Diritto, Immigrazione e Cittadinanza
Fascicolo n. 1/2020

L'INTEROPERABILITÀ FRA LE BANCHE-DATI DELL'UNIONE SUI CITTADINI DEGLI STATI TERZI

di Giandonato Caggiano

Abstract: *L'articolo analizza la complessa struttura legale che regola la raccolta, il trattamento e l'accesso ai dati personali dei cittadini dei Paesi terzi nell'Unione europea, evidenziando la difficile delimitazione delle competenze sulla materia tra Unione europea e Stati membri. In particolare è messa fuoco la normativa relativa all'interoperabilità delle varie banche-dati, analizzando la sua evoluzione e le criticità ancora presenti.*

Abstract: *The article analyzes the complex legal structure that regulates the collection, processing and access to personal data of third-country nationals in the European Union, highlighting the difficult delimitation of competences on the matter between the EU and the Member States. It focuses in particular on the regulations on the interoperability of the various databases, analyzing their evolution and the critical points still present.*

ISSN 1972-4799

L'INTEROPERABILITÀ FRA LE BANCHE-DATI DELL'UNIONE SUI CITTADINI DEGLI STATI TERZI*

di Giandonato Caggiano**

SOMMARIO: 1. Introduzione e oggetto del contributo. – 2. I limiti all'ingerenza nel diritto alla tutela dei dati personali nella giurisprudenza della Corte di giustizia. – 3. Lo sviluppo della questione dell'interoperabilità delle banche-dati. – 4. Le modifiche delle banche-dati per l'allineamento all'interoperabilità. – 5. L'architettura dei sistemi dei dati personali tra migrazione e politiche di contrasto. – 6. I principi del regolamento (UE) 2018/1725 sui dati personali delle Agenzie dell'Unione. – 7. Il funzionamento e le componenti dell'interoperabilità. – 8. Le criticità dell'archivio comune di dati di identità (CIR). – 9. Conclusioni.

1. Introduzione e oggetto del contributo

Tra le misure che determinano un'alta probabilità di ingerenza nei diritti fondamentali vi sono le regole di raccolta, trattamento e accesso ai dati personali conservati dal soggetto responsabile di una banca-dati e/o della loro conservazione nel diritto.

I dati personali dei cittadini degli Stati terzi che, a vario titolo, entrano in contatto con l'ordinamento dell'Unione, sono ora integrati in un'unica architettura informativa. Oltre che dai regolamenti istituivi delle singole banche-dati, la struttura giuridica è costituita: in primo luogo, dall'attività gestionale di un'istituzione, l'Agenzia eu-LISA[1], cui è affidata la responsabilità dei sistemi esistenti e la progettazione di quelli non ancora operativi; in secondo luogo, dai regolamenti 2019/817 e 2019/818 sull'interoperabilità (d'ora in poi citati con il semplice numero)[2], che prevedono procedure complementari a quelle previste

* Il presente contributo è destinato agli Scritti offerti per Claudia Morviducci.

** Ordinario di diritto dell'Unione europea nell'Università di Roma Tre.

Nota redazionale: in questo contributo, i regolamenti sono citati con titolo abbreviato seguito dall'indicazione: (...).

1. Regolamento (UE) n. 2018/1726 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo all'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), v. *European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)*, EP, EPRS, December 2018.

2. 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 (...). Sull'*iter* legislativo, v. C. Dumbrava, *Interoperability of European information systems for border management and security*, EP, June 2017; K. Eisele, *Interoperability between EU information systems for security, border and migration management*, EP, EPRS, February 2018; K. Luyten, S. Voronova, *Interoperability between EU border and security information systems*, EU Legislation in Progress, EP, EPRS, June 2019 (Third edition).

dai sistemi informativi gestiti dall'Agenzia, nel rispetto della loro autonomia e compartimentazione. Difficile appare una giustificazione collegata soltanto alle scelte dell'integrazione differenziata nello Spazio di libertà, sicurezza e giustizia, che andrà attentamente riconsiderata dopo la Brexit. Al reticolo dei regolamenti istitutivi delle banche-dati, corrisponde ora una struttura informativa unificata dotata di procedure a carattere generale.

La materia rappresenta un campo di difficile delimitazione delle competenze tra Unione e Stati membri. Infatti, secondo il TFUE, le disposizioni del Titolo V non ostano all'esercizio delle responsabilità incombenti agli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna (art. 72). Non si tratta però di una vera e propria riserva di competenza agli Stati membri, quanto piuttosto di una sorta di flessibilità nell'attuazione di normative dell'Unione nell'ambito delle nozioni di ordine pubblico e sicurezza interna definite nella giurisprudenza della Corte di giustizia sulla circolazione delle persone.

Il limite delle competenze nazionali in materia di sicurezza a livello dell'Unione trova compensazione nella complessiva "civiltà giuridica dell'integrazione europea" costituita dai "cerchi concentrici" dell'Unione e della CEDU. Quest'ultima consente il controllo sovranazionale sull'ingerenza degli Stati contraenti nel godimento del diritto alla tutela del diritto ai dati personali, secondo il noto meccanismo del doppio margine di apprezzamento (art. 8 CEDU).

Questo contributo intende offrire una prima riflessione sulle questioni giuridiche costituite dai regolamenti 2019/817 e 2019/818. In questa sede non può essere svolta un'analisi puntuale delle modifiche apportate di recente alle singole banche-dati dell'Unione appartenenti allo Spazio di libertà, sicurezza e giustizia. Ci limiteremo ad indicarne le principali caratteristiche nell'ottica dell'interoperabilità.

2. I limiti all'ingerenza nel diritto alla tutela dei dati personali nella giurisprudenza della Corte di giustizia

Se, da un lato, le procedure di identificazione tramite accesso alle banche-dati possono avere un impatto sul diritto al rispetto della vita privata e, in particolare, sul diritto alla propria identità (art. 7 della Carta dei diritti fondamentali dell'Unione europea); dall'altro, le verifiche basate sui dati biometrici rappresentano un'ingerenza nel diritto alla dignità umana, in particolare, se percepite come umilianti dall'interessato e ottenute con il ricorso a costrizioni da parte delle forze di polizia.

Come sottolineato dalla giurisprudenza della Corte di giustizia, il diritto alla protezione dei dati personali non costituisce una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale[3]. Conformemente alla Carta, che vincola sia le istituzioni dell'Unione che gli Stati membri nell'attuazione del diritto dell'Unione (art. 51, par. 1), l'interoperabilità deve conciliarsi con l'obbligo di garantire che le ingerenze nei diritti fondamentali si limitino a quanto strettamente necessario per rispondere effettivamente alle finalità di interesse generale perseguite, nel rispetto del principio di proporzionalità (art. 52, par. 1). Secondo tale disposizione, possono essere apportate limitazioni all'esercizio del diritto alla protezione dei dati purché siano previste dalla legge, rispettino il contenuto essenziale dei diritti e delle libertà e, in ottemperanza al principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Nella sua giurisprudenza, la Corte di giustizia ha statuito i limiti ai poteri di sorveglianza degli Stati membri. Nella sentenza *Digital Rights Ireland* ha considerato incompatibile con il diritto dell'Unione la sorveglianza di massa, dichiarando l'invalidità della direttiva *data retention*[4]; nella sentenza *Tele2* ha affermato l'obbligatorietà dei principi anche a livello degli atti nazionali di attuazione della direttiva *e-privacy*[5]. Nel parere 1/15, relativo al trasferimento di dati PNR dall'UE al Canada, ha invece affermato che non si ha un sistema di sorveglianza generalizzata illecita se la misura in esame riguarda solo specifici viaggiatori[6]. *Mutatis mutandis*, se una banca-dati non può essere in sé qualificata come istituzione di sorveglianza generalizzata e indiscriminata allorché coinvolga solo una parte dei cittadini di Paesi terzi, una nuova architettura di banche-dati interoperabili, che combina informazioni provenienti dai diversi sistemi, può essere più facilmente considerata uno strumento di sorveglianza di massa dei loro movimenti.

Un secondo cambiamento introdotto dall'interoperabilità riguarda le procedure di accesso ai dati dei cittadini di Paesi terzi. Nelle sentenze citate, la Corte di giustizia ha chiarito che l'accesso dovrebbe essere soggetto a condizioni rigorose e previa verifica che tali condizioni siano state soddisfatte da un'autorità giudiziaria o amministrativa

3. Sulle questioni giuridiche generali e sulla relativa bibliografia, v. G. Caggiano, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno*, Atti del convegno Messina, 26 maggio 2017, Napoli, Editoriale scientifica, 2018, p. 13 ss. (anche in *Medialaws*, 2018, fasc. 2, p. 64 ss.); Id., *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi sull'integrazione europea*, 2018, p. 9 ss.

4. Sentenza della Corte (Grande Sezione) dell'8 aprile 2014, *Digital Rights Ireland Ltd*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238.

5. Sentenza della Corte (Grande Sezione) del 21 dicembre 2016, *Tele2 Sverige*, cause riunite C-203/15 e C-698/15, ECLI:EU:C:2016:970.

6. Parere 1/15 della Corte (Grande Sezione) del 26 luglio 2017, ECLI:EU:C:2017:592.

indipendente. Il grave rischio è che l'interoperabilità non solo conservi le modalità problematiche di accesso ai singoli sistemi di banca-dati ma porti progressivamente ad un accesso generale e di *routine*. La verifica dei dati personali in uno dei sistemi sottostanti all'architettura comune dovrebbe avvenire solo dopo aver soddisfatto le condizioni specifiche di accesso prescritte dalla base giuridica di ciascuna banca-dati.

3. Lo sviluppo della questione dell'interoperabilità delle banche-dati

Un aspetto specifico della questione è quello delle banche-dati di cui sono responsabili l'Unione e le sue agenzie specializzate nello Spazio di libertà, sicurezza e giustizia (Titolo V TFUE). A partire dal primo Sistema di Informazione Schengen (SIS II)[7], le banche-dati sono state costituite tramite regolamenti che ne disciplinano obiettivi, meccanismi di funzionamento, destinatari e utilizzatori. Negli ultimi anni, l'azione legislativa dell'Unione si è concentrata sulla ricerca di soluzioni per la loro gestione e utilizzazione frammentaria. In materia particolarmente complesso appare il bilanciamento tra il godimento dei diritti alla *privacy* e alla protezione dei dati e le esigenze di sicurezza pubblica. La riforma dell'Unione in materia (ancora in corso di attuazione) trova un "collante" proprio nella dimensione della sicurezza, che riguarda sia misure amministrative in materia di frontiere/visti/immigrazione/asilo, sia misure di contrasto a livello giudiziario e di polizia.

Il Consiglio europeo ha più volte rilanciato il dibattito sull'interoperabilità sotto l'impulso degli episodi più cruenti di terrorismo e le conseguenti richieste di rafforzamento della sicurezza interna e internazionale. A seguito dell'attacco alle Torri gemelle del 2001 e degli attentati di Madrid del 2004, il Consiglio europeo ha iniziato a promuovere i collegamenti tra le banche-dati allora esistenti. Gli attentati di Parigi del 2015 hanno portato alle Conclusioni del Consiglio europeo sulla necessità di garantire l'interoperabilità di tutti i sistemi esistenti o in via di progettazione[8].

Da allora, la Commissione europea ha seguito un programma di rafforzamento delle funzionalità dei sistemi informatici dell'Unione europea [9]. Tale programma ha

7. V. da ultimo 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, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006.

8. EUCO 28/15, 18 dicembre 2015, par. 5, lett. c).

9. COM (2016) 205 final, 6 aprile 2016, Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza. V. anche COM (2016) 602 final, 14 settembre 2016, rafforzare la sicurezza in un mondo di mobilità: un migliore scambio di informazioni nella lotta al terrorismo e frontiere esterne più solide. Per le informazioni sullo svolgimento dell'*iter* di riforma, v. COM (2017) 466 final, 16 maggio 2017, Settima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza; COM (2018) 470 final, 13 giugno 2018, Quindicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza; COM (2019) 145 final, 20 marzo 2019, Diciottesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza.

profondamente modificato, in un limitato arco di tempo, il quadro giuridico dell'Unione in materia di raccolta e utilizzo di dati dei cittadini degli Stati terzi. Al riguardo, il Parlamento europeo ha svolto un ruolo pienamente propositivo nei confronti dei singoli regolamenti delle banche-dati e, soprattutto, dei regolamenti sull'interoperabilità, per consentirne l'adozione prima della fine della VIII legislatura[10]. Particolarmente rilevanti per l'adozione dei testi legislativi sono risultate le osservazioni e le specifiche competenze del Garante europeo[11].

Durante l'*iter* legislativo per l'adozione dei due regolamenti 2019/817 e 2019/818 si è sostenuto, in vari contesti istituzionali, che le nuove procedure non intaccano la tutela dei diritti fondamentali prevista nella disciplina delle singole banche-dati. Secondo la Commissione, il testo integra tutte le norme sulla protezione dei dati stabilite nel regolamento generale sulla protezione dei dati. I periodi di conservazione dei dati (se pertinenti) sono appropriati e limitati. L'accesso ai dati è riservato esclusivamente al personale autorizzato delle autorità degli Stati membri o degli organismi dell'UE competenti per gli scopi specifici di ciascun sistema di informazione e limitato nella misura in cui i dati sono necessari per l'esecuzione di compiti conformemente a tali scopi[12]. I regolamenti 2019/817 e 2019/818 hanno un potenziale impatto su una serie di diritti fondamentali, quali il diritto al rispetto della vita privata e, in particolare, il diritto alla propria identità (art. 7 della Carta). D'altra parte, lo svolgimento di verifiche basate su dati biometrici può essere percepito come un'interferenza con il diritto alla dignità della persona. Al riguardo, siamo invece convinti che l'introduzione dell'interoperabilità abbia, per definizione, la capacità di stabilire diversi equilibri tra gli interessi in gioco, incidendo diversamente sui medesimi diritti fondamentali. Senza contare le difficoltà di controllo e di sorveglianza della maxi-infrastruttura, assai più ampia di quelle parziali coesistenti.

Nella politica legislativa dell'Unione si registra una vera commistione di procedure. Strumenti di controllo dell'immigrazione/asilo sono intrecciati con strumenti tipici del contrasto di polizia o della cooperazione giudiziaria. Inoltre, le banche-dati esistenti sono state oggetto di modifiche legislative, soprattutto per il rafforzamento dei dati anagrafici e

10. Risoluzione legislativa del Parlamento europeo del 16 aprile 2019 sulla proposta modificata di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (frontiere e visti) (...).

11. European Data Protection Supervisor (EDPS), Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 11 november 2017; Id, Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems.

12. Cfr. le osservazioni critiche in Sintesi del parere del Garante europeo della protezione dei dati sulle proposte di due regolamenti che istituiscono un quadro per l'interoperabilità tra i sistemi di informazione su larga scala dell'UE (doc. 2018/C 233/07), paragrafi 146-149.

biologici delle persone interessate, proprio per consentire la funzione di interoperabilità. In tal senso, sono state concepite le nuove banche-dati costituite o in via di costituzione.

4. Le modifiche delle banche-dati per l'allineamento all'interoperabilità

In questa intensa opera di riforma legislativa, sono state recentemente modificate le seguenti banche-dati, per allineare il loro funzionamento con l'interoperabilità.

Il Sistema di Informazione Schengen (SIS), primo sistema automatizzato per la gestione e lo scambio di informazioni fra i Paesi aderenti alla Convenzione di Schengen (1995), è stato recentemente riformato da tre regolamenti[13]. Il sistema prevede un ampio spettro di segnalazioni relative alle persone (rifiuto di ingresso o di soggiorno, mandato d'arresto europeo, persone scomparse, assistenza nel quadro di un procedimento giudiziario, controllo discreto e controllo specifico) e agli oggetti (inclusi i documenti di identità o di viaggio smarriti, rubati o invalidati). In particolare, il nuovo regolamento (UE) n. 2018/1861 (regolamento «SIS frontiere») precisa le categorie di dati da immettere per segnalare un divieto di entrata. Il regolamento stabilisce le condizioni e le procedure per inserire e trattare le segnalazioni riguardanti cittadini di Paesi terzi nonché per scambiare informazioni supplementari e dati complementari ai fini del respingimento e del rifiuto del soggiorno nel territorio degli Stati membri («Segnalazioni ai fini del respingimento»). Il regolamento prevede consultazioni tramite fotografie, immagini del volto e dati dattiloscopici (impronte digitali e palmari). Per quanto riguarda l'accesso alle segnalazioni, le autorità nazionali hanno diritto di consultare nel SIS i dati relativi alle segnalazioni. Il regolamento (UE) n. 2018/1860 (regolamento «SIS rimpatri») introduce una nuova categoria di segnalazioni nei confronti di cittadini di un Paese terzo in soggiorno irregolare verso cui è stata presa una decisione di rimpatrio ai sensi della direttiva 2008/115/CE[14] per consentire di verificare se costoro abbiano effettivamente lasciato il territorio degli Stati membri.

13. 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 (...); 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. Per un commento, v. N. Atanassov. *Revision of the Schengen Information System for law enforcement*, EP, EPRS, October 2018. Id, *Revision of the Schengen Information System for border checks*, EP, EPRS, October 2018. Id, *Use of the Schengen Information System for the return of illegally staying third-country nationals*, EPRS, EP, October 2018.

14. Direttiva 2008/115/CE del Parlamento europeo e del Consiglio, del 16 dicembre 2008, recante norme e procedure comuni applicabili negli Stati membri al rimpatrio di cittadini di Paesi terzi il cui soggiorno è irregolare.

Il sistema di informazione visti (VIS) contiene attualmente dati sui visti per soggiorni di breve durata[15]. La proposta di riforma della Commissione[16] prevede la centralizzazione dei dati relativi a tutti i titolari di visti per soggiorno di lunga durata e di permessi di soggiorno e il controllo incrociato delle domande di visto con altri sistemi di informazione dell'UE. I dati relativi ai titolari di visti per soggiorno di lunga durata e permessi di soggiorno riguardano l'unica categoria di cittadini di Paesi terzi che attualmente non rientra in nessuno dei sistemi.

Il sistema Eurodac[17] contiene dati relativi alle impronte digitali di richiedenti asilo e cittadini di Paesi terzi che hanno attraversato irregolarmente le frontiere esterne o il cui soggiorno in uno Stato membro è irregolare.

Oltre alla modifica dei suddetti sistemi, l'architettura delle banche-dati è completata da tre nuovi meccanismi: 1) il sistema di ingressi/uscite (EES)[18], che sostituisce il sistema di timbratura manuale dei passaporti, registrando elettronicamente il nome, il tipo di documento di viaggio, i dati biometrici, nonché la data e il luogo di ingresso e di uscita dei cittadini di Paesi terzi che entrano nello spazio Schengen; 2) il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), in grado di raccogliere e verificare le informazioni fornite dai cittadini di Paesi terzi *esenti dal visto* prima di un loro viaggio nello spazio Schengen[19]; 3) il sistema europeo di informazione sui casellari giudiziali

15. Un quarto strumento informativo è costituito dalla rete DubliNet, canale di trasmissione elettronica tra le autorità degli Stati membri, istituito in applicazione del regolamento (CE) n. 1560/2003 (art. 18), ai fini del regolamento (UE) n. 604/2013 del Parlamento europeo e del Consiglio (Dublino III) agli articoli 31, 32 e 34.

16. COM (2018) 302 final, 16 maggio 2018, proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (CE) n. 767/2008 («regolamento VIS») (...). La proposta va ad integrare e modificare il codice dei visti ancora in discussione, COM (2018) 252 final, recante modifica del regolamento (CE) n. 810/2009 che istituisce un codice comunitario dei visti (codice dei visti).

17. 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 (...). Per la modifica, la cui approvazione è legata a quella degli altri atti del pacchetto-asilo, v. COM/2016/0272 final, 4 maggio 2016, Proposta 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 (...). L'attuale architettura non permette tecnicamente l'interoperabilità con gli altri sistemi di informazione, poiché ogni voce contiene soltanto i dati biometrici e un numero di riferimento, ma non altri dati personali (ad es., nome, età, data di nascita). La proposta legislativa del 2016 prevede invece la memorizzazione di dati personali quali nome, età, data di nascita, cittadinanza ed estremi dei documenti d'identità. Per un primo commento, v. A. Orav, *Recast Eurodac Regulation*, EU Legislation in Progress Briefing, EP, EPRS, March 2017.

18. 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 (...). Per un'analisi approfondita, v. A. Orav, A. D'Alfonso, *Smart Borders: EU Entry/Exit System*, EP, EPRS, January 2018.

19. Regolamento (UE) n. 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018. Il sistema destinato ai cittadini dei circa sessanta Stati che sono attualmente esenti da visto sarà attivato nel 2021. Per un

riguardo ai cittadini di Paesi terzi (sistema ECRIS-TCN)[20] sullo scambio di informazioni delle condanne pronunciate da organi giurisdizionali penali all'interno dell'Unione a carico di tali cittadini.

Questi sei sistemi, tra loro complementari, riguardano esclusivamente i cittadini di Paesi terzi, ad eccezione del Sistema d'Informazione Schengen (SIS), che può riguardare anche i cittadini dell'Unione.

5. L'architettura dei sistemi dei dati personali tra migrazione e politiche di contrasto

Dal Trattato di Lisbona, le banche-dati trovano una cornice comune nelle disposizioni preliminari del Titolo V del TFUE nell'ambito dello Spazio di libertà, sicurezza e giustizia. Dalla base giuridica unica dell'art. 16 TFUE[21] derivano diversi atti di diritto secondario: il regolamento generale, la direttiva sui dati di polizia e il regolamento sui dati delle Agenzie dell'Unione[22].

Come abbiamo detto, la base giuridica della legislazione europea è costituita dall'art. 16, par. 1, TFUE sia per quanto riguarda la protezione dei dati a livello generale che nel settore di polizia, ma è previsto che possa esservi un raddoppio degli strumenti in relazione alla suddetta distinzione. Si realizza anzi persino la necessità di una specializzazione degli strumenti giuridici, com'è accaduto per il sistema SIS che, come già accennato e meglio vedremo, si è articolato recentemente in tre distinti regolamenti: frontiere, polizia e rimpatrio. Infatti, pur a seguito del superamento della divisione fra regime ordinario e regime speciale *ex* terzo pilastro, la Dichiarazione n. 21 della Conferenza di Lisbona relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia riconosce che specializzazioni potrebbero rivelarsi necessarie in considerazione della specificità dei settori in questione.

---

commento, v. A. Radjenovic, *European Travel Information and Authorisation System (ETIAS)*, EPRS, EP, October 2018.

20. 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) (...). Per un'analisi, H. Dalli, *Exchange of Information on Third Country Nationals – European Criminal Records Information System (ECRIS)*, EP, EPRS, March 2016.

21. Una diversa base giuridica è prevista per la tutela dei dati nell'ambito della politica estera e di sicurezza comune (art. 39 TUE).

22. 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 (...); direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati (...); regolamento (UE) n. 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati (...).

Al riguardo merita di essere evidenziata la progressiva assimilazione delle questioni delle banche-dati dell'immigrazione/asilo a quelle della cooperazione giudiziaria/di polizia. I due regolamenti 2019/817[23] e 2019/818[24] del 20 maggio 2019 sono del tutto speculari nella parte della creazione del meccanismo e del funzionamento dell'interoperabilità (capitoli da I a VIII) mentre si occupano distintamente di allineare al meccanismo dell'interoperabilità le banche-dati preesistenti, rispettivamente nei settori di frontiere/visti e di asilo/migrazione/cooperazione di polizia/giudiziaria.

In particolare, la suddivisione *ratione materiae* dei due regolamenti 2019/817 e 2019/818 non corrisponde all'articolazione del Titolo V TFUE. In pratica, il regime dell'interoperabilità separa frontiere e visti dall'immigrazione, che è invece collegata alla cooperazione giudiziaria e di polizia. Non è una divisione di particolare rilievo giuridico perché la parte principale dei due regolamenti è identica, ma la scelta ha un valore non solo semantico ma è anche espressione di una visione politica dell'Unione.

Se, in un contesto del genere, non è certo facile distinguere le misure di carattere propriamente penale da quelle a carattere amministrativo, è però rilevante l'esistenza di diverse basi giuridiche. Anche il regolamento relativo al trattamento dei dati personali da parte degli organi o degli organismi dell'Unione[25] fa salve le norme specifiche (*lex specialis*) del Titolo V applicabili al capo 4 (polizia) e capo 5 (cooperazione giudiziaria), TFUE[26].

Pertanto, immigrazione e applicazione coercitiva della legge costituiscono due settori diversi di ordine pubblico che perseguono specifici obiettivi e finalità di raccolta e, come tali, dovrebbero restare chiaramente distinti in forza dei principi e delle regole dell'Unione sulla tutela dei dati personali. Qualora vi fossero dubbi, si tratta della dimostrazione della tendenza ad associare la gestione della migrazione alla cooperazione giudiziaria e di polizia.

---

23. La base giuridica del regolamento (UE) n. 2019/817 è costituita dall'art. 77, par. 2 TFUE: a) politica comune dei visti e di altri titoli di soggiorno di breve durata; b) controlli ai quali sono sottoposte le persone che attraversano le frontiere esterne; d) istituzione progressiva di un sistema integrato di gestione delle frontiere esterne; e) assenza di controlli sulle persone, a prescindere dalla nazionalità, all'atto dell'attraversamento delle frontiere interne. Risoluzione legislativa del Parlamento europeo del 16 aprile 2019 sulla proposta modificata di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (frontiere e visti) (...).

24. Le basi giuridiche del regolamento (UE) n. 2019/818 riguardano l'asilo (art. 78, par. 2, lett. e)), l'immigrazione clandestina (art. 79, par. 2, lett. c)), la cooperazione giudiziaria (art. 82, par. 1, lett. d)), Eurojust (art. 85, par.), la cooperazione di polizia (art. 87, par. 2, lett. a)) e Europol (art. 88, par 2).

25. Art. 3, regolamento (UE) n. 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati.

26. Considerando 11e 15.

6. I principi del regolamento (UE) 2018/1725 sui dati personali delle Agenzie dell'Unione

Al trattamento dei dati personali da parte dell'Agenzia eu-Lisa si applicano le norme del nuovo regolamento (UE) 2018/1725[27] che stabilisce le norme relative alla protezione in relazione al trattamento dei dati personali da parte delle istituzioni e degli organi dell'Unione. Tale regolamento riguarda un importante aspetto della riforma della protezione dei dati personali, poiché contiene le necessarie specificazioni e integrazioni per l'attività delle istituzioni e agenzie europee rispetto alle disposizioni del regolamento generale sulla protezione dei dati e alla direttiva sui dati di polizia[28].

Secondo il regolamento generale sulla protezione dei dati, la libera circolazione dei dati all'interno dell'UE non deve essere limitata per motivi legati alla protezione dei dati. Soprattutto, in relazione alla questione dell'interoperabilità dei sistemi su larga scala, è necessaria un'attenzione particolare agli obblighi di protezione, secondo il regolamento generale sulla protezione dei dati (art. 25) e la direttiva sulla protezione dei dati nei settori della polizia e della giustizia (art. 20). Il principio da rispettare riguarda la protezione dei dati «fin dalla progettazione» e protezione «per impostazione predefinita», vale a dire una concezione della raccolta dei dati che tenga conto *ex-ante* degli accorgimenti tecnici necessari a minimizzare i rischi di violazioni.

Il principio di compatibilità tra le basi giuridiche dei regolamenti delle singole banche-dati e di quelle dei regolamenti dell'interoperabilità appare particolarmente flessibile e lascia un vasto ambito di discrezionalità all'Unione e alle sue agenzie. Non è richiesta alcuna base giuridica separata se il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti è compatibile con le finalità di un nuovo e diverso trattamento. Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il diritto dell'Unione può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile. Altrettanto vago appare il criterio della compatibilità nel regolamento (UE) 2018/1725[29].

La limitazione delle finalità di raccolta è un principio fondamentale della tutela dei dati personali. A causa dei diversi contesti delle banche-dati dell'Unione, il principio della

27. Regolamento (UE) 2018/1725, cit.

28. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (...); direttiva 2016/680 del Parlamento europeo e del Consiglio d'Europa, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (...).

29. «Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe tener conto, tra l'altro, di ogni nesso delle finalità dell'ulteriore trattamento previsto con il contesto in cui i dati personali sono stati raccolti».

limitazione delle finalità è stato attuato attraverso la «compartimentazione gestionale». Sino ad oggi, questo era il principale motivo della frammentazione della gestione dei dati.

La nuova impostazione dell'interoperabilità è basata sull'integrazione dei sistemi, che conservano però un certo livello di compartimentazione all'interno di un sistema unico e specifiche regole di accesso e utilizzo per ciascuna categoria di dati e di utenti. La «protezione dei dati fin dalla progettazione» e la «protezione dei dati per impostazione predefinita (di *default*)» informano le norme dell'Unione sulla protezione dei dati[30]. Ciò significa integrare la protezione dei dati personali nella base tecnologica dello strumento proposto, limitando il trattamento dei dati a quanto necessario per un determinato scopo e concedendo l'accesso ai dati soltanto ai soggetti che hanno la «necessità di conoscere».

In realtà, l'interoperabilità nega la rilevanza del principio di limitazione delle finalità di raccolta, consentendo di utilizzare variamente le banche-dati. Quanto al principio dell'incompatibilità con lo scopo originale per il quale i dati sono stati originariamente raccolti, le riconfigurazioni dei sistemi nel tempo indicano che la soglia per tale «incompatibilità» è irraggiungibile e che i limiti di questi sistemi sono lungi dall'essere raggiunti.

7. Il funzionamento e le componenti dell'interoperabilità

I regolamenti dell'interoperabilità istituiscono quattro meccanismi che determinano le funzione dell'interoperabilità: un portale di ricerca europeo (ESP), che consente alle autorità competenti di effettuare ricerche simultanee in vari sistemi d'informazione su dati anagrafici e biometrici; un servizio comune di confronto biometrico, che consente la ricerca e il confronto di dati biometrici (impronte digitali e immagini del volto) provenienti da vari sistemi (BMS comune); un archivio comune di dati di identità, che contiene i dati d'identità anagrafici e biometrici di cittadini di Paesi terzi disponibili in vari sistemi d'informazione dell'Unione (CIR); un rilevatore di identità multiple, che controlla se i dati d'identità risultanti dalla ricerca sono presenti in altri sistemi (MID).

Il portale di ricerca europeo segnalerà tramite interrogazione individuale se esistono dati o collegamenti ma il sistema mostrerà a ogni autorità soltanto i dati a cui può già accedere ai sensi della legislazione che istituisce le varie banche-dati. Almeno due dei meccanismi (BMS e CIR) creano invece sistemi che, sommando dati presenti in varie banche-dati, possono essere considerati in realtà una nuova banca-dati. Pertanto, si pone la difficile questione del bilanciamento fra i rischi per la sicurezza e i diritti delle persone in relazione alle caratteristiche originarie di una banca-dati e all'utilizzo e accesso per altre

30. Articolo 25; Considerando 78 del Regolamento generale sulla protezione dei dati, cit.

finalità dei dati medesimi. In questo caso è difficile sostenere che le condizioni dell'accesso ai dati e le finalità di raccolta restino invariati rispetto agli strumenti originari delle singole banche-dati, perché ciò che non era possibile ottenere prima dalle singole banche-dati può mettere in luce la storia e le caratteristiche di una persona.

In definitiva, i regolamenti sull'interoperabilità aumentano potenzialmente il rischio di discriminazione dei cittadini di Paesi terzi sulla base della razza o dell'origine etnica, violando il diritto alla non discriminazione. I controlli di identità sul territorio degli Stati membri ai fini di indagini di polizia hanno un potenziale di incidere negativamente sui diritti fondamentali della Carta. Su suggerimento del Garante europeo, sono state precisate le condizioni di interrogazione tramite il confronto del materiale biologico che deve essere svolto in presenza dell'interessato[31].

Bisogna tenere presente che tali sistemi sono stati istituiti e sviluppati in vista dell'applicazione di politiche specifiche e non come strumento di contrasto. L'accesso di *routine* rappresenterebbe una violazione del principio di limitazione delle finalità. Ciò comporterebbe un'intrusione sproporzionata nella *privacy*, ad esempio, dei viaggiatori che hanno accettato il trattamento dei loro dati al fine di ottenere un visto e si aspettano che i loro dati vengano raccolti, consultati e trasmessi a tale scopo. Inoltre, l'eliminazione delle garanzie introdotte per preservare i diritti fondamentali, principalmente per accelerare una procedura, non sarebbe accettabile. Se è necessario migliorare la procedura, ciò non dovrebbe essere fatto a scapito delle garanzie.

In realtà, l'interoperabilità nega la rilevanza del principio di limitazione degli scopi, consentendo essenzialmente di utilizzare le basi di dati per quasi tutti gli scopi, purché ciò non sia incompatibile con lo scopo originale per il quale i dati sono stati originariamente raccolti.

8. Le criticità dell'archivio comune di dati di identità (CIR)

L'archivio comune di dati di identità (CIR) sarà la componente comune in cui verranno "duplicati" i dati anagrafici e biometrici dei cittadini di Paesi terzi registrati (Eurodac, VIS, EES, ETIAS, ECRIS-TCN). I dati di identità saranno conservati nel CIR, ma continueranno ad "appartenere" alle banche-dati in cui sono stati registrati. Il CIR non duplicherà invece i dati SIS II la cui complessa struttura contiene copie nazionali, copie

31. Le interrogazioni del CIR sono effettuate da un'autorità di polizia nei seguenti casi: a) in assenza di un documento di viaggio o di un altro documento credibile; b) se sussistono dubbi quanto ai dati di identità forniti da una persona; c) se sussistono dubbi quanto all'autenticità del documento di viaggio o di un altro documento credibile fornito da una persona; d) se sussistono dubbi quanto all'identità del titolare del documento di viaggio o di un altro documento credibile; ovvero e) se l'interessato non è in grado o rifiuta di cooperare.

nazionali parziali ed eventuali sistemi nazionali di confronto biometrico. Una duplicazione dei dati SIS renderebbe il CIR talmente complesso da renderlo né tecnicamente, né finanziariamente, realizzabile.

La consultazione del neocostituito Centro CIR è divisa in due fasi: la prima consiste in una interrogazione sull'esistenza di dati relativi alla persona coinvolta nelle varie banche-dati (c.d. ricerca *hit/non hit*). La seconda riguarda l'accesso diretto alle informazioni alle quali l'autorità sia abilitata ad accedere secondo le regole di una specifica banca-dati.

Un aspetto particolarmente delicato della riforma è costituito dalla norma in base alla quale un'autorità di polizia è autorizzata a interrogare il CIR con i dati biometrici di una persona prelevati durante un controllo di identità al solo scopo di identificare quella persona. La proposta originaria della Commissione prevedeva che l'identificazione della persona fosse determinata per prevenire e combattere la migrazione irregolare o contribuire a un livello elevato di sicurezza. Come il Garante europeo della protezione dei dati (GEPD) ha giustamente sottolineato, questi obiettivi erano vaghi e non spiegavano se i controlli di polizia dovessero avvenire nell'ambito del controllo sull'immigrazione o delle procedure di contrasto. Ai fini dell'identificazione di una persona fermata, le autorità di polizia possono interrogare il CIR con i dati biometrici dell'interessato acquisiti sul posto durante una verifica d'identità, a condizione di avviare la procedura in presenza dell'interessato. Per consentire tale facoltà alle autorità nazionali, gli Stati membri adotteranno misure legislative in cui specificano le finalità dell'identificazione, designano le autorità di polizia competenti e stabiliscono le procedure, le condizioni e i criteri di tali verifiche, «evitando qualsiasi discriminazione nei confronti di cittadini di Paesi terzi».

L'accesso è finalizzato all'identificazione di una persona fermata di cui si vuole sapere "rapidamente tutto" senza sottostare alle difficoltà di collaborazione con i Paesi di origine/cittadinanza e, in alternativa, a tempi e costi delle operazioni di *intelligence*. I controlli di identità da parte delle autorità di polizia possono alimentare pratiche discriminatorie per i controlli di identificazione sui cittadini di Paesi terzi *in loco*, ove siano svolti sulla base di una profilazione che renderebbe precario il loro *status*.

Il rinvio all'adozione di norme nazionali di specificazione delle condizioni di accesso non esclude il controllo della Corte di giustizia, ma lo rende complesso, dovendosi esercitare sulle leggi nazionali di attuazione. È facile prevedere che, come accade nei confronti delle leggi nazionali sulla *data retention*, prevalga la tendenza dei giudici nazionali a rivolgersi prioritariamente alle Corti costituzionali anziché alla Corte di giustizia in materie che siano al contempo di diritto dell'Unione e diritto costituzionale (doppia pregiudizialità).

9. Conclusioni

L'ambito di applicazione soggettiva delle banche-dati riguarda i cittadini di Paesi terzi ma si espande progressivamente anche alla mobilità transnazionale dei cittadini dell'Unione. Per quanto riguarda i cittadini dell'Unione il profilo relativo ai controlli sulle banche-dati è stato introdotto nella modifica del Codice frontiere che impone l'obbligo per gli Stati membri di effettuare verifiche sistematiche sui beneficiari del diritto alla libera circolazione quando attraversano la frontiera esterna, consultando le banche-dati sui documenti smarriti o rubati (il Sistema d'Informazione Schengen, la banca dati Interpol sui documenti smarriti o rubati, le banche-dati nazionali contenenti informazioni sui documenti di viaggio rubati, smarriti o invalidati)[32]. Esiste però la possibilità per gli Stati membri di eseguire verifiche mirate nelle banche-dati, in base ad una valutazione dei rischi connessi con la sicurezza interna, l'ordine pubblico o le relazioni internazionali degli Stati membri o con una minaccia per la salute pubblica. A verifiche approfondite sono invece sottoposti i cittadini di Paesi terzi all'ingresso e all'uscita, anche tramite la consultazione delle banche-dati.

Nello stesso senso la direttiva sui dati del codice di prenotazione (PNR), in base alla quale le compagnie aeree dovranno fornire i dati personali per i voli in arrivo o in partenza dall'UE. La direttiva stabilisce anche la facoltà per gli Stati membri di raccogliere i dati PNR anche in relazione a specifici voli *intra*-UE.

La trasformazione del sistema informativo dell'Unione costituisce certamente il primo passo per la creazione di un sistema centralizzato per tutti i dati personali dei cittadini degli Stati terzi. Inoltre, il sistema di informazioni potrà sempre più riguardare anche i cittadini dell'Unione per i quali con la riforma del Codice frontiere e la direttiva sul PNR[33] (entrambe motivate dal fenomeno dei combattenti stranieri e dai sospetti terroristi), sono previsti controlli sistematici tramite le banche-dati pertinenti.

In conclusione, vale la pena di citare la criticità del quadro giuridico che emerge dall'interoperabilità, che è stata oggetto di vari pareri del Garante europeo sulla protezione dei dati personali. L'interoperabilità non rappresenta esclusivamente o prevalentemente il risultato di una scelta tecnica, ma piuttosto quello di una scelta politica,

32. Regolamento (UE) n. 2016/399 del Parlamento europeo e del Consiglio del 9 marzo 2016 che istituisce un codice unionale relativo al regime di attraversamento delle frontiere da parte delle persone (codice frontiere Schengen), v. art. 8 «Consultazione nelle pertinenti banche dati delle informazioni relative esclusivamente ai documenti rubati, altrimenti sottratti, smarriti o invalidati».

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

che può comportare profonde conseguenze giuridiche e sociali, non sottovalutabili come se si trattasse di semplici modifiche tecniche.

Secondo il Garante, la decisione del legislatore dell'UE di realizzare sistemi di informazione su larga scala interoperabili non ha soltanto conseguenze permanenti e profonde sulla loro struttura e sul loro modo di funzionamento, bensì cambia il modo in cui i principi giuridici in questo ambito sono stati tradizionalmente interpretati e segna pertanto un "punto di non ritorno".

In relazione a tale contributo di competenza e consapevolezza dei rischi per la tutela dei dati personali, ci sentiamo in debito con Giovanni Buttarelli, Garante europeo per molti anni, recentemente scomparso.