migratori diretti verso l'Europa mediterranea. La tutela dei dati personali di rifugiati e migranti*, in D. Poletti, A. Mantelero (cur.), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa, 2018, 449 ss.

[18] *Conseil Constitutionnel*, decisione n. 2012-652, 22-03-2012.

[19] Un'ipotesi analoga si è verificata in Belgio, dove alla fine del 2018 il Parlamento approvava una legge che integrava l'obbligo di inserire due impronte digitali (oltre alla fotografia del soggetto) da includere all'interno del microchip della carta d'identità, senza creare un'apposita banca dati, ma imponendo la distruzione degli stessi dati dopo un periodo di tre mesi dalla raccolta. Qui erano state sollevate numerose critiche da parte del Garante della *privacy* sulla normativa di raccolta dei dati ritenuta lesiva del principio di proporzionalità poiché priva di un elenco di finalità nel rispetto delle quali le pubbliche autorità potevano effettuare controlli tra il soggetto sottoposto a verifiche e quelle contenute all'interno del documento di identità. Sul punto v. *Avis d'initiative* n. 106/2018 della *Autorité de protection des données* del 17-10-2018; in precedenza l'Autorità

Tale ricostruzione è utile per sottolineare che negli Stati membri, spesso, vi è una chiara contrapposizione tra la raccolta dei dati a garanzia della sicurezza pubblica e la tutela della *privacy* e della riservatezza, diversamente da altre esperienze extraeuropee che pongono, da un lato, la riservatezza e, dall'altro, la dignità umana[20].

Per tali ragioni i legislatori dei Paesi membri sono chiamati a prestare attenzione alle normative inerenti alla circolazione dei dati personalissimi, giacché il rischio di logorare in qualche misura i diritti fondamentali è sempre presente, a maggior ragione in virtù del fatto che ciascuno Stato raccoglie i dati dei migranti attraverso modalità differenti, spesso invasive e limitative della vita privata degli stessi.

4. L'orientamento della Corte di giustizia

Le problematiche relative al trattamento dei dati personali sono state oggetto di talune pronunce della Corte di giustizia che possono assumere rilievo, *mutatis mutandis*, per definire i limiti dell'utilizzo di quelli dei migranti.

In particolare, la Corte ha avuto modo di pronunciarsi sul requisito del carattere «strettamente necessario» della registrazione dei dati. Nella causa c-205/21[21], la questione aveva ad oggetto il rifiuto della signora V.S. di

si era già espressa in tal senso con l'*Avis* n. 18/2018 del 28-02-2018, ritenendo anche che la nuova proposta di regolamento europeo avanzata dalla Commissione, richiamata dal Governo per legittimare la propria normativa interna, non fosse dotata di salvaguardie volte ad evitare un'intrusione eccessiva nei diritti alla *privacy* e *data protection* dei cittadini. Inoltre, anche il Garante Europeo della Protezione dei Dati (2018/C 338/12) con parere negativo rilevava la mancata previsione, nella proposta della Commissione, di tali garanzie. Si riteneva che nella proposta dovesse essere inserita una disposizione che determinasse la cancellazione dei dati biometrici trattati nel suo contesto dopo il loro inserimento nel microprocessore e un divieto di utilizzo per finalità diverse da quelle esplicitamente indicate nella proposta.

[20] Ad esempio, in India la Corte Suprema è stata investita di una questione di legittimità costituzionale inerente al caso Aadhaar project, un sistema nazionale volto ad individuare in modo uniforme l'identità dei cittadini indiani e di evitare rischi quali la duplicazione di identità o l'accesso illegittimo a tali servizi. Il problema si presentava nella misura in cui mancava una specifica legislazione in materia di *privacy* e di protezione dei dati, facendo emergere dubbi circa la adeguatezza e proporzionalità sull'utilizzo dei dati biometrici. Il nucleo della vicenda ruotava attorno al fatto che la condivisione di tali dati, per la popolazione indiana dava accesso al diritto al cibo e all'abitazione, pertanto il bilanciamento in questo caso operava tra diritto alla riservatezza e diritto alla dignità umana (garantito nella misura in cui tali dati assicuravano dei sussidi alimentari o ancora l'accesso ai servizi). A seguito della vicenda, il progetto Aadhaar è stato vietato nelle ipotesi in cui rappresentasse una condizione esclusiva per la apertura di conti correnti bancari e acquisto di schede telefoniche; il sistema era considerato sproporzionato nella parte in cui statuiva che i dati biometrici fossero forniti per obiettivi che andassero al di là della tutela della dignità umana (mediante l'accesso, i servizi essenziali ed ai sussidi). Si veda: G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i legislatori e le Corti*, op. cit., 1125-1126.

[21] Corte giust., c-205/21, *V.S.*, 26-01-2023; in proposito si vedano le conclusioni dell'Avvocato Generale Pitruzzella presentate il 30-06-2022, c-205/21: «a tal riguardo, rilevo (…) che l'ordine di procedere alla registrazione da parte della polizia interviene

DPCE online
ISSN: 2037-6677

fornire i propri dati biometrici nell'ambito di un procedimento penale. Dalla sentenza si evince che la normativa bulgara[22], richiamava solo l'art. 9 del GDPR, e non l'art. 10 della direttiva 2016/680, anche se il tenore letterale della norma nazionale riprendeva sostanzialmente il contenuto del suddetto articolo della direttiva[23]. Il GDPR enuncia il divieto del trattamento di tali dati, corredato di un elenco di eccezioni in cui però non rientra la lotta contro la criminalità[24]. Mentre il trattamento di dati sensibili da parte delle autorità competenti ai fini di prevenzione e di accertamento dei reati di cui alla direttiva 2016/680 può essere autorizzato solo se strettamente necessario e deve essere soggetto a garanzie adeguate e previsto dal diritto dell'Unione o dal diritto di uno Stato membro.

La legge bulgara, quindi, risultava ambigua e contraddittoria. La Corte ha chiarito che il riferimento all'art. 9 del GDPR e non alla suddetta direttiva, non appare contraddittorio purché dall'interpretazione di tutte le disposizioni applicabili del diritto nazionale appaia sufficientemente chiaro, preciso e inequivocabile che il trattamento di dati biometrici e genetici in questione rientri nell'ambito di applicazione di tale direttiva, e non del GDPR[25]. La seconda questione sollevata dal giudice *a quo*, invece, riguardava l'accesso ad una tutela giurisdizionale effettiva da parte di V.S. Secondo la legge bulgara infatti, il giudice penale competente al fine di autorizzare una misura di esecuzione coercitiva (raccolta di dati sensibili di una persona formalmente accusata), non può controllare nel merito le condizioni della sua accusa formale a causa della mancanza temporanea delle prove. Detto controllo nella fase preliminare del procedimento potrebbe ostacolare lo svolgimento dell'indagine penale. La sentenza ha quindi stabilito che la raccolta sistematica dei dati biometrici e genetici di qualsiasi persona formalmente accusata di un reato doloso perseguibile d'ufficio, ai fini della loro registrazione, è in linea di principio contraria al requisito enunciato

nel corso della fase preliminare del procedimento penale, che costituisce la fase in cui vengono effettuati gli atti di indagine e di raccolta delle prove, al termine della quale è necessario stabilire se sia stato commesso un reato, chi ne è l'autore e se sussiste la responsabilità penale di quest'ultimo. Una volta completata l'indagine penale e rese note le prove, il pubblico ministero dovrà decidere se archiviare il procedimento penale, se sospenderlo, se proporre un'esimente da responsabilità penale corredata di una sanzione amministrativa, se proporre una transazione o se rinviare a giudizio mediante atto di accusa. È il deposito di tale atto d'accusa davanti al giudice che avvia la fase giudiziaria del procedimento penale». Sul punto la Corte ha ritenuto che la normativa nazionale sia giustificata e non sia sproporzionata sempre che il diritto nazionale garantisca successivamente un controllo giurisdizionale effettivo. Invero, la Corte di giustizia ha stabilito che il diritto alla tutela giurisdizionale effettiva di cui all'art. 47 della Carta non costituisce una prerogativa assoluta poiché alla luce dell'art. 52 co. 1 (CDFUE) possono essere apportate limitazioni dalla legge, che tutelino il contenuto essenziale delle libertà e dei diritti in questione nel rispetto del principio di proporzionalità, tali limitazioni siano necessarie e riguardino finalità di interesse generale riconosciute dall'Unione (p.to 89); tale statuizione è conforme a quanto espresso nelle conclusioni dell'Avvocato Generale Pitruzzella, c-205/21, cit.

[22] Art. 25 par. 3 e 25 *bis* par. 1 della legge sul Ministero degli affari interni ZMVR in tema di raccolta coercitiva dei dati biometrici.

[23] Corte giust., *V.S.*, cit., p.to 57.

[24] Corte giust., *V.S.*, cit., p.to 40.

[25] Corte giust., *V.S.*, cit., p.to 76.

dalla direttiva 680/2016[26]. L'art. 10 di tale direttiva mira, difatti, a rafforzare la tutela dei dati sensibili, prevedendo che il trattamento possa essere autorizzato solo se «strettamente necessario» (tenuto conto delle condizioni risultanti dall'articolo 4, paragrafo 1, lettere b) e c), e dall'articolo 8, paragrafo 1) rispetto al raggiungimento dell'obiettivo e sempre che non si possa ricorrere ad una misura meno ingerente nei diritti e nelle libertà del soggetto.

La Corte di giustizia giunge alla medesima conclusione anche nella causa c-393/19[27] nell'ambito della quale ha chiarito che il diritto di proprietà non costituisce una prerogativa assoluta, poiché l'art. 52 par. 1 della CDFUE riconosce talune limitazioni allo stesso a condizione che queste rispondano ad obiettivi di interesse generale perseguiti dall'Unione e non determinino un intervento sproporzionato e inaccettabile che possa ledere la sostanza stessa del diritto in questione.

La Corte ha condannato la raccolta generalizzata dei dati delle persone formalmente accusate, poiché la nozione di «reato doloso perseguibile d'ufficio» è, in linea astratta e generica, applicabile ad un numero piuttosto ampio di reati, senza distinzioni di natura, gravità, circostanze particolari e altro. Essa ha poi aggiunto che il carattere strettamente necessario può essere dimostrato tenuto conto dell'insieme degli elementi pertinenti, della natura e della gravità del reato presunto[28].

Non meno interessanti sono le conclusioni dell'Avvocato generale De la Tour che, nella causa c-80/23[29] presentate il 13 giugno 2024, ha ritenuto che il carattere «strettamente necessario», della registrazione effettuata dall'autorità di polizia, dev'essere verificato dalle autorità competenti prima della raccolta coercitiva dei dati.

Ciò sta a significare che la valutazione di tale requisito non potrà essere svolta in sede di autorizzazione dell'esecuzione coercitiva soltanto nei casi di rifiuto della persona formalmente accusata di sottoporsi alla registrazione e solo alla luce di uno degli scopi contenuti nella normativa nazionale che ne costituisce la base giuridica.

La sentenza c-80/23[30] emessa in data 28 novembre 2024 accoglie le conclusioni dell'Avvocato generale analizzando l'articolo 10 della direttiva 2016/680 in combinato disposto con l'articolo 4, paragrafo 1, lettere da a) a c), nonché con l'articolo 8, paragrafi 1 e 2, di tale direttiva. Secondo tale interpretazione, una normativa nazionale che prevede la raccolta sistematica dei dati biometrici e genetici di qualsiasi persona formalmente accusata di un reato doloso perseguibile d'ufficio, senza prevedere l'obbligo in capo

[26] Dir. (UE) 2016/680 del P.E e del Cons. del 27-04-2016. Essa si applica specificamente al trattamento di dati effettuato dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali. È, dunque, focalizzata sul settore della giustizia e della sicurezza pubblica, ma condivide con il regolamento lo stesso obiettivo di fondo.

[27] La causa aveva ad oggetto la condanna del signor OM per contrabbando doganale aggravato, realizzato mediante l'uso di un trattore di proprietà di un soggetto terzo, direttore della società turca presso cui lavorava.

[28] Corte giust., *V.S.*, cit., p.to 133.

[29] Corte giust., c-80/23, *V.S.*, concl. dell'AG de la Tour, 13-06-2024, p.to 57.

[30] Corte giust., c-80/23, *V.S.*, sent. 28-11-2024.

DPCE online
ISSN: 2037-6677

all'autorità competente[31] di verificare e dimostrare il carattere strettamente necessario di tale raccolta, contrasta con l'art. 10 della direttiva. Il rispetto di tale obbligo non può essere assicurato dall'organo giurisdizionale adito dall'autorità competente ai fini dell'esecuzione coattiva della raccolta, ma spetterebbe proprio alla suddetta autorità effettuare la valutazione richiesta.

Tali orientamenti, che definiscono importanti principi di diritto, dovrebbero essere tenuti in giusto conto nell'applicazione del nuovo "Patto sulla migrazione e l'asilo".

Precisamente, il trattamento dei dati biometrici dei migranti deve necessariamente rispettare rigorosi principi di proporzionalità e necessità, garantendo che tali misure siano utilizzate quando strettamente indispensabili e sempre con un adeguato rispetto dei diritti e della dignità delle persone coinvolte. E questo soprattutto con riferimento all'utilizzo dei dati biometrici così come disciplinato dal nuovo regolamento EURODAC che, come risaputo, ha lo scopo di prevenire, accertare o indagare reati di terrorismo o altri reati gravi. Invero, il concetto di "stretta necessità" è fondamentale per mantenere un equilibrio tra esigenze di sicurezza e la tutela dei diritti fondamentali, come il diritto alla privacy e alla protezione dei dati personali.

Di talché, il carattere «strettamente necessario» dei dati biometrici dei migranti impone un loro utilizzo soltanto quando necessario per uno scopo legittimo. Le autorità devono perciò limitare il ricorso a questi dati a situazioni in cui non esistono alternative meno invasive e devono utilizzare le informazioni raccolte solo per scopi chiaramente definiti e proporzionati. Ad esempio, raccogliere dati biometrici per registrare i migranti può essere considerato necessario se non vi sono altri mezzi efficaci per verificarne l'identità, ma diventa eccessivo se usato per monitoraggi costanti senza giustificazioni.

Il rischio è che un uso eccessivo o indiscriminato dei dati biometrici porti a violazioni dei diritti dei migranti, con conseguenze che vanno dalla sorveglianza continua alla discriminazione. Inoltre, il trattamento inadeguato di questi dati può esporre i migranti a ulteriori vulnerabilità, come furto d'identità o uso improprio da parte di governi autoritari.

D'altronde, la stessa situazione di "migrante" risulta particolarmente vulnerabile, in ragione delle differenti caratteristiche soggettive che riguardano gli stessi (irregolari, richiedenti la protezione internazionale, bambini di età superiore ai 6 anni). A seconda del soggetto di cui si rilevano i dati potrebbe trattarsi di un indagato oppure potrebbe determinarsi una mera presunzione di colpevolezza in capo al soggetto.

Nonostante poi il nuovo regolamento EURODAC assicuri formalmente una tutela giurisdizionale effettiva attraverso l'art. 52 che rinvia all'art. 79 del GDPR, restano numerosi dubbi sulla sua capacità di garantire ad un cittadino di Paese terzo una tutela sostanziale e, dunque, l'accesso alla giustizia nel caso di lesione dei suoi diritti fondamentali derivante da un utilizzo non sufficientemente informato dei suoi dati o comunque illegittimo degli stessi.

È pure evidente che la possibilità di vedere garantita tale tutela potrebbe trovare differenti ostacoli scaturenti da una scarsa conoscenza dei

[31] Ai sensi dell'art. 3, p.to 7, di detta direttiva.

propri diritti; cioè è lecito domandarsi se il migrante avrà piena ed effettiva conoscenza di come verranno utilizzati i dati. Sarà altresì difficile l'individuazione del giudice competente, vista la frammentarietà della competenza giurisdizionale, la natura transnazionale dei dati trattati e la molteplicità di autorità coinvolte. Non da ultimo rileva la considerazione che l'onere della prova incombe sull'interessato che si trova in posizione di evidente squilibrio rispetto a chi detiene i suoi dati personali.

5. Conclusioni

Il "Patto sulla migrazione e l'asilo" è stato dipinto dai maggiori esponenti delle istituzioni europee come il raggiungimento di un "equilibrio tra solidarietà e responsabilità"[32], tuttavia, come innanzi accennato, emerge un atteggiamento securitario volto a difendere i confini nazionali dalle ondate massicce di immigrati irregolari.

Per quanto qui di interesse, un aspetto particolarmente grave risiede nell'assenza di una tutela effettiva della riservatezza e della dignità umana di soggetti privi del potere di rifiutarsi di cedere i propri dati biometrici, poiché questo significherebbe essere rispediti nel territorio di origine.

Invero, preoccupa molto che le soluzioni all'emergenza migratoria vengano testate proprio sui soggetti più deboli (rifugiati e migranti) che non soltanto, spesso, mancano persino delle conoscenze di base relative alle implicazioni derivanti dall'utilizzo dei propri dati personali, ma con grandi difficoltà e non sempre con esito positivo riescono ad opporsi alle decisioni prese alla luce di tali dati (ritorno in un Paese di origine dove i diritti umani non sono rispettati e dove rischiano di essere perseguitati). Le preoccupazioni sono acuite dalla considerazione che, mentre il consenso informato è sempre più trascurato, il "diritto al rifiuto" è sottoposto a meccanismi incomprensibili e farraginosi. E neppure esiste un sistema di controllo efficace per garantire che i governi e le istituzioni siano responsabili dell'utilizzo dei dati degli stessi.

Ulteriori criticità si pongono in relazione al profilo temporale della conservazione dei suddetti dati, poiché quelli relativi ai richiedenti protezione internazionale saranno conservati per dieci anni, mentre quelli inerenti alle persone ammesse nell'ambito di programmi di reinsediamento e agli irregolari, per cinque. In lassi di tempo così prolungati si rischia non solo l'utilizzo dei *data* per scopi diversi da quelli inizialmente previsti, ma anche il furto degli stessi attraverso attacchi informatici. Si aggiunga inoltre, che con l'aumento del numero di enti e persone che possono accedere a questi dati, potrebbero aumentare anche i casi di uso non autorizzato dal momento che correggere eventuali errori, mantenere i dati sicuri per lunghi periodi e garantire un costante aggiornamento a tutela della sicurezza e dell'integrità degli stessi, potrebbe richiedere risorse finanziarie e tecnologiche significative.

[32] Come si evinceva dalle parole del presidente del P.E. Roberta Metzola: «abbiamo elaborato un solido quadro legislativo su come affrontare la migrazione e l'asilo nell'Unione Europea. Ci sono voluti più di dieci anni per realizzarlo. Ma abbiamo mantenuto la parola».

DPCE online
ISSN: 2037-6677

Tali aspetti critici, insieme ai rischi sopra elencati di procedure ancor più celeri e alla difficoltà di far valere i propri diritti, potrebbero portare ad una profilazione dei migranti che contribuirà ulteriormente alla loro stigmatizzazione e discriminazione, e che darà luogo ad altri trattamenti differenziati.

Molteplici sono, dunque, ancora i nodi da sciogliere, con riferimento alle regole di impegno e la durata temporale secondo cui i dati possano essere legittimamente conservati nei *database*[33]; ma a queste domande saranno la Corte di giustizia e il legislatore a dover rispondere.

Intanto, sembra che un aspetto positivo della riforma sia rinvenibile nella riduzione del limite di età dei soggetti sottoposti alle procedure di *screening*; in quanto potrebbe rappresentare una maggiore garanzia per i minori, di cui spesso non si hanno informazioni e che per questo sono facilmente vittime di tratta o di traffico di esseri umani. È bene sottolineare, però, che le autorità devono assicurarsi che venga utilizzato un linguaggio *child-friendly*, adatto alla loro età, in modo che sia ad esso comprensibile, e di garantire il rispetto della dignità umana e il principio di non discriminazione[34].

Rossella Benassai
Dipartimento di Giurisprudenza
Università degli studi di Napoli "Federico II"
rossella.benassai@unina.it

[33] Essendo la giurisprudenza sul tema piuttosto scarna, è interessante approfondire le problematiche inerenti alla conservazione a lungo termine dei dati biometrici per soggetti che hanno commesso reati dolosi v. Corte giust., c-118/22, *Direktor na Glavna direktsia «Natsionalna politsia» pri Ministerstvo na vatreshnite raboti – Sofia*, sent. 30-01-2024; per una fattispecie analoga si veda anche Corte giust., c-205/21, *V.S.*, sent. 26-01-2023; G. Toraldo, *Un difficile bilanciamento tra la conservazione dei dati per fini di sicurezza e il diritto all'oblio del condannato (riabilitato)*, in *DPCE online*, 2024, 1, 617 ss.

[34] M. Mereu, *Gli ostacoli normativi ai diritti dei minori del nuovo Patto UE su immigrazione e asilo*, 27 novembre 2024, https://www.meltingpot.org/2024/11/gli-ostacoli-normativi-ai-diritti-dei-minori-del-nuovo-patto-ue-su-immigrazione-e-asilo/.