

Banche dati delle forze di polizia, dati biometrici e diritti dei cittadini in Europa

Police databases, biometric data and citizens' rights in Europe

REBECCA DIZDARI 
Praticante Avvocato

CHIARA PARIS
Ph.D., Avvocato

RENATO BIONDO
Direttore del Servizio per i Sistemi Informativi della Direzione
Centrale della Polizia Criminale
Ministero dell'Interno, Dipartimento della Pubblica Sicurezza

[FRANCESCO SAVERIO ROMOLO](#) 
Professore Associato di Medicina Legale e del Lavoro
Università degli Studi di Bergamo

Abstract

Le banche dati delle forze di polizia europee e la raccolta di dati biometrici pongono sfide cruciali alla tutela dei diritti dei cittadini nel contesto dello spazio di libertà, sicurezza e giustizia. Il contributo analizza il quadro normativo europeo che regola la circolazione e lo scambio di dati biometrici (DNA, impronte digitali, immagini facciali) tra Stati membri, soffermandosi su procedure di acquisizione, interoperabilità e bilanciamento tra esigenze di sicurezza e protezione dei dati personali, con particolare riguardo al Trattato di Prüm e ai sistemi informativi come SIS II, ECRIS e EURODAC. Si evidenziano criticità operative e giuridiche, prospettando evoluzioni normative che mirano alla massima tutela dei diritti fondamentali.



Abstract

Police databases and the collection of biometric data in Europe pose crucial challenges to the protection of citizens' rights within the area of freedom, security, and justice. This contribution examines the European regulatory framework governing the circulation and exchange of biometric data (DNA, fingerprints, facial images) among Member States, focusing on acquisition procedures, interoperability, and the balance between security needs and data protection, with specific reference to the Prüm Treaty and key systems such as SIS II, ECRIS, and EURODAC. Operational and legal criticalities are highlighted, and regulatory developments aiming for the highest protection of fundamental rights are discussed.

Keywords: Banche dati; dati biometrici; Trattato di Prüm

Summary: [1. Lo spazio di libertà, sicurezza e giustizia europeo.](#) – [2. Le banche dati e i sistemi informativi.](#) – [3. Il quadro normativo europeo che regola gli scambi di dati biometrici e disciplina la riservatezza degli stessi.](#) – [3.1. La Decisione quadro 2006/960/GAI \(cd. Swedish Framework\) e la Direttiva 2023/977.](#) – [3.2. Il Trattato di Prüm e le successive Decisioni.](#) – [3.3. Dagli studi sulle Decisioni di Prüm al Prüm II.](#) – [3.4. L'architettura informatica e le soluzioni interoperabili per lo scambio di dati biometrici.](#) – [4. Discussione e conclusioni.](#)

1. Lo spazio di libertà, sicurezza e giustizia europeo.

Secondo l'art. 3, par. 2, del trattato sull'Unione europea (TUE) l'Unione "offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia"¹.

La cooperazione giudiziaria dell'Unione Europea (UE) è un ambito dove l'attuazione dei principi costituzionali dell'UE ha una particolare rilevanza, a causa del possibile impatto sulla sfera giuridica dei singoli. Per questo motivo il Trattato sul funzionamento dell'Unione prevede che tale spazio di libertà, sicurezza e giustizia deve essere realizzato attraverso misure di coordinamento e cooperazione tra forze di polizia e autorità giudiziarie e altre autorità competenti "nel rispetto dei diritti fondamentali nonché dei diversi ordinamenti giuridici e delle diverse tradizioni giuridiche degli Stati membri"².

Con il termine coordinamento si fa specifico riferimento alla messa in contatto tra magistrati, autorità di contrasto e altri soggetti di almeno due Paesi membri, al fine di combattere le gravi forme di criminalità transfrontaliera, ad opera di diversi organismi europei, quali ad esempio Eurojust (l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale)³. A tale Agenzia compete la c.d. cooperazione giudiziaria, che si

¹ Trattato sull'Unione europea, versione consolidata, art. 3, par. 2, consultabile al seguente link: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0017.02/DOC_1&format=PDF. Ultima consultazione 4 ottobre 2025.

² Trattato sul funzionamento dell'Unione europea, versione consolidata, art. 67, par. 1, consultabile al seguente link: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:12012E/TXT>. Ultima consultazione 4 ottobre 2025.

³ "I rapporti di Eurojust con le altre strutture che si occupano di cooperazione giudiziaria penale, quali Europol, OLAF e EPPO sono regolati dagli articoli che vanno dal 48 al 51, nonché dall'art. 75 del Regolamento UE 2018/1727", Di CANDIA, *Cooperazione giudiziaria europea e criminalità digitale: la relazione annuale 2021 del desk italiano di Eurojust*, in *Cassazione penale*, 2022, 5, 1971, nota n. 5.

estrinseca in una pluralità di azioni, tra cui lo scambio di informazioni e il coordinamento delle indagini, oltre ad aspetti specifici dell'ambito giudiziario quali le estradizioni, il riconoscimento reciproco delle decisioni, l'assistenza giudiziaria reciproca.

Eurojust offre altresì sostegno nella risoluzione di conflitti di giurisdizione e supporto nella definizione e attuazione di strumenti giuridici dell'UE, come il mandato d'arresto europeo (c.d. MAE)⁴, l'ordine europeo di indagine e i provvedimenti/certificati di confisca e congelamento. A tale fine l'Agenzia organizza riunioni di coordinamento, contribuisce alla costituzione e al finanziamento delle squadre investigative comuni (SIC)⁵, gestisce centri di coordinamento e ospita procuratori di collegamento di paesi terzi al fine di creare una rete globale di punti di contatto.

Tra i protagonisti della cooperazione giudiziaria penale in Europa vi sono, inoltre, la Procura europea (EPPO), competente per il rinvio a giudizio di reati che ledono gli interessi finanziari dell'UE⁶, l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), che ha la missione di sostenere gli Stati membri nella prevenzione e nella lotta contro tutte le forme gravi di criminalità organizzata e internazionale, criminalità informatica e terrorismo⁷, e l'Ufficio europeo per la lotta antifrode (OLAF)⁸.

I diversi attori nell'ambito della cooperazione giudiziaria si avvalgono di un nutrito compendio di strumenti giuridici, tra cui il Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio⁹, il quale ha apportato importanti novità in tema di prove elettroniche¹⁰.

⁴ Esso "rappresenta un sistema di cooperazione tra autorità giudiziarie particolarmente adatto alle esigenze di speditezza della giustizia penale", S. C. CONIGLIARO, S. LO FORTE, *Cooperazione giudiziaria in materia penale e tutela dei diritti fondamentali nell'Unione europea*, in *Diritto Penale Contemporaneo*, 3 giugno 2013, p. 2.

⁵ In particolare, le squadre investigative comuni sono "formate con una composizione eterogenea - forze di polizia e magistrati del pubblico ministero -, dai soggetti preposti alle indagini secondo le regole dei rispettivi ordinamenti nazionali", così in C. BARROCU, *Le speciali tecniche di investigazione nel contesto europeo*, in *Cassazione Penale*, 2020, fasc. 3, p. 1325.

⁶ L'EPPO è competente per i reati elencati nella Direttiva (UE) 2017/1371, così come recepita dal diritto nazionale.

⁷ L'Agenzia è entrata in funzione nel 1998 con la Convenzione Europol del 1995 ed è stata riformata da ultimo con il Regolamento n. 2016/794. Essa, con sede a L'Aia, assiste le autorità degli Stati membri coinvolte nel contrasto al crimine fornendo una piattaforma per lo scambio e l'analisi di informazioni su una serie di attività criminali gravi e a carattere transnazionale (che interessano quindi due o più Stati membri). Europol, che vede la propria base giuridica nell'art. 88 TFUE, funge dunque da centro di sostegno per le operazioni di contrasto, centro di informazioni sulle attività criminali e centro di competenze in tema di applicazione della legge.

⁸ Istituito con la Decisione 1999/352/CE, CECA, Euratom, del 28 aprile 1999.

⁹ Il testo del "Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio del 12 luglio 2023 relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali" consultabile al seguente link: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32023R1543>. Ultima consultazione il 4 ottobre 2025.

¹⁰ In sostanza, il testo normativo prevede la possibilità che l'autorità di uno Stato membro possa, nell'ambito di un procedimento penale, emettere un ordine europeo di produzione (OPE) o un ordine europeo di conservazione (OCE) e ingiungere pertanto a un prestatore di servizi che offre servizi nell'Unione e che è stabilito in un altro Stato membro o, alternativamente, rappresentato da un rappresentante legale in un altro Stato membro, di produrre o conservare prove elettroniche, indipendentemente dall'ubicazione dei dati, nel rispetto dei diritti fondamentali dell'uomo.

In tale contesto, si inserisce altresì il Regolamento (UE) 2022/850¹¹, volto a rafforzare la cooperazione digitale tra i vari sistemi giudiziari, tramite lo sviluppo di canali adeguati che consentano lo scambio elettronico transfrontaliero¹² di dati in modo rapido, diretto, interoperabile, sostenibile, affidabile e sicuro¹³. Il principale strumento istituito e disciplinato dal Regolamento 2022/850 è il c.d. sistema di comunicazione e-CODEX (e-Justice Communication via Online Data Exchange system)¹⁴, la cui gestione è affidata all'agenzia eu-LISA.

Parallelamente, la cooperazione di polizia tra le autorità di contrasto è rivolta alla prevenzione, individuazione e indagine di reati in tutta l'UE¹⁵. Nella pratica, questo tipo di cooperazione fa capo ad Europol, coinvolge i servizi di polizia, le dogane e altri servizi incaricati dell'applicazione della legge, ed è mirata a individuare reati gravi (criminalità organizzata, traffico di stupefacenti, riciclaggio di denaro, contraffazione, tratta di esseri umani, criminalità informatica, terrorismo)¹⁶.

Tra gli altri attori e organismi che partecipano alla cooperazione di polizia all'interno dello spazio europeo vi sono CEPOL¹⁷, COSI¹⁸ e, infine, EU INT-CEN¹⁹.

Sin dal 1995, le autorità di contrasto dell'Unione Europea si servono del Sistema di Informazione Schengen (SIS). Esso rappresenta la banca dati a sostegno del controllo delle frontiere esterne e della cooperazione nell'attività

¹¹ Regolamento (UE) 2022/850 del Parlamento europeo e del Consiglio del 30 maggio 2022, relativo a un sistema informatizzato per lo scambio elettronico transfrontaliero di dati nel settore della cooperazione giudiziaria in materia civile e penale (sistema e-CODEX) e che modifica il Regolamento (UE) 2018/1726.

¹² Con tale espressione si fa specifico riferimento a qualsiasi contenuto trasmissibile per via elettronica, ad esempio testo o registrazioni sonore, visive o audiovisive, sotto forma di dati, file o metadati strutturati o non strutturati.

¹³ Tale finalità deve essere necessariamente temperata con altre esigenze, come precisamente indicato all'art. 4 del Regolamento. Esso è preposto al rispetto dei diritti fondamentali dell'uomo, quali il diritto di accesso effettivo alla giustizia, il diritto a un equo processo, il principio di non discriminazione, il diritto alla protezione dei dati personali e il diritto alla riservatezza.

¹⁴ Esso provvede allo scambio di dati nell'ambito della giustizia elettronica e offre a tale settore una soluzione interoperabile per collegare i sistemi IT delle autorità nazionali competenti, come la magistratura, o i sistemi di altre organizzazioni. Il sistema e-CODEX dovrebbe pertanto essere preferito al fine di costruire una rete di comunicazione interoperabile, sicura e decentrata. Esso si compone di due elementi software: un gateway, per lo scambio di messaggi con altri gateway (cioè un dispositivo che, ad esempio, favorisce il collegamento tra due reti differenti, funzionando come punto di scambio tra di esse) e un connettore, che fornisce una serie di funzionalità relative allo scambio di messaggi tra i sistemi IT nazionali, come la verifica delle firme elettroniche e l'avviso di ricevimento. Il connettore, inoltre, è in grado di strutturare, registrare e collegare messaggi, nonché di verificarne l'integrità e l'autenticità. Infine, crea prove e la relativa marca temporale del ricevimento dei messaggi scambiati.

¹⁵ Per approfondimenti si veda A. DAVOLI, *Cooperazione di polizia*, aprile 2024, consultabile al seguente link: <https://www.europarl.europa.eu/factsheets/it/sheet/156/cooperazione-di-polizia>. Ultima consultazione il 4 ottobre 2025.

¹⁶ L'Agenzia è entrata in funzione nel 1998 con la Convenzione Europol del 1995 ed è stata riformata da ultimo con il Regolamento n. 2016/794. Essa, con sede a L'Aia, assiste le autorità degli Stati membri coinvolte nel contrasto al crimine fornendo una piattaforma per lo scambio e l'analisi di informazioni su una serie di attività criminali gravi e a carattere transnazionale (che interessano quindi due o più Stati membri). Europol, che vede la propria base giuridica nell'art. 88 TFUE, funge dunque da centro di sostegno per le operazioni di contrasto, centro di informazioni sulle attività criminali e centro di competenze in tema di applicazione della legge.

¹⁷ L'acronimo sta per Agenzia dell'Unione europea per la formazione delle autorità di contrasto, la quale è dedicata allo sviluppo, all'attuazione e al coordinamento della formazione dei funzionari delle autorità di contrasto.

¹⁸ Il Comitato permanente per la cooperazione operativa in materia di sicurezza interna, istituito nel 2010.

¹⁹ Il Centro UE di situazione e di intelligence si occupa esclusivamente di riesaminare strategicamente le informazioni fornite dai servizi di intelligence, militari, diplomatici e di polizia.

di contrasto ed è operativo nella maggior parte dei paesi UE e nei paesi associati Schengen²⁰. Il SIS viene impiegato dalle autorità di frontiera, di immigrazione, di polizia, doganali e giudiziarie dell'UE e dei paesi associati Schengen, consentendo alle autorità nazionali competenti di inserire e consultare segnalazioni su persone e oggetti in una banca dati comune²¹.

2. Le banche dati e i sistemi informativi.

Gli strumenti che consentono di raccogliere e scambiare dati utili a identificare possibili autori di reato o soggetti condannati in processi penali sono, dunque, importantissimi per la cooperazione di polizia in Europa.

Il sistema SIS è stato aggiornato con l'introduzione del SIS II nel 2013. Una significativa funzionalità aggiuntiva è stata la possibilità di aggiungere impronte digitali e fotografie alle segnalazioni. Il sistema SIS II è stato a sua volta rinnovato, conservando a partire da marzo 2023^{22,23} anche impronte palmari, impronte sconosciute acquisite sulle scene del crimine dei reati gravi, così come i file standardizzati per la ricerca dei profili di DNA delle persone di cui è stata segnalata la scomparsa o dei loro cari, al fine di consentire l'identificazione degli scomparsi, alcune nuove tipologie di oggetti elettronici (IT items), parti di veicoli (i numeri seriali di parti del veicolo quali motore, batterie, etc.), riferimenti del motore di aeromobili

È, invece, operativo dal 2011 il Sistema di Informazione Visti (VIS), una banca dati che agevola la procedura relativa ai visti per soggiorni di breve e lunga durata, permettendo alle autorità di confrontare i dati biometrici²⁴ allo scopo di accertare l'identità delle persone.

Per i viaggiatori esenti dall'obbligo di visto verrà utilizzato un Sistema Europeo di Informazione e Autorizzazione ai Viaggi (ETIAS)²⁵, che consentirà di

²⁰ Per approfondimenti sull'argomento si veda il sito ufficiale del Sistema, consultabile al seguente link: <https://eur-lex.europa.eu/IT/legal-content/summary/a-strengthened-schengen-information-system.html#:~:text=Il%20sistema%20d'informazione%20Schengen,paesi%20membri%20dell'accordo%20di.> Ultima consultazione il 4 ottobre 2025.

²¹ In particolare, il SIS contiene segnalazioni di persone od oggetti che rientrano in una delle seguenti categorie: in attesa di rimpatrio, respinti, ricercati, persone scomparse, minori a rischio di sottrazione, persone vulnerabili a cui deve essere impedito di viaggiare, persone tenute a presenziare ad un procedimento giudiziario, soggetti destinatari di controlli, ignoti ricercati. Inoltre, in riferimento ai soggetti inseriti nel sistema, il SIS conterrà le seguenti informazioni: dati identificativi, motivi della segnalazione, azione da eseguire richiesta, informazioni su procedimenti penali, fotografie, informazioni su oggetti collegati a persone, documenti di identificazione, oltre a dati biometrici, come impronte digitali e profili di DNA. Inoltre, i dati inseriti nel SIS devono essere di qualità, accurati e completi e contenere elementi essenziali, quali il nome del soggetto, l'anno di nascita, il riferimento della decisione che ha dato luogo alla segnalazione e l'azione da eseguire nei suoi confronti.

²² Per maggiori informazioni si rimanda al sito ufficiale: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_it. Ultima consultazione il 4 ottobre 2025.

²³ I dati del SIS fanno riferimento ai regolamenti (UE) 2018/1860, (UE) 2018/1861 e (UE) 2018/1862 del Parlamento europeo e del Consiglio.

²⁴ Nel sistema VIS vengono inserite non solo le informazioni relative alle impronte digitali del soggetto interessato, ma anche un'immagine scannerizzata della pagina dei dati anagrafici del documento di viaggio.

²⁵ Istituito con Regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio del 12 settembre 2018 che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226; visionabile al seguente link: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32018R1240>. Ultima consultazione il 4 ottobre 2025.

effettuare verifiche preventive sui cittadini di paesi terzi. Tale sistema, che doveva essere utilizzato a partire dal 2022, non sarà operativo prima dell'ultimo trimestre del 2026, dovendo attendere la piena operatività del sistema di ingressi/uscite (EES), adottato con Regolamento del novembre 2017²⁶, che sarà introdotto gradualmente nei sei mesi successivi al 12 ottobre 2025. EES registrerà i dati di ingresso, di uscita e di respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne dello spazio Schengen. Nella banca dati EES saranno conservate diverse informazioni, quali: dati contenuti nei documenti di viaggio, data e luogo di ogni entrata e uscita, nonché immagini del volto e impronte digitali. La persona al momento dell'ingresso in frontiera, si reca ad una postazione (*kiosk*) che automaticamente consente autonomamente l'acquisizione delle impronte, la scansione del documento, e l'immagine faciale. Le Autorità che sono deputate al trattamento dei dati coerentemente alla funzione svolta (immigrazione e frontiera), nonché dalle Autorità designate, intese quale Autorità deputate alla repressione di reati gravi e terrorismo (Forze di polizia) avranno accesso ai dati EES²⁷.

Successivamente alla piena operatività dell'EES, i cittadini provenienti dai Paesi esenti da visto dovranno essere in possesso di un'autorizzazione di viaggio ETIAS per potersi recare nei paesi europei²⁸.

Da menzionare è anche la Direttiva sul codice di prenotazione²⁹, che ha dato luogo al sistema PNR, all'interno del quale vengono raccolte e conservate le informazioni personali fornite dai passeggeri ai vettori aerei. Tale normativa disciplina, altresì, il trasferimento di tali dati alle autorità di contrasto degli Stati membri, nonché le modalità di trattamento degli stessi³⁰.

Un altro strumento di grande importanza in Europa è il Sistema Europeo di Informazione sui Casellari Giudiziali (ECRIS)³¹, creato nel 2012 per consentire agli Stati membri di condividere facilmente informazioni sulle condanne penali. Il sistema, riformato nel 2019, include, poi, anche una banca dati centralizzata

²⁶ Regolamento (UE) 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; consultabile al seguente link: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017R2225>. Ultima consultazione il 4 ottobre 2025.

²⁷ Per approfondimenti sul tema si consiglia di visionare il seguente link: https://travel-europe.europa.eu/ees/data-held-ees_en. Ultima consultazione il 27 settembre 2025.

²⁸ L'autorizzazione in parola dovrà essere richiesta online, attraverso la compilazione di un questionario volto a carpire le seguenti informazioni: dati personali e documento di viaggio dell'interessato, durata del soggiorno, presenza di conflittualità nella zona o nel Paese di provenienza ecc. L'autorizzazione ETIAS, infine, verrà abbinata al passaporto del viaggiatore e avrà una durata di tre anni.

²⁹ Si tratta della 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 di reati gravi, visionabile al seguente link: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0681>. Ultima consultazione il 4 ottobre 2025.

³⁰ I dati PNR dei passeggeri vengono conservati per un periodo di cinque anni, al fine di garantire la sicurezza e proteggere la vita e l'incolumità delle persone attraverso la prevenzione, l'accertamento, l'indagine e il perseguimento dei reati di terrorismo e dei reati gravi. Per ulteriori informazioni, si consiglia la seguente lettura al link: <https://www.consilium.europa.eu/it/policies/fight-against-terrorism/passenger-name-record/#pnr>. Ultima consultazione il 4 ottobre 2025.

³¹ «Il pacchetto ECRIS è composto da un regolamento che istituisce un sistema centralizzato per individuare lo Stato membro o gli Stati membri che possono essere in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e una direttiva, che modifica la decisione quadro in vigore concernente ECRIS alla luce di questo nuovo sistema centralizzato per lo scambio di informazioni sui cittadini di paesi terzi», contenuto tratto dal Comunicato Stampa del 09.04.2019 pubblicato sul sito: <https://www.consilium.europa.eu/it/press/press-releases/2019/04/09/exchanging-criminal-records-eu-agrees-a-reformed-ecris-system/>. Ultima consultazione il 4 ottobre 2025.

con informazioni sulle condanne a carico di cittadini di paesi terzi e apolidi (il c.d. ECRIS-TCN)^{32,33}.

È doveroso, infine, menzionare lo *European Dactyloscope* (EURODAC)^{34,35}, il database istituito dal Regolamento CE n. 2725/2000³⁶ e concepito per raccogliere le impronte digitali dei richiedenti asilo e degli immigrati irregolari che varcano i confini di un Paese europeo. Ogni Paese membro procede tempestivamente al rilevamento delle impronte digitali di tutte le dita di ogni soggetto interessato che abbia compiuto i 14 anni di età³⁷, fissando periodi di conservazione differenziati³⁸. EURODAC permette il confronto delle impronte di cittadini stranieri che si trovano illegalmente sul territorio di uno Stato membro con quelle della banca dati centrale, per verificare se l'interessato non abbia già presentato una domanda d'asilo altrove.

Il Regolamento istitutivo di EURODAC si premurava di assicurare la giusta protezione dei dati a carattere personale. Difatti, non vengono «inserite le informazioni relative al nome e alla nazionalità dei soggetti, al fine evidente di escludere alla radice i possibili abusi del database»³⁹. Gli Stati membri devono, infatti, garantire che tutte le operazioni relative al prelievo, utilizzo, trasmissione, conservazione o cancellazione dei dati attinenti alle impronte digitali avvengano nel rispetto delle norme dell'ordinamento europeo. I dati, al momento della loro trasmissione, devono essere esatti e attuali e potranno

³² L'atto istitutivo è costituito dal Regolamento (UE) 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 paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il Regolamento (UE) 2018/1726.

³³ ECRIS-TCN sarà un sistema hit/no-hit centralizzato, utile a supportare il già esistente database ECRIS, in quanto consentirà alle autorità di contrasto degli Stati membri di accedere alle informazioni contenute nel certificato del casellario giudiziale di un soggetto, conoscendo così la sua storia criminale. In tal modo, ECRIS-TCN contribuirà all'implementazione del principio del mutuo riconoscimento delle sentenze e delle decisioni giudiziali all'interno dell'area europea JHA.

³⁴ Per ulteriori informazioni si consiglia "Supporting Asylum and Migration Policies Across Europe" consultabile al seguente link: <https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac>. Ultima consultazione il 4 ottobre 2025.

³⁵ Eurodac, così come A.F.I.S. e VIS, effettua un raffronto delle impronte di una persona con tutte le serie di impronte, svolgendo un'interrogazione molteplice ("one-to-many"), al fine di identificare la persona in base alle impronte. Ciò differenzia detti database dal sistema di informazione Schengen di seconda generazione (SIS II), il quale immagazzina le impronte digitali nel sistema centrale e le utilizza soltanto per confermare l'identità della persona individuata a seguito di un'interrogazione univoca ("one-to-one"), in genere, sul nome e sulla data di nascita. Commento tratto da Commissione europea, *Relazione della Commissione al Parlamento europeo e al Consiglio, Stato di evoluzione e disponibilità della tecnologia che permette di identificare una persona in base alle impronte digitali conservate nel sistema d'informazione Schengen di seconda generazione (SIS II)*, Bruxelles, 29.02.2016, p. 2.

³⁶ 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.

³⁷ Oltre alle impronte digitali, i dati trasmessi, ai sensi dell'art. 5, indicano lo Stato d'origine, il luogo e la data dell'eventuale domanda di asilo, il sesso, un numero identificativo, nonché la data in cui sono state prese le impronte digitali e la data in cui sono stati trasmessi i dati a EURODAC.

³⁸ Per il richiedente asilo la documentazione è conservata per dieci anni, salvo che ottenga la cittadinanza di uno degli Stati membri; in tal caso, gli elementi che lo riguardano devono essere cancellati non appena ottenuto il titolo. Per gli individui stranieri fermati in occasione dell'attraversamento irregolare di una frontiera esterna i dati sono conservati per due anni a decorrere dalla data di acquisizione dei rilievi dattiloscopici. Essi vengono invece cancellati prima dello scadere dei due anni se al soggetto viene rilasciato un permesso di soggiorno, la cittadinanza, o se egli ha lasciato il territorio degli Stati membri.

³⁹ M. GIALUZ, *Principio di accessibilità e banche dati di "primo pilastro"*, in F. PERONI, M. GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, EUT - Edizioni Universitarie Trieste, Trieste, 2009, p. 146.

essere consultati soltanto dallo Stato membro che ne ha chiesto l'invio e per gli scopi espressamente previsti da EURODAC⁴⁰.

L'atto istitutivo di EURODAC è stato abrogato dal Regolamento (UE) n. 603/2013⁴¹, il quale ne ha ampliato l'operatività, al fine di facilitare l'individuazione del Paese membro responsabile della disamina della domanda di asilo. Grazie alla modifica introdotta dal nuovo Regolamento, si consente alle forze dell'ordine di consultare la banca dati in ottica investigativa e quindi per prevenire e contrastare atti terroristici o reati particolarmente gravi di natura transnazionale⁴².

Il nuovo Regolamento (UE) 2024/1358 del Parlamento europeo e del Consiglio istituisce l'Eurodac per il confronto dei dati biometrici ai fini dell'identificazione dei cittadini richiedenti protezione individuale (sistema di asilo), protezione dei minori, cittadini di paesi terzi e apolidi il cui soggiorno è irregolare e le richieste di confronto presentate dalle Autorità designate al contrasto degli Stati membri e da Europol per la prevenzione, l'accertamento o l'indagine di reati gravi o terrorismo⁴³.

Per quanto concerne l'Italia, i dati biometrici sono acquisiti mediante procedure distinte per le finalità ed inseriti nel sistema A.F.I.S.⁴⁴, ma anche in EURODAC, se le finalità rientrano in quanto precedentemente indicato.

⁴⁰ Vi si aggiunga anche una serie di controlli che si possono così declinare: all'ingresso della sede, verifiche dei supporti, della registrazione, dell'inserimento, dell'accesso e della trasmissione dei dati, nonché del loro trasporto. Allo stesso modo viene protetto l'accesso alle registrazioni delle operazioni di trattamento dei dati avvenute nell'unità centrale.

⁴¹ 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, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (rifusione).

⁴² Dal nuovo Regolamento emergono diversi punti chiave che è possibile sintetizzare come segue: trasmissione a EURODAC delle impronte digitali entro il termine di 72 ore; possibilità di interrogare il database per determinare se il soggetto illegalmente presente sul territorio di un Paese abbia precedentemente inoltrato domanda di asilo o se sia stato fermato in occasione di un ingresso illegale; cancellazione dei dati una volta che il richiedente ottiene la cittadinanza di un Paese membro; autorizzazione all'accesso del database da parte delle autorità di contrasto e di Europol al fine di condurre indagini e accertamenti, soltanto a condizione che vi siano ragionevoli motivi di ritenere che ciò possa portare beneficio all'operazione e che rappresenti l'ultima risorsa, esperiti infruttuosamente gli altri tentativi di ricerca. In riferimento a quest'ultima proposta, «il G.E.P.D. raccomanda che le autorità degli Stati membri e gli organi dell'Unione continuino a poter visualizzare solo i dati riguardanti l'esecuzione dei loro compiti specifici, anche nel caso in cui i set di dati siano collegati in una sequenza», così GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Parere del 30 novembre 2020*, pubblicato in G.U.U.E C 99 del 23.03.2021, in *Il diritto dell'informazione e dell'informatica*, 2021, fasc. 3, pp. 623-624.

⁴³ Regolamento (UE) 2024/1358 del Parlamento europeo e del Consiglio, del 14 maggio 2024, che istituisce l'«Eurodac» per il confronto dei dati biometrici ai fini dell'applicazione efficace dei regolamenti (UE) 2024/1351 e (UE) 2024/1350 o del Parlamento europeo e del Consiglio e della direttiva 2001/55/CE del Consiglio e ai fini dell'identificazione dei cittadini di paesi terzi e apolidi il cui soggiorno è irregolare, e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, che modifica i regolamenti (UE) 2018/1240 e (UE) 2019/818 del Parlamento europeo e del Consiglio e che abroga il regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, consultabile al seguente link: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024R1358>. Ultima consultazione il 27 settembre 2025.

⁴⁴ In Italia le impronte digitali rilevate da un sospettato o raccolte sulla scena del crimine vengono inserite all'interno del sistema A.F.I.S. (acronimo di Automated Fingerprint Identification System), un sistema di identificazione biometrica che utilizza la tecnologia di imaging digitale per ottenere, archiviare e analizzare i dati delle impronte digitali. L'impiego dell'A.F.I.S. è sostanzialmente duplice: ricerca decadattilare

3. Il quadro normativo europeo che regola gli scambi di dati biometrici e disciplina la riservatezza degli stessi.

Il diritto alla protezione dei propri dati personali è specificamente riconosciuto dalla Carta dei diritti fondamentali dell'UE⁴⁵. Esso, tuttavia, è destinato a subire una compressione qualora si svolga un'attività di contrasto. A tal proposito, il Regolamento (UE) 2016/679 e la Direttiva (UE) 2016/680 costituiscono un passo essenziale per rafforzare i diritti fondamentali dei singoli nell'era digitale, garantendo che i dati personali di vittime, testimoni e indagati siano debitamente protetti⁴⁶.

Con la pronuncia del 26 gennaio 2023, C-205/21, la Corte di Giustizia dell'UE (CGUE) si esprimeva circa la violazione della *privacy*, dovuta alla registrazione «sistematica» dei dati biometrici e genetici dei soggetti accusati di un reato e alla possibilità di ottenere coattivamente dati nel caso in cui la persona sia indagata per un reato doloso procedibile d'ufficio. In tale sede sosteneva la CGUE che l'autorità competente «è tenuta pertanto a verificare e a dimostrare che tale raccolta sia assolutamente/strettamente necessaria per il conseguimento degli obiettivi specifici perseguiti e, inoltre, che tali obiettivi non possono essere raggiunti mediante misure che costituiscono un'ingerenza grave nei diritti e nelle libertà della persona interessata»⁴⁷.

A questo punto, il richiamo al Programma dell'Aia⁴⁸ risulta doveroso, in quanto esso ha il merito di aver coniato il principio di disponibilità⁴⁹ quale perno della cooperazione informativa e di aver manifestato la primordiale esigenza di trovare il giusto equilibrio fra sicurezza e tutela della *privacy* in sede di scambio di informazioni fra autorità giudiziarie e di polizia.

preventiva, in ossequio a quanto previsto dall'art. 4 T.U.L.P.S., e ricerca di frammento papillare in ambito giudiziario, in relazione ad un accertamento tecnico svolto sulla scena del crimine ex art. 354 c.p.p.

In particolare, «quando uno Stato membro introduce una segnalazione, ma non dispone delle impronte per completarla, un altro Stato membro che ha già avuto a che fare con la persona in questione può disporre delle impronte nel proprio A.F.I.S. nazionale. Il manuale SIRENE descrive come inviare le impronte da allegare alla segnalazione. Poiché le impronte possono essere acquisite in altri sistemi, è necessario garantire che le impronte siano corredate di un registro del "punteggio di qualità", in modo che ogni uso delle impronte avvenga in un contesto informato», così in Commissione europea, *Relazione della Commissione al Parlamento europeo e al Consiglio, Stato di evoluzione e disponibilità della tecnologia che permette di identificare una persona in base alle impronte digitali conservate nel sistema d'informazione Schengen di seconda generazione (SIS II)*, Bruxelles, 29.02.2016, pp. 7-8.

⁴⁵ A cui è stata attuazione in Italia dapprima con la L. n. 675 del 31 dicembre 1996 (per un approfondimento si veda C. M. BIANCA, F.D. BUSNELLI (a cura di), *Tutela della privacy*, in *Le nuove leggi commentate*, 1999) e successivamente con il D. Lgs. 196/2003 Codice in materia di protezione dei dati personali (per un approfondimento si veda C. M. Bianca, F.D. Busnelli, *La protezione dei dati personali - Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*, CEDAM, 2007).

⁴⁶ Per approfondimenti sul tema si veda GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Relazione 2023 del Garante per la protezione dei dati personali*, 3 luglio 2024, reperibile al sito: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10032003>. Ultima consultazione il 4 ottobre 2025.

⁴⁷ S. EL SABI, *La tutela della privacy nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, in *Il diritto dell'informazione e dell'informatica*, 2023, fasc. 4/5, p. 790.

⁴⁸ Programma dell'Aia sul rafforzamento della libertà, della sicurezza e della giustizia nell'Unione Europea, allegato n. 1 delle Conclusioni della Presidenza del Consiglio europeo di Bruxelles del 4-5 novembre 2004 e visionabile al seguente sito internet: <https://www.orientamentoirreer.it/sites/default/files/norme/UE%20029%202004%20bruxelles.pdf>.

Ultima consultazione il 4 ottobre 2025.

⁴⁹ Esso prevede che qualsiasi agente dei servizi di polizia di uno Stato membro, che abbia bisogno di determinate informazioni nell'esercizio delle proprie funzioni, possa ottenerle dai servizi di un altro Stato membro, purché siano rispettate alcune condizioni.

3.1. La Decisione quadro 2006/960/GAI (cd. Swedish Framework) e la Direttiva 2023/977.

Un ruolo eminente nel contesto della protezione dei dati biometrici viene svolto dal c.d. Swedish Framework (su iniziativa del Regno di Svezia), ossia la Decisione quadro 2006/960/GAI^{50,51}, recepita nel nostro Paese dal D. Lvo n. 54/2015⁵². Con l'obiettivo di rendere sempre più celere ed efficiente la trasmissione di informazioni da paese a paese, la Decisione prevede regole specifiche in relazione alle tempistiche da rispettare e agli standard comuni da impiegare per lo scambio di dati⁵³. Ben più importante è che essa pone l'accento su tre principi essenziali dell'attività: il principio di disponibilità, atto ad assicurare che le Forze dell'Ordine degli Stati membri compulsanti possano accedere alle informazioni necessarie contenute nei *database* degli Stati consultati, e il principio dell'accesso equivalente, posto a garanzia di una procedura di comunicazione esente da condizioni più rigorose di quelle applicabili a livello nazionale. Questo secondo principio non esclude, in ogni caso, la necessità, talvolta, di subordinare il rilascio di determinate informazioni alla richiesta di un'autorizzazione da parte dell'autorità giudiziaria. In ogni caso, il rispetto del principio di proporzionalità deve rivestire carattere preminente⁵⁴, assicurando la protezione e la riservatezza dei dati coinvolti nello scambio, sulla base della normativa nazionale dello Stato membro che li riceve. Tali dati, considerato il loro carattere sensibile, devono essere salvaguardati durante tutte le fasi di *information sharing*.

Ciononostante, nel 2007, il Garante europeo per la protezione dei dati aveva già evidenziato le potenziali criticità nonché i pericoli che una normativa generica e non armonizzata in materia di circolazione e scambio dei dati avrebbe potuto comportare su tali importantissimi diritti⁵⁵.

⁵⁰ Decisione quadro 2006/960/GAI del Consiglio dell'Unione europea del 18 dicembre 2006, relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge, il cui testo completo è visionabile al sito: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:IT:PDF>. Ultima consultazione il 15.02.2025.

⁵¹ All'interno del sistema delle fonti del diritto comunitario, le decisioni quadro afferiscono all'area del c.d. Terzo Pilastro, strettamente correlato, appunto, al settore della cooperazione di polizia e giudiziaria in materia penale. Si ricorda, inoltre, che le decisioni quadro sono vincolanti per gli Stati membri quanto al risultato da ottenere, salva restando la competenza delle autorità nazionali in merito alla forma e ai mezzi.

⁵² Decreto legislativo 23 aprile 2015, n. 54, Attuazione della decisione quadro 960/2006/GAI del Consiglio del 18 dicembre 2006 relativa alla semplificazione dello scambio di informazioni e intelligence tra le Autorità degli Stati membri dell'Unione Europea incaricate dell'applicazione della legge.

⁵³ La Decisione impone dei termini ben precisi per la comunicazione delle informazioni richieste che siano di particolare urgenza, a partire dalle otto ore per quelle direttamente accessibili fino a un periodo di tre giorni per i dati il cui ottenimento è considerato più dispendioso. Nel caso, invece, di richieste non urgenti i termini risultano più dilazionati e corrispondono a sette e a quattordici giorni, rispettivamente nell'ipotesi di informazioni direttamente o indirettamente accessibili. Dal punto di vista della lingua e del canale di scambio delle informazioni, la Decisione svedese pare essere piuttosto generica, poiché nulla specifica a tal proposito, limitandosi ad affermare che possa essere utilizzato qualsiasi canale di comunicazione e che la lingua debba essere quella applicabile al canale utilizzato. Tale genericità si è rivelata nel corso degli anni un punto debole dell'intera catena di trasmissione delle informazioni e, infatti, sarà oggetto di modifiche.

⁵⁴ Si tratta di un principio postulato dall'art. 7, che così recita: "le informazioni e l'intelligence fornite si limitano a quanto ritenuto utile e necessario per l'individuazione, la prevenzione o l'indagine sui reati o le attività criminali in questione".

⁵⁵ Preme ricordare, sul punto, che la più recente normativa in tema di 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

La Decisione 2006/960/GAI è stata abrogata recentemente con l'entrata in vigore della Direttiva 2023/977⁵⁶, recepita dal nostro ordinamento con il decreto legislativo 12 novembre 2024, n.181, che all'art.2 rubricato "Definizioni" distingue l'Autorità di contrasto competente (Le Forze di polizia ai sensi dell'art.16 della legge 1 aprile 1981, n.121) dall'Autorità di contrasto designata come autorizzata a presentare richieste di informazioni al punto di contatto unico nazionale. Nell'ambito del Dipartimento della Pubblica Sicurezza il punto di contatto nazionale è normalmente individuato nel Servizio per la Cooperazione internazionale di Polizia della Direzione Centrale della Polizia Criminale, che ha carattere interforze⁵⁷.

Il nuovo testo, al fine di fornire una definizione di «dati personali» oggetto del trattamento, richiama il Regolamento (UE) 2016/679⁵⁸ e la Direttiva (UE) 2016/680⁵⁹ che, all'art. 3, punto 1) considera tali «qualsiasi informazione riguardante una persona fisica identificata o identificabile, (l'«interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica».

Per quanto attiene nello specifico alle informazioni oggetto di trasmissione, la Direttiva del 2023 amplia il significato terminologico⁶⁰ e istituisce i cc.dd.

dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, è da rinvenirsi nella Direttiva UE n. 2016/680, che fa parte del c.d. nuovo pacchetto protezione dati, insieme al noto Regolamento generale sulla protezione dei dati, c.d. GDPR, Regolamento UE 2016/679. Essa dunque mira a regolare la protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale ma lascia impregiudicate le disposizioni che attengono al funzionamento di Europol, Eurojust, al sistema di informazione di Schengen (SIS) e il sistema informativo doganale (SID) nonché, per quanto in questa sede interessa maggiormente, restano intoccate le disposizioni sul trasferimento automatizzato tra Stati membri di profili DNA, dati dattiloscopici e dati di immatricolazione dei veicoli, sulla base della Decisione 2008/615/GAI, in L. SCAFFARDI, *Next Generation Prüm e le scelte strategiche della UE: dall'ampliamento nello scambio di dati genetici all'introduzione del riconoscimento facciale*, in *Federalismi.it*, 2021, fasc. 8, p. 205.

⁵⁶ Direttiva 2023/977 del Parlamento europeo e del Consiglio, del 10 maggio 2023, relativa allo scambio di informazioni tra le autorità di contrasto degli Stati membri, il cui testo integrale può essere consultato al seguente link: <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32023L0977>. Ultima consultazione il 4 ottobre 2025.

⁵⁷ Decreto legislativo 12 novembre 2024, n. 181, di attuazione della Direttiva (UE)2023/977 del Parlamento europeo e del Consiglio, del 10 maggio 2023, relativa allo scambio di informazioni tra le autorità di contrasto degli Stati membri e che abroga la decisione quadro 2006/960/GAI del Consiglio. (24G00197), visionabile al seguente link: <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024-11-12;181>. Ultima consultazione il 15.02.2025.

⁵⁸ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

⁵⁹ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio; visionabile al seguente link: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680>. Ultima consultazione il 15.02.2025.

⁶⁰ Comprendendovi "qualsiasi contenuto relativo a una o più persone fisiche o giuridiche, fatti o circostanze pertinenti per le autorità di contrasto competenti ai fini dello svolgimento dei loro compiti, previsti dal diritto nazionale, di prevenzione o individuazione dei reati o di relativa indagine, incluse le informazioni di polizia di natura penale" (art. 2, n. 4). La Decisione quadro, invece, considerava tali, in modo generico, "qualsiasi tipo di informazioni o dati detenuti da autorità incaricate dell'applicazione della legge" e "da autorità pubbliche o da enti privati che siano accessibili alle autorità incaricate dell'applicazione della legge".

“punti di contatti unici” adibiti a richiederle⁶¹, che costituiscono i mittenti delle richieste e a loro volta i destinatari delle stesse dei Paesi membri. Ogni richiesta deve rispettare, poi, delle prescrizioni ben precise, ossia contenere riferimenti specifici circa i dettagli, la finalità sottostante e i motivi dell’urgenza, se presenti.

Il nuovo testo opera poi una distinzione tra le informazioni basata sulla loro reperibilità e accessibilità⁶². La Direttiva ambisce anche a creare una collaborazione sempre più stretta con Europol, facendo così un passo in avanti rispetto alle previsioni contenute nel testo del 2006⁶³.

Relativamente ai canali di scambio, il nuovo atto sollecita l’utilizzo del canale di comunicazione sicuro di Europol SIENA⁶⁴, il cui utilizzo potrà essere accantonato solo in particolari ipotesi (ad esempio per un guasto tecnico o perché l’urgenza della richiesta necessita dell’utilizzo di un altro canale di comunicazione).

Un ulteriore aspetto originale attiene all’istituzione, presso i punti di contatto unici, del c.d. sistema di gestione dei casi, che l’art. 16 configura come “un sistema elettronico unico di trattamento dei casi che funga da archivio e consenta al punto di contatto unico di svolgere i suoi compiti ai sensi della presente direttiva”⁶⁵. Inoltre, il sistema registra gli accessi ai fini di rendicontabilità e di cybersicurezza. Questo perché i dati oggetto di trasmissione necessitano di ricevere una copertura adeguata, stante la loro stretta correlazione con la sfera più personale del soggetto.

Oltre alle accortezze previste dall’art. 9 (esattezza, completezza e aggiornamento dei dati), viene stabilito che le informazioni debbano e possano essere utilizzate solo per gli scopi per i quali sono state trasmesse, mentre il

senza il ricorso a mezzi coercitivi, a norma dell’articolo 1, paragrafo 5. Sempre da un punto di vista terminologico, la Direttiva sostituisce l’espressione “autorità competente dell’applicazione della legge” con i termini “autorità di contrasto competente” e “autorità di contrasto designata”, con la prima facendo riferimento a “qualsiasi autorità di polizia, doganale o altra autorità degli Stati membri competente, ai sensi del diritto nazionale, a esercitare l’autorità e ad adottare misure coercitive ai fini della prevenzione e dell’individuazione dei reati o delle relative indagini, o qualsiasi autorità che partecipi a entità comuni istituite tra due o più Stati membri ai fini della prevenzione e dell’individuazione dei reati o delle relative indagini” (art. 2, n. 1). Con la seconda denominazione si indica, invece, “un’autorità di contrasto competente autorizzata a presentare richieste di informazioni ai punti di contatto unici di altri Stati membri” (art. 2, n. 2).

⁶¹ Se questo aspetto era totalmente assente nel precedente testo, la recente Direttiva gli attribuisce un valore imprescindibile dedicandogli l’intero capo V, al fine di regolarne l’istituzione, i compiti, le capacità, l’organizzazione, la composizione e la formazione degli operatori. Tale organo assicura un’operatività e un’attività 7/7 su 24h, con un personale qualificato anche grazie alla partecipazione a corsi di formazioni erogati da CEPOL.

⁶² I dati direttamente accessibili dovranno essere comunicati entro il termine di otto ore, mentre la trasmissione delle informazioni indirettamente accessibili potrà essere posposta, fino a un massimo di tre giorni. Questi sono i termini fissati per le trasmissioni caratterizzate da particolare urgenza, sicché per tutte le altre richieste varrà il termine di sette giorni di calendario.

⁶³ L’art. 12, infatti, ammette la possibilità di comunicare determinate informazioni all’Agenzia valutando caso per caso se tali dati coinvolgano reati che rientrano nell’ambito dei suoi obiettivi, come indicati dall’art. 3 del Regolamento (UE) 2016/794.

⁶⁴ Per informazioni più dettagliate si consiglia di visionare il seguente link: <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena>. Ultima consultazione il 4 ottobre 2025.

⁶⁵ Esso costituisce l’entità centrale incaricata di coordinare e agevolare lo scambio di informazioni, registrando le richieste di informazioni ricevute e inviate. L’archivio memorizza le connessioni instaurate sia tra i diversi punti di contatto unici, sia tra le autorità di contrasto competenti e, infine, tra queste ultime e i punti di contatto unici.

trattamento per una finalità diversa potrà essere consentito solo previa autorizzazione giudiziale dello Stato membro che fornisce tali dati.

Da ultimo, la Direttiva esplicita i cinque principi fondanti lo scambio di informazioni nell'ambito della cooperazione transnazionale: il principio di disponibilità, dell'accesso equivalente, il principio di riservatezza nonché quello relativo alla proprietà e affidabilità dei dati. Chiaramente le prescrizioni e le accortezze di cui sopra sono riservate in modo particolare ai dati biometrici, in virtù della loro capacità di identificare in modo univoco una persona fisica. In generale, tali sono «quei dati personali che derivano da caratteristiche fisiche o comportamentali uniche e, pertanto, identificative di ciascun individuo (si pensi alle impronte digitali, alla particolare conformazione fisica della mano o del volto, dell'iride o della retina, alla forma grafometrica nonché al timbro e alla tonalità della voce)»⁶⁶.

3.2. Il trattato di Prüm e le successive Decisioni.

Nella città tedesca di Prüm il 27 maggio 2005 Belgio, Germania, Spagna, Lussemburgo, Austria, Paesi Bassi e Francia hanno sottoscritto un importante trattato in materia di dati biometrici, sin da subito aperto all'adesione di tutti gli Stati Membri. Tale accordo si focalizzava principalmente su cinque aree di intervento: la raccolta e lo scambio di informazioni relative al DNA; la raccolta e lo scambio di dati sulle impronte digitali; lo scambio di dati relativi ai registri di immatricolazione degli autoveicoli; le misure atte a prevenire reati terroristici e infine le misure dirette al contrasto dell'immigrazione illegale. Le parti essenziali del Trattato venivano, poi, attuate con le Decisioni-quadro 2008/615/GAI e 2008/616/GAI, ossia le cc.dd. Decisioni Prüm⁶⁷. L'Italia aderì al trattato di Prüm solo con la Legge del 30 giugno 2009, n. 85, con la quale venne istituita la banca dati nazionale del DNA e il laboratorio centrale "Grazie De Carli"^{68,69}.

⁶⁶ S. EL SABI, *op. cit.* pp. 791-792.

⁶⁷ A. MARANDOLA, *Information sharing nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione*, in F. PERONI, M. GIALUZ (a cura di), *op. cit.*, pp. 167-168.

⁶⁸ Come specificato da R. BIONDO, *La banca dati nazionale DNA italiana*, in *Rivista Italiana di Medicina Legale*, 2016, fasc. 1, pp. 215-217, l'attività consiste nella raccolta dei profili di DNA dei soggetti destinatari di un provvedimento restrittivo della libertà personale e nel successivo confronto con i profili acquisiti da reperti biologici trovati sulla scena del crimine, aderendo alle Decisioni Prüm. Con l'istituzione di questa banca dati si è definito un nuovo e più efficace metodo di identificazione basato sia sull'impronta digitale che sull'impronta genetica: i dati personali del soggetto che viene sottoposto a un prelievo di saliva sono inseriti nel sistema A.F.I.S. e vengono contrassegnati con un numero identificativo del soggetto. Questo indicatore viene associato al profilo di DNA del soggetto. Soltanto nel momento in cui la banca dati troverà una concordanza tra un profilo di DNA noto e un profilo sconosciuto avverrà l'abbinamento dei dati anagrafici attraverso il numero identificativo rilasciato al momento del prelievo dal sistema A.F.I.S., garantendo sino a questo momento l'anonimato delle informazioni.

⁶⁹ Già all'art. 1, il testo dell'accordo esprimeva l'auspicio che potesse diventare parte integrante del diritto comunitario, manifestandosi favorevole, dunque, a una "europeizzazione" della materia. Il trattato di Prüm enumerava i settori di applicazione e, in particolare, prevedeva disposizioni concernenti lo scambio di dati relativi a DNA e impronte digitali, nonché lo scambio di informazioni su persone ricercate o sospettate, su autoveicoli e sui proprietari degli stessi. Contemplava, inoltre, la possibilità di avvalersi dei cc.dd. *Sky Marshals*, ossia gli "scheriffi del cielo", a bordo degli aerei commerciali al fine di prevenire e contrastare eventuali attacchi o dirottamenti aerei. Infine, delineava disposizioni relative allo scambio di informazioni sulla falsificazione di documentazioni, sui rimpatri congiunti e sui pattugliamenti congiunti di frontiera. Il Trattato prevedeva altresì la possibilità di costituire squadre miste per effettuare interventi comuni nel

L'obiettivo delle suddette Decisioni è rappresentato dalla volontà di fare un passo avanti nell'ambito della cooperazione transfrontaliera nella materia della giustizia e degli affari interni, facendo sì che gli Stati membri si concedano «reciprocamente diritti di accesso ai rispettivi schedari automatizzati di analisi del DNA, ai sistemi automatizzati di identificazione dattiloscopica e ai dati di immatricolazione dei veicoli»⁷⁰, tramite un sistema *hit/no-hit*, che offre una struttura di raffronto dei profili anonimi⁷¹.

Per quanto concerne i dati dattiloscopici, viene esclusa l'identificazione diretta della persona interessata⁷² e, come avviene per i profili di DNA, anche nell'ipotesi di trasmissione di dati dattiloscopici, informazioni aggiuntive sono inviate solo a seguito di un primo riscontro positivo sulla base di dati anonimi.

Risulta chiaro come le Decisioni Prüm abbiano svolto il ruolo di promotrici di un approccio innovativo nella cooperazione transfrontaliera a livello comunitario, nonostante i ritardi di alcuni paesi⁷³ e le diverse criticità emerse⁷⁴.

Una criticità particolarmente significativa riguardava la tipologia di profili da registrarsi all'interno delle banche dati. Alcuni Stati membri apparivano maggiormente inclusivi, e quindi pro-securitari, nella scelta dei soggetti da considerare ai fini archivistici (registrazione di individui anche solo sospettati di aver commesso un crimine e poi assolti, ad esempio); mentre altri, come Belgio e Francia, hanno optato per l'inserimento soltanto di profili di individui condannati per gravi reati, dimostrandosi così maggiormente garantisti in termini di protezione dei dati e del diritto alla riservatezza. È evidente, dunque, che "l'efficacia del modello di circolazione e condivisione di dati nel contesto europeo ha risentito e risente tuttora del diverso livello di operatività e connessione negli scambi di dati, che varia molto da Stato a Stato"⁷⁵.

territorio di uno degli Stati contraenti e la mutua assistenza in occasione di manifestazioni di massa, catastrofi e altre gravi calamità.

⁷⁰ V. Considerando n. 10 delle Decisioni Prüm.

⁷¹ In tal modo, i dati aggiuntivi a carattere personale vengono scambiati solo a seguito di un riscontro positivo. La trasmissione e ricezione dei suddetti dati sono disciplinate dalla legislazione nazionale. In particolare, H. MACHADO, R. GRANJA, *Risks and benefits of transnational exchange of forensic DNA data in the EU: The views of professionals operating the Prüm system*, trad. *Rischi e benefici dello scambio transnazionale di dati di DNA in EU: il punto di vista degli operatori del Sistema Prüm*, in *Journal of Forensic and Legal Medicine*, 2019, fasc. 68, p. 1, specifica che "il sistema Prüm funziona in due fasi: durante lo step 1 viene effettuata una ricerca di un profilo di DNA, prelevato da una scena del crimine, all'interno del database nazionale. Qualora non vi sia alcuna corrispondenza, le Decisioni consentono che il numero di riferimento di quel profilo venga trasmesso ai database nazionali di altri Paesi membri. Dopodiché il Paese membro richiedente viene informato circa l'esito positivo o negativo della ricerca. Se vi è una corrispondenza, si apre lo step 2 in cui potranno essere inviate ulteriori informazioni attraverso i canali di comunicazione di polizia o giudiziari esistenti".

⁷² Gli Stati membri devono garantire la disponibilità dei dati indicizzati relativi al contenuto dei sistemi nazionali automatizzati di identificazione dattiloscopica, creati per la prevenzione dei reati e per le relative indagini. Tali dati indicizzati contengono unicamente informazioni dattiloscopiche e un numero di riferimento che le contraddistingue.

⁷³ Si veda sul punto L. SCAFFARDI, *op. cit.*, p. 209.

⁷⁴ Non poche difficoltà, infatti, sono emerse in sede attuativa, stante l'assenza di regolamentazioni e strumenti utili a implementare il "sistema Prüm". Difatti, molti Stati membri aderirono alle Decisioni senza prima dotarsi di banche dati e archivi in cui conservare i dati citati, impedendo così anche la consultazione da parte degli altri partecipanti. Diversi Paesi, quali Italia, Croazia, Grecia, Irlanda e Portogallo, ricevettero, da parte della Commissione europea, una lettera di costituzione in mora per la mancata attuazione delle Decisioni Prüm. A tale prima fase seguì, nel 2017, l'invio di un parere motivato con cui si esortava l'Italia a rispettare gli obblighi giuridici da esse derivanti.

⁷⁵ L. SCAFFARDI, *op. cit.*, pp. 210-211.

Con l'obiettivo di migliorare, semplificare e facilitare lo scambio di informazioni tra le Autorità responsabili della prevenzione, dell'indagine e dell'accertamento dei reati, nel nuovo quadro normativo Prüm II, la cui entrata in funzione è stimata per il 2028, verranno trattati i dati del DNA delle persone scomparse e di resti umani non identificati, immagini del volto ed estratti del casellario giudiziale⁷⁶.

3.3 Dagli studi sulle Decisioni di Prüm al Prüm II.

Uno studio commissionato dal Dipartimento per i diritti dei cittadini e gli affari costituzionali del Parlamento europeo (*European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs*) riconosceva già nel 2018 che, nonostante venga registrato un elevato numero di corrispondenze durante la c.d. Fase 1, solo un numero limitato di queste era segnalato alle autorità pubbliche nazionali⁷⁷.

Tra gli studi sviluppati si inserisce quello di Deloitte, intitolato «*Study on the feasibility of improving information exchange under the Prüm Decisions*» del maggio 2020⁷⁸.

Detta relazione considera diversi aspetti e li raggruppa in 5 ambiti, a partire dal perfezionamento dello scambio automatizzato di informazioni al miglioramento della procedura di follow-up. Si focalizza, inoltre, sull'introduzione di nuove categorie di dati oltre che di una nuova "architettura" informatica, annunciando anche la necessità di introdurre soluzioni di interoperabilità.

Per quanto riguarda il primo profilo di interesse, si prospettava un ampliamento della portata del Prüm *framework*⁷⁹, a cui è strettamente correlata l'aggiunta di ulteriori tipologie di soggetti⁸⁰.

⁷⁶ Infatti, le inefficienze, i ritardi e le difficoltà operative ed applicative sopra evidenziate, unitamente al progresso tecnologico e all'affermarsi di nuove tecniche e strumenti di indagine fondati sull'impiego di dati – anche genetici e biometrici –, nonché le nuove sfide connesse al fenomeno del terrorismo, della criminalità organizzata e dei cyber-crimes, hanno portato le Istituzioni dell'UE, in particolare Consiglio e Commissione, a porre in essere iniziative, mediante la promozione di studi, ricerche, dibattiti tra esperti ed autorità degli Stati membri, volte a promuovere una modernizzazione delle Decisioni di Prüm (adottate nel 2008) e del relativo meccanismo di circolazione dei dati.

⁷⁷ Si fa riferimento allo studio intitolato *Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision STUDY* del 2018 consultabile al seguente link [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU\(2018\)604971_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf). Ultima consultazione 4 ottobre 2025.

⁷⁸ Commissione Europea, Dipartimento Generale per le Migrazioni e gli Affari Interni, *Study on the feasibility of improving information exchange under the Prüm decisions – Advanced technical report – Final version*, Ufficio Pubblicazioni dell'Unione Europea, 2020, consultabile al seguente link: <https://data.europa.eu/doi/10.2837/1710>. Ultima consultazione il 16.02.2025.

⁷⁹ A tal proposito, pare opportuno premettere che nell'ottemperare allo scopo fissato dalle Decisioni Prüm, gli Stati membri sono vincolati al rispetto della propria legislazione nazionale. Le autorità giudiziarie interrogano il sistema per cercare persone scomparse o per identificare civili deceduti, solo se tali circostanze sono considerate parte di un'indagine penale ai sensi della legislazione nazionale; dall'altro lato, in alcuni Paesi membri, come l'Italia, l'autorità giudiziaria non è autorizzata a servirsi del sistema Prüm in detti casi. Ciò, purtroppo, diminuisce notevolmente le probabilità di ritrovare persone scomparse o di identificare resti umani.

Ecco come, talvolta, le differenze contenute in ciascun sistema legale nazionale inibiscono le autorità giudiziarie dalla fruizione del Prüm framework. Pertanto, acconsentire ad un tale cambiamento significherebbe accrescere la quantità di dati e informazioni scambiati tra i vari Stati membri, assicurando al contempo la riservatezza, l'integrità, la disponibilità e la privacy di tali dati.

⁸⁰ La categoria "persone scomparse" (così come altri soggetti presumibilmente deceduti e, quindi, corrispondenti a "corpi umani non identificati") dovrebbe essere aggiunta alle altre categorie già

Lo studio propone anche di adottare il formato standard ANSI/NIST-ITL 1-2011⁸¹ per lo scambio automatizzato di tutte le tipologie di dati in tutti gli Stati membri, i quali a loro volta dovrebbero gradualmente implementare il sistema con le ultime versioni disponibili (quella del 2015 o anche successive)⁸².

Vi è poi da considerare il miglioramento dell'efficienza del meccanismo di inserimento delle impronte digitali⁸³, imponendo requisiti tecnici e standard di qualità che le immagini dovrebbero avere, così da rifiutare l'inserimento di immagini insoddisfacenti.

Per quanto concerne il numero limite di candidati da indicare all'interno delle liste di ricerca, lo studio suggerisce di mantenere tale misura a dieci. Infatti, gli Stati membri concordano sul fatto che ridurre tale numero potrebbe indurre a trascurare potenziali candidati e, quindi, sospettati importanti⁸⁴.

considerate nell'ambito Prüm, in quanto spesso si tratta di soggetti con un passato criminale o sospettati di condotte illecite. Naturalmente, è d'uopo affrontare le seguenti considerazioni: ai sensi della legislazione nazionale, le persone scomparse sono considerate come persone naturali, titolari di diritti e di obblighi. Decorso un certo periodo di tempo fissato dalla legge, tali soggetti vengono considerati deceduti. Inoltre, spesso accade che determinati individui considerati "vulnerabili" (come persone anziane, individui affetti da disturbi psichiatrici o psicologici, bambini ecc.) ricadano nella categoria di "persone scomparse" accanto a profili criminali. In tal caso, risulta necessario predisporre un sistema informatico "rinforzato", in grado di proteggere adeguatamente i dati personali di tali soggetti. Per quanto riguarda le ricerche effettuate sotto la barra "corpi umani non identificati", spetterà allo Stato membro decidere se anche le persone decedute, incluse in tale ricerca, debbano beneficiare di una protezione dei dati estensiva (che ricomprenda il rispetto al diritto dell'immagine personale, la dignità e la reputazione).

⁸¹ Lo standard ANSI-NIST-ITL 1-2011 descrive il formato di file e la qualità richiesti per lo scambio di dati. L'ultima revisione risale al 2015. Lo standard prevede un file conforme, nominato *contenitore NIST*, che contiene un *set* di una o più registrazioni e può inglobare dati relazionati a una o più identità. Il contenitore NIST funziona tramite l'impiego di un codice basato sul linguaggio di programmazione "XML". Tale codice offre diversi benefici, quali: una più facile integrazione con altri sistemi e moderne tecnologie, l'eliminazione della necessità di utilizzare tecnologie esterne per leggere i *files* NIST, il supporto per l'adozione di comunicazioni tramite servizi web, maggior facilità di trasformare file tra differenti standards.

⁸² Tale standard, conformemente alle esigenze contemplate dalle Decisioni Prüm, dovrebbe includere, all'interno di un primo campo nominato "Type-1 Records": l'indicazione della versione dello standard utilizzato; il "IDC registrations", ossia un registro dei record biometrici contenuti nel pacchetto di scambio; il "Transaction control number" (TCN), ossia un identificatore unico che sarà utile anche nella procedura di follow up; le "Originating/destination agencies", ossia un identificatore unico per le forze dell'ordine che inviano e ricevono le richieste e, infine, l'indicazione numerica della priorità della richiesta (che può andare da 1 a 9, dove il numero 1 segnala la massima urgenza). In un secondo campo denominato "Type-2 Record" saranno inclusi specifici elementi, relativi alle informazioni scambiate, utili ad assicurare la compatibilità e la tracciabilità dei risultati in una successiva fase. Tali indicatori sono: l' "IDC", ovvero il riferimento al soggetto a cui si riferisce l'indagine; il numero della pratica; il numero di riferimento del ricercato, se conosciuto e, infine, la lista dei risultati. Dalla prospettiva della riservatezza dei dati ottenuti, preme specificare che gli indicatori contenuti nel Type-1 Records coinvolgono dati che possono direttamente identificare quella specifica trasmissione o ricerca, ma non persone. Ciò si contrappone a quanto può risultare dalla ricerca sotto i campi previsti dal Type-2 Record, in quanto essi possono agevolmente condurre alla precisa identificazione di un soggetto. In ogni caso, essendo la protezione della *privacy* un interesse coperto da un'importanza preminente, sarà necessario prevedere delle misure di controllo molto più restrittive. Ecco che, allora, possono essere adottati i seguenti accorgimenti: memorizzazione dei dati per un periodo di tempo breve oppure utilizzo di pseudonimi o anche anonimizzazione del risultato nel caso in cui dovesse essere conservato nel sistema per periodi più lunghi. A ciò si aggiunge anche la necessità di istruire al meglio gli operatori, di modo che vengano sensibilizzati sulla natura sensibile di determinate informazioni.

⁸³ In Italia, il sistema AFIS è in uso da più di 30 anni e costituisce, per l'autorità giudiziaria che se ne serve, un fondamentale strumento per identificare i criminali sospettati, usando sia le impronte digitali complete (denominate ten-print) sia le immagini di porzioni di impronte latenti.

⁸⁴ La preoccupazione principale manifestata dagli Stati membri è, però, rappresentata dalla quota giornaliera di ricerche e richieste che è consentito inoltrare, in quanto una tale restrizione può inficiare la loro capacità di effettuarne in quantità sufficiente. La soluzione che viene proposta consiste nell'utilizzare un approccio basato sulla priorità. Infatti, per gestire l'ammontare di richieste è opportuno stabilire, di comune accordo, dei livelli di priorità: le richieste di priorità di livello uno (che suggeriscono la sussistenza di crimini seri che richiedono indagini più approfondite) dovranno essere processate entro 12 ore; le istanze di

Un ulteriore aspetto che lo studio vaglia riguarda il perfezionamento della corrispondenza di DNA a partire dalla configurazione di una soglia minima di corrispondenze di *loci*, che dovrebbe essere preferibilmente pari a sei.

Altro profilo di rilevante importanza è quello che riguarda la procedura di follow-up, non disciplinata dalle Decisioni Prüm e, quindi, rimessa alle legislazioni nazionali. Le divergenze tra norme nazionali hanno condotto a inefficienze operative⁸⁵ e il report suggerisce di stabilire una tempistica ragionevole⁸⁶, predisponendo dei sistemi automatici, senza scartare ipotesi di controllo manuale, e impiegando l'unico canale di comunicazione SIENA⁸⁷.

Tra i vari accomodamenti contemplati dal report si annovera anche l'implementazione del formato UMF (*Universal Message Format*)⁸⁸, che ottimizzerebbe le comunicazioni.

Lo studio di Deloitte valuta altresì la possibilità di introdurre nuove categorie di dati, a partire dalle immagini che consentono il riconoscimento facciale. Il report propone di adottare delle linee guida relative alla qualità dell'immagine richiesta, di decidere il formato della lista dei possibili candidati e, infine, di predisporre una pianificazione basata sulla priorità⁸⁹. Tale linea di azione è

livello due sottostanno a una tempistica di 24 ore; mentre quelle di priorità di livello tre dovranno essere processate entro 48 ore.

⁸⁵ Le carenze operative si sono sostanziate, ad esempio: in un'inerzia attuativa, per cui i Paesi membri hanno dovuto attendere diversi mesi prima di ricevere le informazioni di follow-up; nell'utilizzo di diversi canali di comunicazione, fattore che ha condotto all'impiego di evitabili sforzi di coordinazione; nella disarmonia delle informazioni scambiate, dovuta all'indeterminatezza dei dati considerati dai vari Paesi membri.

⁸⁶ Questo step comporta lo scambio, tra i vari Paesi membri, di un gruppo minimo di informazioni relative al rispettivo profilo biometrico (nome e cognome, data e luogo di nascita, sesso, nazionalità, infrazione o reato commesso più recentemente per cui è stato necessario acquisire impronte digitali o DNA, i contatti delle forze dell'ordine responsabili dell'indagine, informazioni aggiuntive come le foto segnaletiche). Dopo che lo Stato membro compulsante riceve tali informazioni potrà sollecitare l'invio di ulteriori dati più dettagliati, dando luogo così alla cosiddetta fase tre.

⁸⁷ Tale strumento consente alle forze dell'ordine di indicare la priorità delle richieste inoltrate (bassa, normale, alta). In aggiunta, potranno essere messi in rilievo nei parametri del "soggetto" o del "contenuto del reato" i criteri "molto urgente" o "urgente". Inoltre, nonostante SIENA non contempli delle regole sui tempi da rispettare, lo Swedish Framework potrà costituire una base per stabilire i limiti di tempo entro cui le forze dell'ordine debbano fornire l'informazione richiesta, segnatamente: otto ore, una settimana, 14 giorni. Tra i vari aspetti vi è da sottolineare che SIENA si dimostra essere uno strumento facile da usare e consente un accesso decentralizzato, adotta un formato standardizzato e dispone di un elevato livello di sicurezza e di confidenzialità. Dall'altro lato, invece, SIENA non prevede un monitoraggio 24/7; aspetto per il quale il canale I-24/7 risulta essere particolarmente all'avanguardia.

⁸⁸ Esso è un formato di dati basato sul linguaggio XML che agisce da strato intermedio tra i vari sistemi o database e viene utilizzato ogni qualvolta vengano inviati messaggi strutturati tra i sistemi delle forze dell'ordine. Il formato in esame consentirebbe agli Stati membri di comunicare senza sforzi traduttivi, che spesso conducono a commettere errori.

⁸⁹ Per far ciò sarà necessario: implementare o aggiornare i sistemi di riconoscimento facciale in uso alle forze dell'ordine nazionali; integrare tali sistemi con l'architettura informatica Prüm; costruire un'interfaccia per ogni utente; formare i futuri utilizzatori del sistema e, infine, stabilire collegamenti tra ogni Stato membro. Il processo di acquisizione di tali immagini si articolerà come segue: un Paese membro confeziona il file della richiesta di cattura di un'immagine facciale. La domanda viene inoltrata ad ogni Stato membro e, così, lo Stato destinatario conduce una ricerca nelle gallerie delle foto segnaletiche. Sempre quest'ultimo invia i risultati della ricerca allo Stato membro compulsante, il quale effettuerà l'aggiudicazione confermando oppure invalidando l'esito e approderà alla fase 2, propendendo per l'utilizzo di soluzioni automatizzate e assicurando una disponibilità 24/7. A loro volta le risposte inviate allo Stato membro richiedente dovranno contenere un numero massimo di candidati fissato a 50 ed essere inoltrate anche se la ricerca non abbia prodotto alcun esito (zero candidati). L'innovazione contenuta in detto sistema consiste, inoltre, nell'indicare informazioni circa l'ordine di posizionamento e il punteggio di corrispondenza di ciascun candidato, nonché nell'attenzione circa eventuali errori verificatisi. Un altro punto da considerare risiede nel procurare uno standard comune ad ogni Stato membro che possa garantire un livello minimo di accuratezza. Un'adesione carente a tali standard potrebbe compromettere l'adeguata acquisizione delle

improntata alla protezione della privacy dei soggetti ivi raffigurati⁹⁰, evitando loro possibili conseguenze negative⁹¹, senza dimenticare che l'aggiunta dei fotogrammi facciali richiederà un maggiore apporto di componenti tecnici e di personale⁹².

Per quanto riguarda, poi, le informazioni relative alle armi da fuoco, gli Stati membri non considerano ancora l'ipotesi di uno scambio di tali dati⁹³. Le banche

immagini e causare una bassa accuratezza, nonché un tasso di errori più elevato. È noto che non tutti gli elementi delle foto segnaletiche standard influenzano la performance durante la fase di riconoscimento facciale automatizzato e, infatti, solo i seguenti devono essere considerati come elementi chiave: risoluzione minima di 90 px (per occhio); posa frontale; rimozione degli accessori (come occhiali, cappelli, foulard ecc.); rapporto 1:1; illuminazione uniforme (è da evitare l'esposizione diretta alla fonte di luce). Chiaramente, la raccolta di tali immagini può essere ulteriormente migliorata pensando, ad esempio, di raggruppare le fotografie in separati archivi sulla base di una divisione logica. Si potrà distinguere, nel "tipo di trasmissione" (TOT), fra foto segnaletiche (di un individuo conosciuto) e wild (riferite a persone non identificate). Il TOT viene impiegato anche nell'ambito delle impronte digitali per indicare se una traccia è qualificabile come ten print oppure come latente.

⁹⁰ Ad esempio, se su una lista di cinquanta risultati ricevuti soltanto uno appare corrispondere all'identità del sospettato, lo Stato membro richiedente si troverà ad avere a disposizione altri 49 fotogrammi relativi a soggetti estranei. Questa problematica potrebbe essere risolta in tre modi: definendo un numero massimo di immagini per ogni richiesta inoltrata. Lo studio suggerisce che cinquanta immagini siano sufficienti se la qualità delle stesse viene mantenuta alta, mentre sarà ammissibile una lista di cento fotografie se si tratta di wild o trace images; stabilendo concordemente che le immagini che non abbiano ottenuto un riscontro vengano eliminate, decorso un determinato periodo di tempo (ad esempio 24 ore); stilando una lista contenente un numero di candidati inferiore, fino a cinquanta.

⁹¹ Per il momento è sufficiente conoscere che l'invio di falsi positivi possa provocare conseguenze negative a persone innocenti coinvolte, ad esempio, in un intervento delle forze dell'ordine a causa di un'errata corrispondenza. Tuttavia, l'utilizzo di tipologie di dati più comuni, come le immagini facciali, limitatamente per scopi investigativi che rientrano nel quadro Prüm, si differenzia dagli altri diversi casi di uso di fotogrammi facciali, come avviene nelle situazioni di identificazione di massa o verifiche durante gli attraversamenti di frontiera. In ogni caso, l'impiego delle immagini facciali potrebbe rendere la ricerca di sospettati più agevole ed efficiente; questo perché lo *stock* di immagini disponibile per le forze dell'ordine è maggiore rispetto a quello delle impronte digitali o del DNA (alcuni criminali, infatti, potrebbero non lasciare impronte, ma essere successivamente inquadrati da una telecamera e così identificati).

⁹² Perciò, come affermato per le impronte digitali, anche in questo caso sarà opportuno definire una quota giornaliera massima di richieste inoltrabili, basandosi su un approccio prioritario. Le richieste di livello di priorità uno (queste dovrebbero costituire il minor numero, essendo dedicate solo ai crimini più efferati) dovranno essere processate entro un'ora; le richieste di livello due dovranno essere elaborate entro 24 ore, mentre quelle di livello tre entro le successive 48 ore. Anche per lo scambio di immagini facciali il *report* invita a adottare lo standard NIST/ANSI-ITL 1:2011 (nella sua versione aggiornata del 2015) in quanto, oltre a consentire l'uniformazione degli standard impiegati, fornisce elevati livelli di interoperabilità con altri sistemi. Le registrazioni relative alle immagini facciali, inoltre, dovranno includere i seguenti campi: *IDC* (il riferimento del soggetto a cui si riferisce l'indagine); tipo di immagine (inserendo "viso"); dimensione; posa del soggetto (frontale, profilo destro o sinistro); numero di riferimento per l'immagine facciale; punteggio sulla qualità dell'immagine. Sarà facoltà degli Stati membri utilizzare anche algoritmi. Non saranno da escludere eventuali errori, ad esempio: invalidità del TCN (transaction control number, ossia il numero identificativo dell'operazione, che viene utilizzato anche nella fase di follow-up), qualità dell'immagine insufficiente, volto non trovato, formato del file non valido, mancanza di un'informazione obbligatoria, sistema non disponibile.

⁹³ Tuttavia, le tecnologie si sono evolute e hanno avuto luogo delle iniziative transnazionali al fine di facilitarne la trasmissione. Per quanto riguarda la balistica, lo studio in oggetto suggeriva agli Stati membri di creare un sistema di identificazione balistico che consentisse di acquisire le prove ottenute, di creare un profilo dei segni presenti sul proiettile o sulla cartuccia e di compararlo con altri profili per poter estrarre una corrispondenza. Gli odierni sistemi di identificazione garantiscono un elevato livello di accuratezza nelle corrispondenze. Inoltre, i Paesi Nordici e la Penisola Iberica stanno già sperimentando meccanismi automatizzati di comparazione e di correlazione fra proiettili e cartucce. Ciononostante, vi sono diversi sistemi di identificazione balistica, utilizzati dai vari Stati Membri, che non sono interoperabili. In Europa, la maggior parte dei Paesi membri ha implementato uno dei tre sistemi qui elencati: IBIS (Integrated Ballistic Identification System): è il più utilizzato. Esso consente di effettuare ricerche mirate e contemporaneamente realizza una comparazione automatica tra tutti i profili registrati nel sistema non appena quello specifico profilo viene acquisito. È l'unico strumento che consente di svolgere tale ultima azione. Per questo motivo, IBIS è utilizzato da Interpol, all'interno di IBIN (Interpol Ballistic Information Network), un database balistico

dati nazionali contengono, per ovvie ragioni, registrazioni qualitativamente adeguate di armi da fuoco legali, mentre le raccolte di dati relativi ad armi clandestine, bossoli e proiettili soffrono ancora di gravi criticità⁹⁴.

Infine, per quanto riguarda i dati biografici, nel 2017 cinque Stati membri (Francia, Finlandia, Germania, Irlanda e Spagna) hanno lanciato un progetto pilota chiamato "Automatizzazione del processo di scambio di dati - Sistema di registrazione delle informazioni della Polizia Europea" (ADEP-EPRIS), fondato dalla Commissione Europea, con lo scopo di automatizzare i processi manuali di identificazione, al fine di consentire e facilitare il conseguente scambio bilaterale o multilaterale di informazioni⁹⁵.

3.4 L'architettura informatica e le soluzioni interoperabili per lo scambio di dati biometrici.

Per quanto riguarda il disegno strutturale informatico, le attuali Decisioni Prüm specificano che gli Stati membri sono tenuti ad utilizzare un network denominato TESTA per lo scambio elettronico di dati genetici, dattiloscopici e VRD (dall'inglese *Vehicle Registration Data*).

Nello studio Deloitte si riferisce che l'attuale architettura informatica presenta alcune lacune, a partire dall'assenza di un sistema centralizzato che

con cui i Paesi membri possono comparare le immagini dei dati balistici attraverso il loro corrispondente IBIS. Tra i Paesi che utilizzano questo sistema figura anche l'Italia; EVOFINDER: è un sistema di identificazione balistica basato su un network. Significa che ogni Paese possiede un server nazionale che consente l'immagazzinamento, la comparazione di dati balistici e l'identificazione, così come l'accesso a tutti i servizi dei laboratori degli altri Paesi collegati. Questo sistema non ammette la ricerca automatica di profili, ma tale funzionalità è in corso di sviluppo. Ciò consente per ora soltanto un approccio reattivo (e non proattivo); ARSENAL: è un sistema di identificazione balistica ideato per costituire parte di un network. Similmente a Evofinder, il sistema consente solo di svolgere una ricerca mirata e, ugualmente, è in fase di elaborazione una soluzione automatizzata.

Per quanto attiene, invece, alle armi da fuoco, quelle legali dovrebbero essere registrate nel database di ciascuno Stato, stante l'obbligatorietà di un'autorizzazione per il loro uso e possesso. I dati che vengono registrati possono variare di paese in paese, ma possono esserne definiti alcuni imprescindibili, in ottemperanza alla Direttiva 91/477/EEC sulle armi da fuoco: il numero seriale dell'arma, il tipo, la marca, il calibro, il modello, il nome e la sede del fornitore, il numero seriale del fornitore e l'anno di produzione. Gli Stati membri possono ricercare informazioni relative ad armi da fuoco attraverso i seguenti sistemi: iARMS (Illicit Arms Records and tracing Management System), che è un database di armi da fuoco fondato dall'Unione Europea e gestito da Interpol, in cui gli operatori possono controllare se determinate armi sono state registrate come "smarrite", "rubate", "trafficate", "contrabbandate"; EIS: il sistema di informazioni di Europol contiene dati riguardanti persone e oggetti ricollegati a crimini e terrorismo; SIS II: alcune autorità di polizia utilizzano il "sistema di informazione Schengen di seconda generazione" per immagazzinare e ricercare dati circa armi da fuoco collegate alla commissione di crimini, sequestrate e ricercate.

Ciò premesso, tuttavia, il report non avalla l'inclusione, all'interno dell'ambito Prüm, di dati relativi alle armi da fuoco in quanto i database nazionali contengono, per ovvie ragioni, registrazioni di armi da fuoco legali. Se gli investigatori non sono in possesso di quella specifica arma, non sono in grado di avviare l'iter di tracciamento e, se volessero ricercare il possessore di un'arma che hanno sequestrato, potrebbero direttamente contattare il venditore e ottenere le informazioni richieste.

⁹⁴ A ciò si aggiungano motivazioni più tecniche: il formato di alcuni dati considerati nello scambio (ad esempio il tipo, la marca e il modello) può variare tra i venditori e, peraltro, alcuni di essi utilizzano il medesimo numero seriale per diverse armi da fuoco, creando così una barriera all'armonizzazione in materia. Tale scarsa accuratezza potrebbe generare dei falsi positivi che, di conseguenza, potrebbero sollevare problematiche connesse alla protezione dei dati. Per questo motivo, gli Stati membri stanno considerando l'ipotesi di utilizzare European Search Portal (ESP) come canale di default per cercare e scambiare dati relativi ad armi da fuoco.

⁹⁵ Si allude a diversi dati, quali, ad esempio: nome, cognome, soprannome o alias, data e luogo di nascita, genere.

possa processare le richieste fino alla mancanza di soluzioni interoperative e si individuano possibili soluzioni⁹⁶. Innanzitutto, per motivi di sicurezza e di privacy, i dati personali non crittografati non dovrebbero essere immagazzinati a livello centrale⁹⁷. In secondo luogo, il *network* TESTA dovrebbe rimanere lo standard di comunicazione sicuro. Gli Stati membri dovrebbero, inoltre, considerare la possibilità di modificare l'architettura introducendo un *router* centrale, a cui gli Stati membri possono collegarsi tramite un'unica connessione, attraverso cui inviare richieste e ricevere riscontri (sistema "a stella" o *hub-and-spoke*). Se, dunque, la topologia dovesse passare da un'architettura a rete a una a stella, il numero delle connessioni necessarie verrà drasticamente diminuito. Ai dati scambiati tramite il router centrale si può applicare un modello di crittografia su più livelli per assicurare che solo le informazioni rilevanti per ogni siano accessibili⁹⁸.

Nel maggio 2019 il Parlamento e il Consiglio Europeo hanno adottato i regolamenti n. 2019/817 e 2019/818, stabilendo un quadro per garantire l'interoperabilità⁹⁹ tra i vari sistemi d'informazione europei. L'obiettivo era quello di assicurare che le forze dell'ordine avessero un accesso sistematico ed efficace alle informazioni necessarie ai loro compiti istituzionali.

Una condivisione di dati migliore può aumentare il grado di sicurezza in Europa, consentendo controlli più efficaci dei migranti illegali¹⁰⁰. Lo studio di Deloitte prevede anche la possibilità di coinvolgere anche gli organismi Europol, Interpol e i Paesi terzi¹⁰¹.

⁹⁶ Potranno essere apportati i seguenti miglioramenti: facilità e costi minimi nell'implementazione del sistema di scambio; accesso centralizzato e una registrazione delle statistiche; monitoraggio sui tempi di funzionamento del sistema (con indicazione di eventuali tempi di inattività); protocollo di integrazione ammodernato che permetta un'implementazione rapida e consistente dei sistemi utilizzati dai Paesi membri.

⁹⁷ Lo studio in esame suggerisce, infatti, di immagazzinare a livello centrale soltanto i dati non direttamente identificativi dei soggetti (quali, ad esempio, il tipo di richiesta, il Paese membro richiedente, il Paese membro destinatario ecc.). I dati biometrici, dunque, sono protetti da un processo di crittografia multilivello a cui il router centrale non è in grado di accedere.

⁹⁸ Il sistema di sicurezza pensato per il router consiste in: un trasporto di sicurezza (SSL fornisce un elevato livello di crittografia delle richieste mentre sono in transito e ciò avviene in aggiunta alla trasmissione tramite il network sicuro TESTA); messaggi crittografati (l'intero messaggio è criptato tramite l'impiego di una password conosciuta solo dagli Stati Membri e dal router centrale; quest'ultimo la usa per decriptare l'intestazione del messaggio); carico utile o payload crittografato (in cui il testo effettivo del messaggio è protetto da un codice conosciuto solo dallo Stato richiedente e ricevente). Si tratta di un approccio stratificato chiave, poiché assicura la non identificabilità dei dati immagazzinati o visibili a livello centrale.

⁹⁹ I sistemi usano lo stesso formato di dati, gli stessi standard e soluzioni interoperabili all'interno del quadro Prüm. Gli Stati membri possono, quindi, ricorrere al medesimo formato di dati per interrogare i sistemi Prüm e le soluzioni interoperabili.

¹⁰⁰ Ciò verrà sviluppato tramite: un canale di ricerca Europeo (c.d. ESP), un servizio di corrispondenze biometriche condiviso (c.d. sBMS), un magazzino di dati biografici e biometrici (c.d. CIR) e un rilevatore di identità multiple.

Su sei dei maggiori sistemi d'informazione europei che saranno resi interoperativi tramite l'uso di componenti centrali, cinque registrano informazioni biometriche, impronte digitali e immagini facciali. Si stima che circa 300 milioni di persone verranno registrate nel Common Identity Repository (CIR), il quale conterrà sia dati biografici che biometrici.

¹⁰¹ La connessione con questi ultimi dovrebbe avvenire nella modalità così descritta: Europol, Interpol e i Paesi Terzi dovranno avere le medesime capacità tecniche dei Paesi membri (ad esempio, mettere a disposizione il proprio database affinché gli Stati membri possano interrogarlo e viceversa, ricevere un responso hit/no-hit ecc.). Nonostante i database di Europol siano relativamente esigui rispetto a quelli dei Paesi membri, questi ultimi potranno comunque trarre beneficio da una loro consultazione, in quanto essi contengono informazioni provenienti anche da Paesi terzi, che attualmente non sono accessibili nel contesto Prüm. In riferimento a Interpol, vale la medesima considerazione. L'inclusione di Paesi terzi amplierà anch'essa il numero dei database connessi. Ciò consentirà di svolgere ricerche su larga scala e, come

Vale, infine, indicare che in data 13 marzo 2024 veniva siglato il Regolamento Prüm II¹⁰², il quale accoglie con favore le proposte e le valutazioni offerte dallo studio analizzato poc'anzi e, infatti, prevede: la creazione di *router* centrali, lo scambio automatizzato dei dati complementari delle immagini facciali e degli estratti dei casellari giudiziali, la collaborazione di Europol, la revisione del processo di follow-up a seguito di riscontro positivo e via dicendo.

4. Discussione e conclusioni.

Le banche dati utilizzate dalle forze di polizia, nelle quali sono registrati dati biometrici, pongono una sfida al diritto alla protezione dei dati personali, riconosciuto a partire dalla Carta dei diritti fondamentali dell'UE.

Il Garante europeo per la protezione dei dati ha evidenziato le potenziali criticità in materia di circolazione e scambio dei dati dovute a una normativa generica e non armonizzata nel 2007 e la Corte di Giustizia dell'UE (CGUE) si è già espressa nel 2023 circa la violazione della *privacy* in relazione alla registrazione «sistematica» dei dati biometrici e genetici di soggetti accusati di un reato e alla possibilità di ottenere coattivamente dati di persone indagate per un reato doloso procedibile d'ufficio.

Il *database* EURODAC, dove sono archiviate le impronte digitali dei richiedenti asilo e degli immigrati irregolari che varcano i confini di un Paese europeo è stato istituito dal Regolamento CE n. 2725/2000 e realizzato preoccupandosi di assicurare la giusta protezione dei dati a carattere personale sin dal suo regolamento istitutivo, che prevedeva di non inserire le informazioni relative al nome e alla nazionalità dei soggetti, al fine di escludere i possibili abusi.

Un accorgimento che risulta dal bilanciamento tra necessità di sicurezza e diritto alla protezione dei dati personali, compresi quelli biometrici, è la fissazione di periodi di conservazione differenziati. Per il richiedente asilo la documentazione è conservata per dieci anni, salvo che ottenga la cittadinanza di uno degli Stati membri (in tal caso, gli elementi che lo riguardano devono essere cancellati non appena ottenuto il titolo). Per gli individui stranieri fermati in occasione dell'attraversamento irregolare di una frontiera esterna i dati sono conservati fino a un massimo di due anni a decorrere dalla data di acquisizione dei rilievi dattiloscopici. Essi vengono infatti cancellati prima dello scadere dei due anni se viene rilasciato un permesso di soggiorno, la cittadinanza, o se egli ha lasciato il territorio degli Stati membri.

per Europol e Interpol, se nuovi Paesi si aggiungono al network Prüm, dovranno essere assegnate risorse umane aggiuntive per poter gestire le richieste. Da un punto di vista tecnico, l'inclusione di Europol e di Interpol richiede che i loro database vengano collegati alla rete Prüm, o tramite la topologia a stella o con quella a rete. Inoltre, al fine di evitare la duplicazione dei medesimi dati, provenienti sia dai Paesi membri sia da Europol o Interpol, soltanto i dati di queste due agenzie Europee che provengono da Paesi Terzi devono essere resi fruibili. La procedura di connessione dei diversi database prevede che questi vengano prima di tutto configurati, per poi connetterli al network Prüm.

¹⁰² Regolamento (UE) 2024/982 del Parlamento europeo e del Consiglio, del 13 marzo 2024, sulla consultazione e lo scambio automatizzati di dati per la cooperazione di polizia e che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio (Regolamento Prüm II), consultabile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202400982. Ultima consultazione il 4 ottobre 2025.

Particolari garanzie di rispetto delle norme dell'ordinamento europeo devono poi essere fornite dagli Stati membri relativamente al prelievo, utilizzo, trasmissione, conservazione o cancellazione dei dati attinenti alle impronte digitali.

Per quanto riguarda la trasmissione dei dati, questi ultimi potranno essere consultati soltanto dallo Stato membro che ne ha chiesto l'invio e per gli scopi espressamente previsti da EURODAC, che ne garantisce esattezza e attualità al momento della trasmissione.

A partire dal 2005, in seguito al trattato di Prüm, ci si è resi conto che diversi paesi europei utilizzavano criteri diversi, in base ai quali registrare i profili nelle banche dati. Inserire individui anche solo sospettati di aver commesso un crimine e poi assolti è una scelta pro-securitaria, inaccettabile in paesi più attenti alla protezione dei dati personali e al diritto alla riservatezza, che registrano solo i profili di individui condannati per gravi reati.

Esempi di bilanciamento tra i suddetti diritti sono il numero limite di candidati da indicare all'interno delle liste di ricerca e la soglia minima di corrispondenze di *loci*. Il Regolamento Prüm II, sottoscritto nel 2024, ha stabilito che siano forniti 10 candidati, sulla base di una corrispondenza di almeno sei *loci*.

Nel caso dei campioni biologici è necessario considerarne la duplice valenza, da un punto di vista giuridico, in quanto materiali ed in quanto informazioni. Il materiale biologico, infatti, è costituito da una parte fisica e da un corollario di informazioni che rappresentano il grado di "conoscenza" che si ha su tale campione. Nell'ambito delle banche dati forensi il diritto all'autodeterminazione cede di fronte alle esigenze di natura pubblicistica legate al perseguimento dei reati e il prelievo del campione biologico può avvenire su base coattiva, ovvero contro la volontà del soggetto da cui esso proviene. Anche i criteri per ottenere un prelievo coattivo e i tempi di conservazione del campione sono frutto di un bilanciamento tra diritti contrapposti, sulla base del contenuto di informazioni nel campione biologico, che va ben oltre i *loci* utilizzati per l'identificazione personale.

Le Decisioni di Prüm non hanno definito i profili dei soggetti che devono essere inclusi nel database nazionali, né per quanto tempo tali profili debbano essere conservati, oltre a non specificare se i campioni di DNA debbano essere conservati o meno¹⁰³, generando criticità nello scambio di dati personali legati ai profili di DNA¹⁰⁴. Tale mancanza di uniformità comporta che solo in un limitato numero di casi l'accesso al database nazionale di un altro Stato membro consente di identificare il soggetto cui appartiene il campione biologico ed eventualmente instaurare un procedimento penale nei suoi confronti¹⁰⁵.

¹⁰³ B. PRAINSACK, V. TOOM, *Performing the Union: The Prüm Decision and the European dream*, *Studies in History and Philosophy of Science Part C Studies in History and Philosophy of Biological and Biomedical Sciences*, 2013, p. 44.

¹⁰⁴ F. SANTOS, H. MACHADO, *Patterns of exchange of forensic DNA data in the European Union through the Prüm system*, in *Science & Justice*, 2017, fasc. 57, pp. 307–313.

¹⁰⁵ A tal proposito si veda lo studio commissionato dalla Commissione per gli affari costituzionali (AFCO) del Parlamento europeo: V. Toom, *Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision STUDY*, 2018.

È stato il Regolamento attuativo D.P.R. n. 87 del 2016 che ha precisato i criteri di inserimento dei profili del DNA nella Banca dati, distinguendo l'attività di consultazione, cui sono dedicate specifiche norme volte a definire determinate cautele, limitando i tempi di conservazione dei profili di DNA ottenuti dalle persone soggette a restrizione della libertà personale nonché la distruzione dei relativi campioni biologici, abbreviandoli rispetto alle previsioni della Legge del 2009.

L'utilizzo dei dati biometrici deve sempre rispettare la disciplina in materia di trattamento dei dati personali e, in particolare, la Direttiva (UE) 2016/680, cui è stata data attuazione in Italia con il D.lgs. 18 maggio 2018, n. 51.

Tale decreto attuativo è stato criticato poiché non giustifica un'applicazione circoscritta delle restrizioni e non le correda da specifiche garanzie poste a tutela dell'interessato che vede limitati i suoi diritti¹⁰⁶.

Come correttamente osservato successivamente «nello scrutinare la *quality of law* che legittima il trattamento, si esigono precetti normativi chiari e dettagliati idonei a orientare il potere di gestire dati biometrici e genetici altrui entro argini prestabiliti e, al contempo, a garantire ai singoli di conoscere, con sufficiente margine di certezza, i casi e i modi entro i quali sono ammesse compressioni dei propri diritti, permettendo così di censurare eventuali interferenze indebite»¹⁰⁷.

Così può essere sintetizzata la conclusione cui è pervenuta recentemente la C.G.U.E., Grande Sezione, con la sentenza del 30 gennaio 2024, N.G., Causa C-118/22¹⁰⁸; intervento giurisprudenziale di significativa importanza, che deve costituire il faro di ogni legislazione nazionale in tema di trattamento dei dati personali.

Lo studio dell'evoluzione delle norme sulle banche dati di polizia rappresenta dunque un buon esempio di quanto sia indispensabile un continuo confronto esauriente tra tutte le parti coinvolte per consentire di trovare un equilibrio tra i diritti in gioco, equilibrio necessario a cogliere le opportunità delle nuove tecnologie come strumento di maggiore sicurezza dei cittadini da utilizzare sempre nel rispetto dei loro diritti fondamentali.

¹⁰⁶ A. RICCI, *Il trattamento di dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati. riflessioni sul d.lgs. 18 maggio 2018, n. 51, di attuazione della dir. 2016/680/UE*, in *Nuove Leggi Civ. Comm.*, 2019, p. 565 ss., spec. p. 574.

¹⁰⁷ L. BELVINI, *Questioni aperte. Conservazione di dati biometrici e genetici*, in *Archivio Penale*, 2024, fasc. 1, p. 11.

¹⁰⁸ «Contrasta con il diritto dell'Unione una normativa nazionale che prevede la conservazione da parte delle autorità di polizia a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, di dati personali, in particolare di dati biometrici e genetici, riguardanti persone che hanno subito una condanna penale definitiva per un reato doloso perseguibile d'ufficio, fino al decesso della persona interessata, anche in caso di riabilitazione di quest'ultima, senza porre a carico del titolare del trattamento l'obbligo di esaminare periodicamente se tale conservazione sia ancora necessaria, né riconoscere a detta persona il diritto di cancellazione di tali dati, dal momento che la loro conservazione non è più necessaria rispetto alle finalità per le quali sono stati trattati o, eventualmente, il diritto alla limitazione del loro trattamento».