



## Il rafforzamento del controllo digitale nel nuovo Patto sulla migrazione e l’asilo

**Simone Marinai\***

SOMMARIO: 1. Premessa. – 2. La sorveglianza digitale delle frontiere dell’area Schengen: cenni al quadro giuridico esistente. – 3. Il nuovo Patto e l’interoperabilità. – 4. I dati raccolti nella nuova procedura di esame pre-ingresso. – 5. La riforma di Eurodac. – 6. Considerazioni conclusive.

1. Nell’ambito dei controlli che gli Stati membri dell’Unione sono chiamati a compiere sulle persone che attraversano le frontiere esterne, sempre maggiore rilevanza ha assunto, negli ultimi anni, l’impiego delle nuove tecnologie digitali attraverso le quali agevolare la gestione dei flussi migratori e garantire la sicurezza dell’area Schengen<sup>1</sup>.

Lo sviluppo di banche dati elettroniche sempre più pervasive e tra loro interoperabili, la raccolta e la verifica di dati biometrici, l’uso di porte di ingresso automatizzate ai punti di ingresso ed uscita dal territorio nazionale, rappresentano esempi di strumenti mediante i quali i controlli di frontiera

---

\* Professore associato di Diritto dell’Unione europea presso l’Università di Pisa.

<sup>1</sup> Per un aggiornato esame della gestione delle frontiere esterne da parte dell’Unione, v. G. CAGGIANO, *Recenti sviluppi del regime delle frontiere esterne nello spazio di libertà, sicurezza e giustizia*, in A. DI STASI, L.S. ROSSI (a cura di), *Lo spazio di libertà, sicurezza e giustizia. A vent’anni dal Consiglio europeo di Tampere*, Napoli, 2020, p. 383.

sono stati rafforzati in una logica securitaria che indubbiamente caratterizza la politica dell'Unione in materia di immigrazione<sup>2</sup>.

Le principali implicazioni, dal punto di vista della tutela dei diritti fondamentali dei singoli, derivanti dall'impiego di simili strumenti digitali, sono note<sup>3</sup>. Si pensi, ad esempio, ai problemi collegati alla tutela della vita privata e, in particolare, alla protezione dei dati personali dei soggetti inseriti all'interno delle banche dati in questione. Oppure, alle difficoltà che quanti si trovino inseriti nelle predette banche dati possono incontrare al fine di ottenere la rettifica dei dati ivi registrati, soprattutto nel caso in cui questi ultimi abbiano comportato l'impossibilità di accedere al territorio dell'Unione.

Oggetto del presente contributo è quello di analizzare l'ulteriore rafforzamento della sorveglianza digitale che emerge – in modo trasversale – dal pacchetto di misure (o, quanto meno, da alcune di esse) che la Commissione europea ha proposto nell'ambito del nuovo Patto sulla migrazione e l'asilo presentato il 23 settembre 2020<sup>4</sup>. In particolare, dopo aver premesso alcune considerazioni generali sull'attuale quadro giuridico che caratterizza l'impiego delle nuove tecnologie nel controllo delle frontiere dell'area Schengen (par. 2), ci soffermeremo sul rilievo che nel nuovo Patto viene dato all'interoperabilità tra le diverse banche dati (par. 3), sui principali profili problematici sollevati dalle modalità con cui si intendono raccogliere ed utilizzare i dati nell'ambito della c.d. procedura di pre-ingresso (par. 4) e, infine, sulle implicazioni, in termini di rafforzamento dei controlli digitali, derivanti dalla proposta di riforma della banca dati Eurodac (par. 5). In sede di considerazioni conclusive (par. 6), potremo così valutare

---

<sup>2</sup> Tra le numerose voci critiche rispetto all'approccio securitario che caratterizza, in gran parte, la politica dell'Unione europea in materia di immigrazione, v. ad es., F. CRÉPEAU, *Report of the Special Rapporteur on the human rights of migrants, Regional study: management of the external borders of the European Union and its impact on the human rights of migrants*, A/HCR/23/46 del 24 aprile 2013, punto 31 ss.

<sup>3</sup> Sulle varie implicazioni che la creazione di frontiere digitali produce sui diritti fondamentali degli individui, v. ad es. E. BROUWER, *Digital Borders and Real Right. Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden, 2008.

<sup>4</sup> V. comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale, al Comitato delle regioni, *Un nuovo patto sulla migrazione e l'asilo*, COM (2020) 609 final, 23 settembre 2020. Per una prima valutazione complessiva del Patto, v. S. CARRERA, *Whose Pact? The Cognitive Dimensions of the New Pact on Migration and Asylum*, CEPS Policy Insights, 2020, n. 22; P. DE PASQUALE, *Il Patto per la migrazione e l'asilo: più ombre che luci*, in *I Post* di AISDUE, II, in questo *Focus*, n. 1, 5 ottobre 2020; A. DI PASCALE, *Il nuovo patto per l'immigrazione e l'asilo: scontentare tutti per accontentare tutti*, *Eurojus.it*, 28 settembre 2020; C. FAVILLI, *Il patto europeo sulla migrazione e l'asilo "c'è qualcosa di nuovo, anzi di antico"*, in *Questione Giustizia*, 2 ottobre 2020; S. PEERS, *First analysis of the EU's new asylum proposals*, in *statewatch.org*, 28 settembre 2020; D. THYM, *European Realpolitik: Legislative Uncertainties and Operational Pitfalls of the 'New' Pact on Migration and Asylum*, in *eumigrationlawblog.eu*, 28 settembre 2020.

se le misure previste dal nuovo Patto comportino un valore aggiunto in funzione della creazione di meccanismi di controllo digitale efficienti e, al contempo, rispettosi dei diritti degli individui che sono ad essi sottoposti.

2. Vari sono gli strumenti digitali che l'Unione europea ha sviluppato per il controllo delle proprie frontiere<sup>5</sup>.

In considerazione dell'attenzione che il nuovo Patto sulla migrazione e l'asilo dedica alle banche dati centralizzate, istituite dall'Unione al fine di consentire la raccolta e lo scambio di informazioni tra autorità incaricate di vigilare le frontiere, gestire i flussi migratori e pronunciarsi sulle domande di protezione internazionale, è in questa sede opportuno richiamare i principali caratteri delle stesse.

Occorre precisare, ad ogni modo, che gli strumenti digitali sviluppati dall'Unione per il controllo delle proprie frontiere non sono rappresentati esclusivamente da banche dati. Basti pensare, a titolo meramente esemplificativo, ai sistemi *self-service*, ai varchi automatici ed ai sistemi di controllo di frontiera automatizzato il cui impiego è stato di recente disciplinato mediante modifiche introdotte al Codice frontiere Schengen<sup>6</sup>.

Tornando, invece, alle banche dati istituite a livello di Unione europea<sup>7</sup>, tra queste devono innanzitutto essere richiamate il SIS, l'Eurodac ed il VIS.

Il SIS (Sistema informativo Schengen) è stato in origine previsto dalla Convenzione di applicazione dell'Accordo di Schengen<sup>8</sup>, al fine di preservare la sicurezza pubblica, compresa la sicurezza dello Stato, all'interno dello spazio Schengen, e facilitare la circolazione delle persone

<sup>5</sup> In proposito, v. ad es., J. J. RIJMA, *Brave New Borders: The EU's Use of New Technologies for the Management of Migration and Asylum*, in M. CREMONA (ed.), *New Technologies and EU Law*, Oxford, 2017, p. 197; P. HANKE, D. VITIELLO, *High-Tech Migration Control in the EU and Beyond: The Legal Challenges of "Enhanced Interoperability"*, in E. CARPANELLI, N. LAZZERINI (eds.), *Use and Misuse of New Technologies. Contemporary Challenges in International and European Law*, Cham, 2019, p. 3 e spec. p. 11 ss.

<sup>6</sup> V. art. 8 *bis* e ss. introdotti nel Codice frontiere Schengen dal regolamento (UE) n. 2017/2225 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che modifica il regolamento (UE) 2016/399 per quanto riguarda l'uso del sistema di ingressi/uscite.

<sup>7</sup> Per una panoramica sugli obiettivi e sulle caratteristiche delle varie banche dati istituite a livello di Unione europea, v. D. BIGO, S. CARRERA, B. HAYES, N. HERNANZ, J. JEANDESBOZ, *Justice and Home Affairs Databases and a Smart Borders System at EU External Borders. An Evaluation of Current and Forthcoming Proposals*, in *CEPS Papers in Liberty and Security in Europe*, 2012, n. 52, [www.ceps.eu](http://www.ceps.eu); N. VAVOULA, *EU immigration databases under scrutiny. Towards the normalisation of surveillance of movement in an era of 'Privacy Spring'?*, in G. VERMEULEN, E. LIEVENS (eds.), *Data Protection and Privacy under Pressure. Transatlantic tensions, EU surveillance, and big data*, Antwerp, Apeldoorn, Portland, 2017, p. 215.

<sup>8</sup> V., in particolare, gli artt. 92-119 della Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 relativo all'eliminazione graduale dei controlli alle frontiere comuni, del 19 giugno 1990.

usando informazioni comunicate attraverso il sistema stesso. Le sue funzionalità sono state successivamente potenziate, tanto da arrivare ad istituire un Sistema d'informazione Schengen di seconda generazione (SIS II) che è entrato in funzione il 9 aprile 2013<sup>9</sup>. Di recente, nel 2018, mediante tre nuovi regolamenti dell'Unione, l'ambito di applicazione e le funzionalità del sistema in questione sono stati ulteriormente ampliati, sotto diversi punti di vista<sup>10</sup>.

Gli Stati membri possono inserire nel SIS, attraverso le c.d. segnalazioni, i dati di cittadini di Paesi terzi ai fini della non ammissione<sup>11</sup>, nonché di persone ricercate per l'arresto ai fini di estradizione, oppure soggette a monitoraggio straordinario in quanto costituiscono una minaccia per la sicurezza pubblica o la sicurezza dello Stato. Ai dati possono accedere, nell'ambito delle rispettive competenze, le autorità di polizia, le autorità di controllo alla frontiera, le autorità doganali, le autorità giudiziarie nei procedimenti penali, le autorità competenti per l'immigrazione e le autorità consolari. I dati personali possono essere usati solo per le finalità delle segnalazioni specifiche per le quali sono stati forniti.

Con i tre citati regolamenti del 2018 vengono previste<sup>12</sup>, tra l'altro, nuove categorie di segnalazioni, vengono ampliate le categorie di dati

---

<sup>9</sup> V. regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) e decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II). Attualmente, il SIS II è operativo in 30 Stati: oltre ai 26 Stati dell'area Schengen, anche Bulgaria, Croazia, Romania e Regno Unito sono collegati a tale sistema, anche se il suo impiego da parte di Croazia e Regno Unito è sottoposto ad alcune limitazioni.

<sup>10</sup> Regolamento (UE) n. 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di Paesi terzi il cui soggiorno è irregolare; regolamento (UE) n. 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera (...); regolamento (UE) n. 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale (...).

<sup>11</sup> Sulla (discutibile) disciplina della segnalazione ai fini della non ammissione, v. M. DI FILIPPO, *La circolazione dello straniero nel diritto dell'Unione europea: una geometria variabile dei diritti e delle garanzie*, in A. M. CALAMIA, M. DI FILIPPO, M. GESTRI, *Immigrazione, Diritto e Diritti: profili internazionalistici ed europei*, Padova, 2012, p. 159 e spec. p. 198 ss.

<sup>12</sup> L'attuazione di tali nuove disposizioni è stabilita in modo graduale. In una prima fase, conclusasi a fine 2019, viene consentito l'accesso alle nuove funzionalità delle segnalazioni SIS a Europol ed ai membri delle squadre dispiegate dall'Agenzia europea della guardia di frontiera e costiera. Nella seconda fase, la cui attuazione è fissata entro fine 2020, si prevede che tutti gli Stati membri siano in grado di utilizzare il sistema automatico per il riconoscimento delle impronte digitali (c.d. AFIS) per compiere ricerche sulla base delle impronte digitali nel SIS. Nella terza fase, che dovrà essere pronta entro fine 2021, verrà data piena attuazione a tutte le disposizioni dei nuovi regolamenti SIS.

collegati alle singole segnalazioni, vengono introdotte nuove possibilità tecniche e nuove capacità biometriche, viene consentito un più ampio accesso alle segnalazioni SIS a livello nazionale ed europeo. Quanto ai dati biometrici che possono essere conservati nel SIS al fine di consentire o confermare l'identificazione univoca del destinatario della segnalazione, questi possono consistere in fotografie, immagini del volto, dati dattiloscopici (impronte digitali e palmari), profili del DNA.

Altra banca dati istituita a livello europeo è Eurodac, un sistema centralizzato e informatizzato di identificazione delle impronte digitali dei richiedenti asilo e dei cittadini dei Paesi terzi non appartenenti allo Spazio economico europeo<sup>13</sup>. Eurodac – operativo dal gennaio 2003 – è stato originariamente creato per agevolare l'applicazione della Convenzione di Dublino del 15 giugno 1990 e, poi, del successivo regolamento Dublino sulla determinazione dello Stato competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri<sup>14</sup>.

Alle persone di età non inferiore a 14 anni che chiedono protezione internazionale in uno Stato membro (anche alla frontiera) e a coloro che sono fermati in relazione all'attraversamento irregolare di una frontiera esterna, sono rilevate le impronte digitali di tutte le dita ed i relativi dati devono essere trasmessi a Eurodac. Gli Stati membri, confrontando le impronte digitali con i dati presenti in Eurodac, possono verificare se il richiedente protezione internazionale o il cittadino straniero che si trovi irregolarmente sul territorio dell'Unione, abbia già presentato una domanda di protezione internazionale in altro Stato membro o se lo stesso sia entrato irregolarmente sul territorio dell'Unione. Accanto a questo utilizzo, presente

---

<sup>13</sup> V., in origine, regolamento (CE) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione della Convenzione di Dublino. Tale regolamento è stato successivamente abrogato e sostituito dal regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un Paese terzo o da un apolide 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 (...). Sui caratteri di Eurodac, v. E. BROUWER, *Eurodac: Its Limitations and Temptations*, in *European Journal of Migration and Law*, 2002, p. 231; E. GUILD, *Unreadable Papers? The EU's First Experiences with Biometrics: Examining Eurodac and the EU's Borders*, in J. LODGE (ed.), *Are You Who You Say You Are? The EU and Biometric Borders*, Nijmegen, 2007, p. 31; V. FERRARIS, *Eurodac e i limiti della legge: quando il diritto alla protezione dei dati personali non esiste*, in *Diritto, Immigrazione e Cittadinanza*, 2017, n. 2, p. 1.

<sup>14</sup> Regolamento (UE) n. 604/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un Paese terzo o da un apolide (c.d. Dublino III).

fin dall'origine, i dati di Eurodac sono adesso utilizzati anche al fine di prevenire, accertare o indagare reati di terrorismo o altri reati gravi<sup>15</sup>.

Le autorità che hanno accesso alla banca dati Eurodac sono, innanzitutto, le guardie di frontiera e le autorità competenti per l'asilo e l'immigrazione. A certe condizioni (pensate tenendo conto dell'esigenza di tutela del diritto fondamentale alla vita privata), anche le forze di polizia ed Europol possono confrontare le impronte digitali rilevate nel corso di indagini penali con quelle contenute in Eurodac. Ciò può avvenire, in particolare, solo se vi siano ragionevoli motivi di ritenere che tale consultazione sia necessaria per prevenire, accertare o indagare su un reato di terrorismo o altro reato grave e, comunque, solo in ultima istanza dopo lo svolgimento di diversi altri controlli.

Difficoltà sono state riscontrate nella prassi applicativa soprattutto con riferimento ai casi di cittadini di alcuni Stati terzi (in particolare, eritrei e siriani) che si sono rifiutati di consentire il rilevamento delle impronte digitali. La Commissione europea, tenendo conto di tali problematiche, ha elaborato alcune *best practices* suggerendo determinati approcci comuni agli Stati membri<sup>16</sup>. Nelle stesse viene indicato, ad es., che gli Stati membri dovrebbero informare il destinatario dei controlli dell'obbligo di sottoporsi al rilevamento delle impronte sulla base del diritto dell'Unione, spiegando che è nel suo interesse cooperare pienamente. L'interessato, infatti, in caso di rifiuto a cooperare, può essere considerato migrante irregolare e lo Stato membro può anche adottare nei suoi confronti misure coercitive a carattere detentivo. L'interessato corre poi il rischio di vedersi applicata una procedura accelerata, con maggiore probabilità che la domanda di asilo venga ritenuta manifestamente infondata. In tali casi, un ordine di espulsione può essere accompagnato da un divieto di ingresso sul territorio dell'Unione per cinque anni. Lo Stato membro, se non riesce a farlo altrimenti, può raccogliere coercitivamente le impronte digitali, facendo comunque attenzione a rispettare la dignità e l'integrità fisica dell'interessato, nonché le particolari esigenze delle persone più vulnerabili. Qualora l'interessato danneggi le sue impronte digitali, lo Stato membro può tenerlo in stato di detenzione per il periodo necessario a consentire che le impronte possano essere rilevate.

---

<sup>15</sup> Tale ampliamento dell'ambito di applicazione di Eurodac è stato introdotto con il citato regolamento Dublino III.

<sup>16</sup> Commission staff working document on Implementation of the Eurodac as regards the obligation to take fingerprints, SWD (2015) 150 final del 27 maggio 2020.

Terza banca dati istituita a livello di Unione europea è il VIS (Sistema d'informazione visti)<sup>17</sup>. Il VIS è funzionale all'attuazione della politica comune riguardante il rilascio di visti per soggiorni di breve durata e permette di scambiare dati ed informazioni – sulle domande di visto (incluso fotografie ed impronte digitali) e sulle relative decisioni – tra i consolati degli Stati membri nel mondo, le autorità centrali competenti per i visti, le autorità nazionali poste ai valichi di frontiera esterni. Consente poi di svolgere confronti biometrici, principalmente delle impronte digitali, ai fini di identificazione e verifica. L'impiego del VIS permette di migliorare la procedura relativa alle domande di visto, contribuisce alla lotta all'elusione dei criteri di determinazione dello Stato membro competente per l'esame delle relative domande, alla lotta contro la frode, all'esecuzione dei controlli ai valichi di frontiera, all'identificazione di qualsiasi persona che non soddisfi o non soddisfi più le condizioni di ingresso, soggiorno o residenza sul territorio degli Stati membri, all'applicazione del regolamento Dublino ed alla prevenzione delle minacce alla sicurezza interna degli Stati membri.

Le autorità per il visto, l'asilo e l'immigrazione e le autorità di controllo alla frontiera hanno accesso alla banca dati VIS per verificare l'identità del titolare del visto e l'autenticità del visto. In specifici casi, anche le forze di polizia ed Europol possono consultarla ai fini della prevenzione e della lotta al terrorismo e ad altre forme gravi di criminalità.

Un ulteriore strumento introdotto in vista del rafforzamento della sorveglianza digitale delle frontiere dell'area Schengen è rappresentato dal c.d. *Entry/Exit System* (EES), un sistema IT automatico per la registrazione di ingressi e uscite che è stato istituito dal regolamento n. 2017/2226<sup>18</sup> e la cui piena operatività è prevista per la prima metà del 2022. Con tale sistema verranno registrati i dati di ingresso, di uscita e di respingimento dei cittadini di Paesi terzi che attraversano le frontiere esterne dell'area Schengen. Si applicherà sia a chi ha bisogno di un visto di soggiorno di breve durata, sia a chi proviene da Stati terzi esenti dall'obbligo del visto. L'EES registrerà inoltre i dati dei cittadini di Stati terzi ai quali sia stato rifiutato l'ingresso per un soggiorno di breve durata. L'EES conserverà i dati sull'identità, sui documenti di viaggio e quelli biometrici. I dati dei viaggiatori che

<sup>17</sup> Cfr. decisione 2004/512/CE del Consiglio, dell'8 giugno 2004, che istituisce il sistema di informazione visti (VIS) e il regolamento n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS).

<sup>18</sup> Regolamento (UE) n. 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di Paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto (...).

rispettano le norme di durata del soggiorno breve autorizzato verranno conservati per un periodo di tre anni, mentre quelli dei viaggiatori che hanno superato lo scadere del periodo di soggiorno autorizzato (c.d. *overstayers*) verranno conservati per un periodo di cinque anni. I dati conservati saranno accessibili alle autorità di frontiera, alle autorità incaricate del rilascio dei visti e alle autorità responsabili di monitorare se i cittadini di Paesi extra UE soddisfano le condizioni di ingresso o di soggiorno. Allo scopo di prevenire, accertare e indagare su reati di terrorismo o altri reati gravi, autorità incaricate dell'applicazione della legge designate ed Europol potranno richiedere di consultare i dati dell'EES. L'EES sostituirà l'attuale sistema di apposizione manuale del timbro sul passaporto, che viene considerato dispendioso in termini di tempo e non in grado di fornire dati affidabili sull'attraversamento dei valichi di frontiera, né di consentire di rintracciare i soggiornanti fuori termine.

Menzione a parte merita, poi, il Sistema europeo di informazione e autorizzazione ai viaggi, ETIAS, che è stato introdotto dal regolamento n. 2018/1240<sup>19</sup> per consentire di raccogliere in modo automatizzato informazioni sui cittadini di Paesi terzi esenti dal visto addirittura prima del loro arrivo alle frontiere esterne, in modo tale da poter valutare eventuali rischi di migrazione irregolare, sicurezza o salute pubblica. Il sistema prevede che i cittadini di Paesi terzi in questione siano tenuti a richiedere, in via telematica, un'autorizzazione al viaggio con "sufficiente anticipo" rispetto al viaggio previsto oppure, se si trovano già sul territorio degli Stati membri, prima della scadenza della validità dell'autorizzazione che già possiedono. Nonostante che il regolamento istitutivo precisi che l'autorizzazione è per sua natura diversa da un visto e che non richiederà maggiori informazioni, né oneri più gravosi ai richiedenti rispetto ad un visto, sono molti i profili critici che il meccanismo in questione solleva in ordine al rispetto dei diritti dei viaggiatori provenienti da Paesi terzi<sup>20</sup>.

Le modifiche apportate al Codice frontiere Schengen da parte del regolamento n. 2017/458<sup>21</sup> hanno poi tra l'altro permesso che, sia nei confronti dei beneficiari della libera circolazione, sia della generalità dei cittadini di Stati terzi, le verifiche nelle banche dati possano essere compiute

---

<sup>19</sup> Regolamento (UE) n. 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (...).

<sup>20</sup> V. ad es. S. PEERS, *Brave new world? The new EU law on travel authorisation for non-EU citizens*, 26 aprile 2018, <http://eulawanalysis.blogspot.com/2018/04/>.

<sup>21</sup> V. regolamento (UE) n. 2017/458 del Parlamento europeo e del Consiglio, del 15 marzo 2017 che modifica il regolamento (UE) n. 2016/399 per quanto riguarda il rafforzamento delle verifiche nelle banche dati pertinenti alle frontiere esterne.

anche in anticipo rispetto all'arrivo in frontiera<sup>22</sup>. In particolare, tali verifiche possono essere compiute sulla base dei dati dei passeggeri ricevuti dai vettori, dati che poi dovranno essere verificati al valico di frontiera mettendoli a confronto con i dati contenuti nel documento di viaggio.

Dalla panoramica appena svolta emerge che il quadro giuridico esistente si caratterizza per la coesistenza di vari strumenti basati sull'impiego di tecnologie digitali e che mirano a sottoporre a controllo i cittadini di Stati terzi che giungono alle frontiere esterne dell'Unione. Il cittadino di Stato terzo è sottoposto sistematicamente al controllo nel SIS; laddove chiedi protezione internazionale o sia fermato nel tentativo di attraversare le frontiere irregolarmente, vengono rilevate le impronte digitali per un loro inserimento nel sistema Eurodac; laddove abbia l'obbligo di possedere un visto per un soggiorno di breve durata, è altresì sottoposto al controllo nella banca dati VIS. A ciò si aggiungono, poi, i nuovi sistemi di raccolta dati EES (per la registrazione di ingressi e uscite di tutti i cittadini di Paesi terzi che attraversano le frontiere esterne) e ETIAS (per la raccolta di informazioni sui cittadini di Paesi terzi esenti dal visto addirittura prima del loro arrivo alle frontiere esterne).

La consapevolezza delle difficoltà derivanti dal parallelo funzionamento di una pluralità di banche dati attive su piattaforme tecnologiche distinte, ha spinto le istituzioni dell'UE a porre in essere le riforme necessarie per consentire l'interoperabilità tra i vari sistemi di informazione applicabili nell'ambito dello spazio di libertà, sicurezza e giustizia. Tra gli atti normativi a tal fine adottati, meritano particolare menzione i regolamenti n. 2019/817 e n. 2019/818<sup>23</sup> che, peraltro, sono già stati oggetto di critiche per il rischio che l'interconnessione di sistemi IT pone sia dal punto di vista della moltiplicazione di eventuali errori che gli stessi possono contenere, sia dal punto di vista della tutela dei diritti fondamentali dei titolari di tali dati e, in particolare, del rispetto della normativa a tutela della vita privata<sup>24</sup>.

<sup>22</sup> V. art. 8, par. 2 *sexies*, e art. 8, par. 3, lett. i *bis*), del regolamento n. 2016/399.

<sup>23</sup> Regolamento (UE) n. 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti (...); regolamento (UE) n. 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione (...).

<sup>24</sup> V. E. BROUWER, *Interoperability of Databases and Interstate Trust: a Perilous Combination for Fundamental Rights*, in *Verfassungsblog.de*, 25.5.2019; G. CAGGIANO, *L'interoperabilità fra le banche-dati dell'Unione sui cittadini degli Stati membri*, in AA.VV., *Temi e questioni di diritto dell'Unione europea, Scritti offerti a Claudia Morviducci*, Bari, 2019, p. 657 e spec. p. 664 ss.

**3. Elemento essenziale nell'ambito del nuovo Patto sulla migrazione e l'asilo** è rappresentato dal rafforzamento delle frontiere esterne. Solo mediante tale rafforzamento viene ritenuto possibile realizzare un più adeguato funzionamento dello spazio Schengen senza controlli alle frontiere interne.

Tra le misure previste per il conseguimento di tale obiettivo, viene indicata l'esigenza di avvalersi di sistemi informatici aggiornati in grado di consentire la registrazione degli arrivi e dei richiedenti asilo<sup>25</sup>.

In particolare, la Commissione afferma l'esigenza che le varie banche dati esistenti funzionino secondo il criterio dell'interoperabilità e fissa un cronoprogramma per l'attuazione delle riforme a tal fine previste.

All'interno del nuovo Patto, viene infatti sottolineato che tutti i sistemi europei relativi a frontiere, migrazione, sicurezza e giustizia debbano essere tra loro interoperabili. I diversi strumenti esistenti dovranno cioè essere in grado di dialogare tra loro in modo tale da consentire alle autorità nazionali di avere informazioni complete, affidabili e precise. In questo modo, la Commissione ritiene che verrà dato un forte impulso alla lotta contro la frode d'identità<sup>26</sup>.

La Commissione dimostra, quindi, di aver ormai definitivamente abbandonato la convinzione, in passato dalla stessa affermata, secondo cui la creazione di un sistema di informazione unico e globale a livello di Unione europea con finalità multiple, costituirebbe una limitazione grave e illegittima del diritto della persona alla vita privata e alla protezione dei dati<sup>27</sup>. Già da qualche anno, infatti, alla luce del nuovo quadro generale di protezione dei dati personali nell'UE e dei significativi progressi nel campo delle tecnologie e della sicurezza informatica, la Commissione ha ritenuto possibile superare la frammentazione dell'architettura della gestione dei dati raccolti per il controllo delle frontiere esterne e la sicurezza dell'Unione<sup>28</sup>.

Quanto al cronoprogramma fissato a tal fine all'interno del nuovo Patto, la Commissione ritiene essenziale che i sistemi di informazione aggiornati siano operativi e pienamente interoperabili entro la fine del 2023. Anche per la procedura per il rilascio dei visti si prevede la completa digitalizzazione

---

<sup>25</sup> COM (2020) 609, p. 14.

<sup>26</sup> *Ibidem*.

<sup>27</sup> In tal senso, v. Comunicazione della Commissione al Parlamento europeo e al Consiglio, Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia, COM (2010) 385 def. del 20 luglio 2010, p. 3.

<sup>28</sup> V. in tal senso, Comunicazione della Commissione al Parlamento europeo e al Consiglio, Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza, COM (2016) 205 final del 6 aprile 2016, p. 5.

entro il 2025, con il rilascio di un visto digitale e la possibilità di presentare le domande di visto *on-line*.

Traspare, ad ogni modo, la consapevolezza che le riforme adottate al fine di creare una nuova architettura dei diversi sistemi informativi dell'Unione presentano profili di criticità. Da una parte, la Commissione afferma che ogni banca dati, nonostante l'interoperabilità, dovrà mantenere le salvaguardie che ciascuna di esse stabilisce. Dall'altra, afferma che sarà suo compito monitorare e sostenere i preparativi che sono chiamati a compiere gli Stati membri e le diverse Agenzie dell'Unione. A tal fine, la Commissione potrà avvalersi di una procedura di allarme rapido per i sistemi informativi, che le consentirà di intervenire tempestivamente e, se necessario, di avviare un'azione correttiva rapida e mirata. Tramite tale procedura, verranno inviate informazioni ad un *forum* di attuazione ad alto livello composto da coordinatori in rappresentanza degli Stati membri, della Commissione e delle Agenzie e che si riunirà con cadenza semestrale<sup>29</sup>.

All'interno del pacchetto di misure proposte con il nuovo Patto, gli atti che, più di altri, si soffermano sull'esigenza di procedere verso il rafforzamento del controllo digitale delle frontiere, sono rappresentati dalla proposta di regolamento volta ad introdurre una procedura di esame pre-ingresso e dalla proposta di riforma della banca dati Eurodac. All'esame degli aspetti di tali proposte che, ai nostri fini, appaiono più rilevanti, dedicheremo i due prossimi paragrafi. Fin d'ora anticipiamo, comunque, che nelle due proposte in questione appare chiara la scelta della Commissione a favore di meccanismi che favoriscono e rendono sempre più effettiva l'interoperabilità tra i diversi sistemi di raccolta e conservazione dei dati.

**4.** Uno degli strumenti più significativi elaborati dalla Commissione europea nell'ambito del pacchetto di misure collegate al nuovo Patto sulla migrazione e l'asilo, presentato il 23 settembre 2020, è senz'altro rappresentato dalla proposta di regolamento volta ad introdurre una procedura di pre-ingresso cui vengono sottoposti: *a)* tutti i cittadini di Paesi terzi che hanno attraversato le frontiere esterne in modo non autorizzato; *b)* coloro che hanno presentato domanda di protezione internazionale durante le verifiche di frontiera senza soddisfare le condizioni di ingresso; *c)* coloro che sono sbarcati a seguito di un'operazione di ricerca e soccorso<sup>30</sup>.

---

<sup>29</sup> *Ibidem*.

<sup>30</sup> V. art. 1 della proposta di regolamento del Parlamento europeo e del Consiglio che introduce accertamenti nei confronti dei cittadini di Paesi terzi alle frontiere esterne (...), COM (2020) 612 final, del 23 settembre 2020. A commento della proposta, v. il contributo di G. CAGGIANO in questo *Focus*; L. JAKULEVIČIENĖ, *Re-decoration of existing practices?*

Con riferimento a tali cittadini di Stati terzi, la proposta mira a creare un meccanismo uniforme che dovrebbe consentire di indirizzare gli stessi verso la procedura più adeguata<sup>31</sup>. I controlli svolti in tale fase sono infatti funzionali ad accelerare il processo volto a determinare lo *status* di una persona ed il tipo di procedura da applicare<sup>32</sup>.

Tra gli accertamenti da compiersi nell'ambito della procedura di pre-ingresso, rilevano, ai nostri fini: la verifica dell'identità mediante la consultazione delle informazioni contenute nella banche dati europee; la registrazione dei dati biometrici (relativi alle impronte digitali e all'immagine del volto) nelle banche dati pertinenti, nella misura in cui non sia ancora avvenuta; il controllo di sicurezza mediante interrogazione delle pertinenti banche dati nazionali e dell'UE, in particolare il SIS, volto a verificare che la persona non rappresenti una minaccia per la sicurezza interna.

Gli accertamenti obbligatori nei confronti dei cittadini di Paesi terzi fermati al di fuori dei valichi di frontiera dovrebbero applicarsi alle persone delle quali gli Stati membri sono tenuti a rilevare i dati biometrici conformemente al regolamento Eurodac. Quanto invece a coloro che si presentano ai valichi di frontiera, gli accertamenti in questione devono svolgersi nel caso in cui si tratti di cittadini di Stati terzi che non soddisfano le condizioni di ingresso di cui all'art. 6 del Codice frontiere Schengen e che fanno domanda di protezione internazionale.

Al fine di stabilire l'identità della persona sottoposta agli accertamenti, viene avviata, alla presenza dell'interessato, una verifica dei dati biometrici di quest'ultimo che vengono riscontrati, mediante l'interrogazione di ogni banca dati pertinente<sup>33</sup> e dei dati contenuti nel CIR, l'archivio comune di dati di identità, che è stato istituito mediante il regolamento n. 2019/817<sup>34</sup>. L'impiego del CIR rappresenterebbe, secondo quanto specificato nel testo della proposta, uno strumento rapido ed affidabile<sup>35</sup>. Il CIR, infatti, consente di consultare simultaneamente tutti i dati di identità presenti nell'EES, nel VIS, nell'ETIAS, nell'Eurodac<sup>36</sup> e nell'ECRIS-TCN<sup>37</sup>. Se nel CIR sono

---

*Proposed screening procedures at the EU external borders*, in *Immigration and Asylum Law and Policy*, eumigrationlawblog.eu, 27 ottobre 2020.

<sup>31</sup> COM (2020) 612 final, considerando 8.

<sup>32</sup> V. COM (2020) 609 final, p. 4.

<sup>33</sup> V. COM (2020) 612 final, art. 10, par. 2.

<sup>34</sup> V. regolamento (UE) n. 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti (...).

<sup>35</sup> V. COM (2020) 612 final, considerando n. 29.

<sup>36</sup> Sui caratteri di tali banche dati, v. *supra*, par. 2.

<sup>37</sup> ECRIS-TCN è un sistema che permette di verificare quali altri Stati membri siano in possesso di informazioni sul casellario giudiziale di un cittadino di Stato terzo. Pur

conservate informazioni riguardanti l'interessato, le autorità dello Stato membro vi hanno accesso per consultare i dati di identità, i dati del documento di viaggio e i dati biometrici, senza che il CIR fornisca alcuna indicazione sul sistema di informazione dell'UE cui tali dati appartengono<sup>38</sup>.

In questo modo, viene proposta l'estensione dell'ambito di applicazione del CIR, visto che il regolamento istitutivo di tale banca dati aveva previsto che il ricorso alla stessa sarebbe stato possibile solo nel contesto dei controlli di polizia nel territorio degli Stati membri<sup>39</sup>. Tale estensione si pone certo in linea con la logica della interoperabilità tra i diversi sistemi IT istituiti a livello di diritto dell'Unione. È indubbio, peraltro, che così facendo si contribuisce a rafforzare la sensazione che le misure volte a gestire i flussi migratori vengano sempre più percepite come necessariamente associate ai controlli di polizia volti invece a garantire la sicurezza dell'area Schengen. A ciò si aggiunge, poi, che la rapidità con cui i controlli devono essere compiuti nell'ambito della procedura di pre-ingresso, può quanto meno sollevare perplessità in ordine alla loro reale affidabilità.

I controlli di sicurezza cui sono sottoposti i cittadini di Stati terzi che sono presenti alle frontiere esterne e che non soddisfino le condizioni di ingresso o che sono sbarcati a seguito di un'operazione di ricerca e soccorso, non possono essere minori rispetto a quelli che vengono compiuti nei confronti dei cittadini di Paesi terzi che hanno presentato una domanda di autorizzazione all'ingresso nell'UE per un soggiorno di breve durata<sup>40</sup>. Di conseguenza, i cittadini di Stati terzi che, in virtù della loro nazionalità, sono esenti dall'obbligo del visto, sono comunque tenuti a presentare domanda di autorizzazione ai viaggi prima di recarsi nell'UE per un soggiorno di breve durata e in tale occasione sono sottoposti a controlli di sicurezza mediante la consultazione del sistema informazione visti (VIS), del sistema di informazione Schengen (SIS), del sistema di ingressi/uscite (EES), del sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), dei dati Europol, dei dati presenti nel sistema ECRIS-TCN, delle banche dati

---

trattandosi, quindi, di uno strumento volto a prevenire e combattere la criminalità, compresa la criminalità organizzata ed il terrorismo, lo stesso può essere utilizzato anche nell'ambito di procedure in materia di visti, acquisizione della cittadinanza e migrazione, comprese quelle di asilo. In proposito, v. art. 7, par. 1 del regolamento (UE) n. 2019/816 del Parlamento europeo e del Consiglio, 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 giudiziari (...).

<sup>38</sup> COM (2020) 612 final, considerando 30.

<sup>39</sup> COM (2020) 612 final, considerando 31.

<sup>40</sup> I controlli in questione e le modalità con cui gli stessi sono espletati vengono disciplinati dagli articoli 11 e 12, COM (2020) 612 final.

Interpol sui documenti di viaggio rubati o smarriti (SLTD) e sui documenti di viaggio associati a segnalazioni (TDAWN)<sup>41</sup>.

A maggior ragione, tali controlli sono applicabili alle persone che, in virtù della loro cittadinanza, sono sottoposte all'obbligo del visto conformemente a quanto previsto dal c.d. regolamento liste<sup>42</sup>.

Le ricerche nelle predette banche dati devono essere svolte in modo tale da garantire che dalle stesse siano estratti solo i dati indispensabili ai fini dei controlli di sicurezza<sup>43</sup>. Di conseguenza, i dati estratti si limitano ad indicare se l'interessato si è visto rifiutare l'autorizzazione al viaggio o all'ingresso, nonché le decisioni di rifiuto, annullamento o revoca di un visto o di un permesso di soggiorno giustificati da motivi di sicurezza<sup>44</sup>.

Se, a seguito della consultazione delle banche dati, emergano corrispondenze con dati rilevanti a fini di sicurezza, l'autorità competente dello Stato membro è tenuta a informarne, a seconda dei casi, Europol o Interpol, in modo tale da consentire di adottare, se necessario, le opportune misure<sup>45</sup>.

Nel commentare la proposta, il Garante europeo della protezione dei dati personali ha osservato che la stessa appare molto generica con riferimento alle modalità di raccolta dei dati dei cittadini di Stati terzi. Ciò può comportare rischi per la protezione della *privacy* dei soggetti interessati, anche in considerazione del fatto che gli Stati membri impiegano tipologie eterogenee nell'identificazione e verifica dell'identità dei cittadini degli Stati terzi nel caso in cui manchino prove documentali affidabili<sup>46</sup>. Tra i diversi mezzi utilizzati<sup>47</sup>, alcuni appaiono particolarmente invasivi e senz'altro in grado di produrre effetti pregiudizievoli per la tutela della vita personale dell'interessato. Si pensi, ad es., al fatto che alcuni Stati membri, oltre a sottoporre l'interessato ad un'intervista nel corso del quale si cerca di capire la provenienza dello stesso anche mediante l'esame della lingua parlata, analizzano le transazioni elettroniche compiute in modo tale da ricostruire i

---

<sup>41</sup> COM (2020) 612 final, considerando 37.

<sup>42</sup> Regolamento (UE) n. 2018/1806 del Parlamento europeo e del Consiglio, del 14 novembre 2018, che adotta l'elenco dei Paesi terzi i cui cittadini devono essere in possesso del visto all'atto dell'attraversamento delle frontiere esterne e l'elenco dei Paesi terzi i cui cittadini sono esenti da tale obbligo.

<sup>43</sup> COM (2020) 612 final, considerando 40.

<sup>44</sup> COM (2020) 612 final, art. 11, par. 4.

<sup>45</sup> COM (2020) 612 final, art. 12.

<sup>46</sup> EDPS, *Opinion 9/2020*, cit., par. 31.

<sup>47</sup> Per un quadro dettagliato sulle diverse modalità con cui i singoli Stati membri procedono all'accertamento dell'identità dei cittadini degli Stati terzi nel caso in cui non abbiano la disponibilità di prove documentali, v. EMN Synthesis Report for the EMN Focussed Study 2017, *Challenges and practices for establishing the identity of third-country nationals in migration procedures*, dicembre 2017, p. 31 ss.

contatti dallo stesso avuti con autorità pubbliche o private. Così facendo, gli Stati membri possono venire a conoscenza di dati quali, ad es., quelli relativi al pagamento di tasse o ai benefici sociali usufruiti o, ancora, ai rapporti bancari intercorsi. Talvolta, poi, gli Stati membri prevedono la possibilità di compiere verifiche accedendo ai *social media* utilizzati dall'interessato. Gli accertamenti possono a tal fine comportare la confisca, temporanea o permanente, di *smartphone* o di altri strumenti digitali, dai quali vengono ricavate informazioni relative all'interessato. La mancata specificazione delle modalità di raccolta dei dati nell'ambito della procedura di pre-ingresso lascia dubbi sull'effettiva rispondenza delle stesse a quanto strettamente necessario per il perseguimento dei fini prefissati.

5. Tra le misure proposte con il nuovo Patto sulla migrazione e l'asilo rileva, ai nostri fini, la prospettata revisione del regolamento Eurodac.

In proposito, occorre innanzitutto ricordare che già nel 2016 la Commissione europea aveva presentato una proposta di riforma del regolamento in questione<sup>48</sup>. Parlamento europeo e Consiglio erano riusciti a trovare un accordo sulle principali questioni problematiche ma, ciò nonostante, la volontà di chiudere il negoziato insieme alla revisione del sistema Dublino aveva impedito di giungere all'approvazione della riforma<sup>49</sup>.

Con il nuovo Patto sulla migrazione e l'asilo, la Commissione ha elaborato una versione modificata della proposta di riforma del regolamento Eurodac<sup>50</sup>, tenendo fermi, come punto di partenza, i risultati conseguiti durante il precedente negoziato. La proposta del 2020 riprende, quindi, l'intenzione di ampliare l'ambito di applicazione di Eurodac e di trasformare

---

<sup>48</sup> Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di Paese terzo o da un apolide, per l'identificazione di cittadini di Paesi terzi o 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 (rifusione), COM (2016) 272 final del 4 maggio 2016.

<sup>49</sup> In particolare, un accordo sulla maggior parte delle questioni in sospeso è stato raggiunto nel corso del trilogico del 19 giugno 2018. V. Consiglio dell'Unione europea, Doc. N. 12826/18 del 4 ottobre 2018, par. 8.

<sup>50</sup> Proposta modificata di regolamento del Parlamento europeo e del Consiglio che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) XXX/XXX [*regolamento sulla gestione dell'asilo e della migrazione*] e del regolamento (UE) XXX/XXX [*regolamento sul reinsediamento*], per l'identificazione di cittadini di Paesi terzi o 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 (...), COM (2020) 614 final del 23.9.2020.

la stessa in una banca dati comune europea a sostegno delle politiche dell'UE in materia di asilo, reinsediamento e migrazione irregolare. Viene quindi in gran parte diluita la finalità originaria di Eurodac che, come già osservato, era quella di costituire uno strumento volto ad agevolare il compito di determinare lo Stato membro competente per l'esame di una domanda di protezione internazionale.

Vengono poi introdotte modifiche finalizzate a garantire il corretto funzionamento di Eurodac nell'ambito del nuovo quadro per l'interoperabilità. Visto che all'interno di Eurodac sono, allo stato, incluse solo le impronte digitali e non anche altri dati sull'identità dell'interessato, risulta difficile comparare le informazioni contenute in tale sistema con quelle di altre banche dati esistenti. L'ampliamento delle informazioni raccolte è quindi avvertito come strumento necessario per allineare Eurodac agli altri sistemi IT e consentire, di conseguenza, un'effettiva possibilità di dialogo tra gli stessi.

Nella riforma proposta nel 2016, poi, l'ampliamento dei dati raccolti all'interno di Eurodac era anche dovuta alla necessità di prendere atto delle difficoltà che si manifestano in caso di rifiuto di rilevamento delle impronte digitali da parte dei cittadini di Stati terzi. Per superare un simile *impasse*, era quindi già stato proposto di includere in Eurodac non più soltanto impronte digitali, ma anche immagini facciali, nonché informazioni riguardanti il nome, la cittadinanza, il luogo e la data di nascita, il documento di viaggio dell'interessato. Nel caso in cui quest'ultimo fosse un richiedente asilo, veniva previsto l'inserimento anche del numero della domanda di asilo e dello Stato membro responsabile a prendere in carico la stessa. Sempre nella proposta del 2016 era stato previsto l'abbassamento, da 14 a 6 anni, dell'età dei soggetti sottoposti al rilevamento delle impronte digitali. Tale modifica veniva giustificata alla luce dell'evidente aumento del traffico dei minori di età inferiore a 14 anni<sup>51</sup>. Inoltre, visto anche che spesso tali minori giungono sul territorio degli Stati membri separati dai genitori, il rilevamento degli elementi biometrici veniva considerato utile per stabilire legami familiari nei confronti di genitori o altri parenti soggiornanti sul territorio di diversi Stati membri. L'ampliamento dei minori destinatari del rilevamento poteva poi contribuire ad impedire che i bambini venissero sottratti all'intervento delle istituzioni che si occupano della cura degli stessi ed ai servizi sociali.

La proposta del 2020 mantiene l'ampliamento dei dati raccolti all'interno di Eurodac già previsto nel testo del 2016. Rispetto a quest'ultimo, nella più

---

<sup>51</sup> Alcuni dei motivi della proposta in questione sono evidenziati nella relazione introduttiva alla proposta COM (2016) 272 final, cit., p. 2.

recente versione della proposta va segnalata, tra l'altro, la previsione in base alla quale tutti i dati registrati in Eurodac corrispondenti allo stesso cittadino di Stato terzo o apolide, dovrebbero essere collegati in un'unica sequenza, in modo da consentire al sistema di conteggiare i richiedenti e, di conseguenza, fornire un quadro preciso del numero di richiedenti asilo nell'Unione europea<sup>52</sup>. Mediante l'aggregazione di tali dati con altri dati, quali, ad es., quelli relativi ai trasferimenti a norma del regolamento sulla gestione dell'asilo e della migrazione<sup>53</sup>, sarà possibile dare un contributo utile al fine di valutare i movimenti secondari all'interno dell'Unione. Bisogna tener conto, infatti, che il sistema attualmente vigente consente di calcolare il numero di procedure amministrative avviate al fine di ottenere una forma di protezione internazionale, ma non anche di calcolare il numero delle persone che hanno presentato le relative domande.

Nel valutare l'impatto sulla protezione dei dati personali della misura in questione, la Commissione ha affermato che tale nuovo meccanismo, non comportando la raccolta di dati aggiuntivi, non impedisce agli Stati membri di esercitare le proprie responsabilità per il trattamento dei dati derivanti dal regolamento GDPR<sup>54</sup> e non pregiudica l'esercizio, da parte degli interessati, dei diritti di accesso, rettifica, cancellazione, limitazione<sup>55</sup>.

Pur essendo chiaro l'intento perseguito mediante il collegamento in un'unica sequenza di tutti i dati registrati in Eurodac, critiche sono state espresse dal Garante europeo della protezione dei dati personali sulla base della considerazione che la modifica proposta deve essere valutata anche tenendo conto dell'estensione delle categorie di dati personali processati nella banca dati in questione e dell'ampliamento delle autorità che hanno accesso agli stessi nel contesto dell'interoperabilità tra diverse banche dati<sup>56</sup>. Lo stesso Garante europeo, poi, visto che, ai sensi dell'art. 4, par. 2, della

<sup>52</sup> V. il considerando n. 14 e l'art. 4 par. 6 della proposta COM (2020) 614 final.

<sup>53</sup> V. proposta di regolamento del Parlamento europeo e del Consiglio sulla gestione dell'asilo e della migrazione e che modifica la direttiva 2003/109/CE del Consiglio e la proposta di regolamento (UE) XXX/XXX [Fondo Asilo e migrazione], COM (2020) 610 final del 23 settembre 2020. A commento della proposta, v. M. T. MOSCHETTA, *L'impasse Dublino: l'incompiuta riforma dei criteri di competenza nella proposta di regolamento su asilo e immigrazione*, in *I Post di AISDUE*, 2020, in questo *Focus*, p. 78 e spec. p. 81 ss.

<sup>54</sup> Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

<sup>55</sup> In tal senso, v. Commission Staff Working Document, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on asylum and migration management and amending Council Directive (EC) 2003/109 and the proposed Regulation (EU) XXX/XXX [Asylum and Migration Fund], SWD (2020) 207 final del 23 settembre 2020, p. 81 e pp. 102-103.

<sup>56</sup> EDPS, *Opinion 9/2020*, cit., par. 16.

proposta modificata, per parte dei dati raccolti viene prevista la conservazione nel CIR, mentre per i rimanenti dati viene prevista la conservazione nel sistema centrale Eurodac, ha sottolineato l'esigenza di chiarire esattamente quali dati e in quali sistemi devono essere conservati.

Più in generale, poi, va ribadito che l'estensione dell'ambito di applicazione della banca dati Eurodac (che, come sopra osservato, dovrà consentire il contrasto al fenomeno dei movimenti secondari e facilitare il ritorno dei migranti irregolari) desta preoccupazioni dal punto di vista del rispetto del principio di limitazione delle finalità (c.d. *purpose limitation principle*)<sup>57</sup>. In virtù di tale principio, il trattamento dei dati personali deve essere compiuto in funzione di una finalità determinata, esplicita e legittima. Visto che, in origine, Eurodac era stato concepito esclusivamente come strumento di supporto per l'attuazione del regolamento Dublino, è indubbio che le nuove finalità rischiano di non essere in linea con quelle previste al momento in cui sono stati raccolti i dati fino ad oggi presenti all'interno di tale banca dati<sup>58</sup>.

Tali rischi sono poi accentuati dal fatto che Eurodac, secondo la proposta della Commissione, verrà inserita nel novero delle banche dati sottoposte al criterio della interoperabilità. Ciò comporterà, ad esempio, che autorità di polizia saranno in grado di interrogare il CIR con i dati biometrici di una persona raccolti durante un controllo svolto al solo fine di identificare la stessa. Bisogna tener conto che, già in base alla versione attualmente vigente del regolamento Eurodac, le autorità di polizia e Europol potevano interrogare la banca dati in questione al fine di prevenire, investigare ed accertare la commissione di gravi crimini o reati terroristi. È indubbio, però, che con la piena interoperabilità di Eurodac con le altre banche dati, le potenzialità di tali impieghi vengono aumentati in modo esponenziale.

Bisogna poi tener conto che la proposta del 2020 prevede, tra l'altro, l'inserimento, tra le informazioni raccolte all'interno di Eurodac, di un nuovo campo nel quale registrare un'allerta di sicurezza nel caso in cui il cittadino di Stato terzo o l'apolide possa rappresentare una minaccia per la sicurezza<sup>59</sup>.

---

<sup>57</sup> In generale, sul principio in questione, v. E. BROWER, *Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation*, in L. BESSELINK, F. PENNING, S. PRECHAL (eds.), *The Eclipse of the Legality Principle in the European Union*, Alpen aan den Rijn, 2011, p. 273; Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, Doc. 00569/13/EN, WP 203 del 2 aprile 2013.

<sup>58</sup> In tal senso, v. EDPS, *Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)*, *Opinion 07/2016*, 21 settembre 2016, p. 8.

<sup>59</sup> V. art. 12, lett. v) della proposta COM (2020) 614 final.

L'impressione complessiva che si ricava è quella di aver voluto rafforzare la tendenza, indubbiamente già presente nella politica di immigrazione dell'Unione, ad intrecciare gli strumenti predisposti in funzione dell'esame delle domande di asilo, al fine del contrasto all'immigrazione irregolare, e, infine, della prevenzione e lotta ai fenomeni criminali<sup>60</sup>.

6. L'indagine svolta ha permesso di evidenziare quanto lo sviluppo tecnologico sia sempre più rilevante nel controllo delle frontiere dell'Unione europea.

Per poter adeguatamente valutare la portata delle novità previste dal nuovo Patto in funzione del rafforzamento del controllo digitale delle frontiere, è stato preliminarmente necessario riepilogare il quadro giuridico esistente.

Le istituzioni dell'Unione, dopo aver creato banche dati (SIS, Eurodac, VIS, EES, ETIAS), ciascuna caratterizzata da finalità ben specifiche, ha compiuto, soprattutto con le riforme approvate nel 2019, una chiara scelta a favore dell'interoperabilità tra le diverse piattaforme digitali.

Questa scelta viene confermata e rafforzata all'interno del nuovo Patto. L'interoperabilità non rappresenta, quindi, una novità. Piuttosto, la Commissione dimostra, con il recente pacchetto di misure, di voler proseguire lungo la strada già intrapresa, nonostante i dubbi da più parti sollevati, derivanti dal rischio che l'interconnessione tra le varie banche dati può comportare dal punto di vista del rispetto del principio di limitazione delle finalità, principio essenziale ai fini della tutela dei dati personali dell'interessato.

Certo, la Commissione fa affidamento sugli sviluppi tecnologici che, a suo dire, rendono possibili soluzioni in grado di assicurare che il trattamento dei dati avvenga in conformità ai principi fissati nel GDPR.

Sul punto, sarà certo interessante verificare le applicazioni concrete dei meccanismi in questione, in modo tale da poter valutare – alla prova dei fatti – se le soluzioni tecniche siano effettivamente in grado di prevenire le paventate criticità dal punto di vista del rispetto dei dati personali.

Fin d'ora, peraltro, può lasciare perplessi il fatto che la Commissione abbia scelto di rafforzare l'interoperabilità senza prima aver potuto compiere una "valutazione *ex post*" della normativa a tal fine introdotta nel 2019.

---

<sup>60</sup> In tal senso, v. B. MENEZES QUEIROZ, *The Impact of EURODAC in EU Migration Law: The Era of Crimmigration?*, in *Market and Competition Law Review*, 2019, p. 157 e spec. p. 165.

Quest'ultima, infatti, non è ancora pienamente applicabile<sup>61</sup> e, di conseguenza, le sue implicazioni non sono del tutto chiare. Non sembra quindi che la Commissione abbia tenuto in adeguata considerazione il rilievo che, invece, una “valutazione *ex post*” della legislazione vigente dovrebbe avere nell'ambito del processo decisionale delle istituzioni dell'Unione, come sottolineato anche dall'Accordo interistituzionale “legiferare meglio”, concluso tra il Parlamento europeo, il Consiglio dell'Unione e la Commissione europea<sup>62</sup>.

Per quanto è comunque già possibile osservare, è indubbio che le soluzioni previste dal nuovo Patto, combinate con le misure già approvate con i regolamenti sull'interoperabilità, produrranno l'effetto di aumentare in modo esponenziale i dati a disposizione delle diverse autorità. Ciò può forse essere letto come un elemento positivo dal punto di vista del contrasto alle attività criminali. D'altra parte, però, così facendo viene rafforzata l'impressione che le istituzioni dell'Unione tendano ad associare i fenomeni migratori a quelli criminali. Tale impressione emerge anche dall'estensione dell'ambito di applicazione del regolamento Eurodac che, secondo la proposta della Commissione, è destinato a perdere la sua originaria funzione di strumento volto ad agevolare la determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale, per acquisire invece anche la funzione di contribuire al contrasto dei movimenti secondari all'interno dell'Unione e di facilitare il ritorno dei migranti irregolari.

Tra i vari profili che abbiamo evidenziato con riferimento alla procedura di pre-ingresso, uno degli aspetti che più preoccupa consiste nel fatto che la celerità che la caratterizza non sempre si accompagna ad una adeguata tutela dei diritti fondamentali degli interessati. Qualora la proposta in questione venga approvata, sulla base degli accertamenti compiuti tramite banche dati, nel giro di pochi giorni potranno essere prese decisioni che incideranno sulla permanenza o meno dell'interessato sul territorio dell'Unione. Tali termini brevi rendono, evidentemente, più difficoltoso l'esercizio effettivo di diritti di difesa che, in linea di principio, sono assicurati all'interessato.

---

<sup>61</sup> I regolamenti sull'interoperabilità (n. 2019/817 e n. 2019/818) prevedono infatti che la Commissione europea adotti una normativa di esecuzione al fine di integrare e attuare alcuni loro aspetti tecnici dettagliati. In proposito v. Relazione della Commissione al Parlamento europeo e al Consiglio sullo stato di avanzamento dei preparativi per la piena attuazione dei regolamenti sull'interoperabilità a norma dell'articolo 78, paragrafo 5, del regolamento (UE) 2019/817 e dell'articolo 74, paragrafo 4, del regolamento (UE) 2019/818, COM (2020) 428 final del 21 agosto 2020.

<sup>62</sup> V. GUUE L 123 del 12 maggio 2016, p. 1 e spec. p. 5.

Abbiamo ricordato, poi, che la proposta volta ad introdurre una procedura di pre-ingresso non tiene conto del fatto che le modalità di raccolta dei dati dei cittadini di Stati terzi sono eterogenee nei diversi Stati membri. Alcune di tali modalità sono particolarmente invasive e potenzialmente pregiudizievoli della vita privata degli interessati. Sono emersi, di conseguenza, dubbi sull'effettiva rispondenza degli strumenti previsti a quanto strettamente necessario per il perseguimento dei fini prefissati.

La moltiplicazione dei dati raccolti che è conseguente al rafforzamento dei controlli digitali, rappresenta, inevitabilmente, un fattore in grado di aumentare il rischio che eventuali errori nell'inserimento delle informazioni nelle banche dati possano produrre un effetto cumulato, oltremodo pregiudizievole per i diritti dell'interessato. Ciò, sia perché i dati in questione possono essere impiegati per giustificare l'allontanamento del cittadino dello Stato terzo dal territorio dell'Unione; sia perché ad essere in pericolo possono anche essere alcuni aspetti particolarmente sensibili della vita privata dell'interessato.

Molte delle problematiche alle quali abbiamo in questa sede fatto cenno erano già note alla Commissione europea. Nel nuovo Patto, così come già osservato da altri con riferimento a diversi profili<sup>63</sup>, anche ai fini del controllo digitale non sono state introdotte soluzioni particolarmente innovative.

Certo, le nuove possibilità offerte dai sistemi tecnologici devono senz'altro poter essere sfruttate nell'ambito dei controlli alle frontiere dell'Unione. Non bisogna però mai dimenticare la posizione di particolare debolezza in cui i migranti si trovano quando sono di fronte alle autorità degli Stati membri all'interno del cui territorio chiedono di entrare. Creare un'architettura digitale che produca l'effetto di mettere sotto sorveglianza tutti i viaggiatori e considerarli, *a priori*, come potenziali violatori della legge, non appare la soluzione più adeguata per una riforma che, secondo le parole della stessa Presidente della Commissione europea, si pone come un nuovo inizio ("*a fresh start*") per la politica di immigrazione dell'Unione<sup>64</sup>.

---

<sup>63</sup> V., ad es., P. DE PASQUALE, *Il Patto per la migrazione e l'asilo: più ombre che luci*, cit., p. 11 ss.

<sup>64</sup> V. *Press statement by President von der Leyen on the New Pact on Migration and Asylum*, 23 settembre 2020, disponibile al sito internet [https://ec.europa.eu/commission/presscorner/detail/it/statement\\_20\\_1727](https://ec.europa.eu/commission/presscorner/detail/it/statement_20_1727).

## **ABSTRACT**

### *The strengthening of digital borders in the New Pact on Migration and Asylum*

The article analyses the measures laid down in the New Pact on Migration and Asylum which aim at strengthening the digital surveillance at the EU's external borders. After having recapped the existing legal framework, attention has been paid to the use of database within the proposal introducing a screening of third country nationals at the external borders and to the relevant provisions foreseen by the proposal to recast the Eurodac regulation. The inquiry is carried out always bearing in mind that the securitarian logic that is apparent from the extended use of digital technologies for border surveillance should not be to the detriment of fundamental rights of migrants.

### *Il rafforzamento del controllo digitale nel nuovo Patto sulla migrazione e l'asilo*

Nel presente articolo vengono analizzate le misure che, all'interno del nuovo Patto sulla migrazione e l'asilo, mirano al rafforzamento della sorveglianza digitale delle frontiere esterne dell'Unione. Dopo aver riepilogato il quadro giuridico esistente, viene prestata particolare attenzione all'impiego delle banche dati nell'ambito della proposta volta ad introdurre una procedura di pre-ingresso, nonché alle novità previste nella proposta di riforma del regolamento Eurodac. L'indagine viene condotta tenendo come costante riferimento l'esigenza che la logica securitaria che caratterizza l'ampliamento dell'impiego delle tecnologie digitali non vada a discapito della tutela dei diritti fondamentali dei migranti che sono sottoposti ai controlli alle frontiere.