NOVITÀ SOVRANAZIONALI
SUPRANATIONAL NEWS

di *Lucio Camaldo*

NUOVI STRUMENTI PER AMPLIARE E MIGLIORARE LA COOPERAZIONE INFORMATIVA NELL'UNIONE EUROPEA

Sono stati recentemente approvati dalle istituzioni europee tre nuovi regolamenti, pubblicati in stretta successione tra di loro, volti a rafforzare e completare il sistema di gestione e scambio di dati o informazioni (c.d. "cooperazione informativa") tra paesi appartenenti all'Unione europea. In particolare, il regolamento 2019/816 istituisce un nuovo strumento centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi; mentre i due regolamenti "gemelli" 2019/817 e 2019/818 prevedono moderni meccanismi per garantire l'interoperabilità (ossia l'interazione reciproca) tra i sistemi di informazione dell'UE, rispettivamente, nel settore delle frontiere e dei visti, e in quello della cooperazione di polizia e giudiziaria, asilo e migrazione.

Il regolamento (UE) 2019/816: il nuovo sistema relativo alle informazioni sulle condanne pronunciate nei confronti di cittadini di paesi terzi e apolidi (ECRIS-TCN).

Il primo (e il più rilevante) atto normativo della triade è il regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio del 17 aprile 2019 (in G.U.U.E., 22 maggio 2019, L 135/1), riguardante l'istituzione di un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (denominato ECRIS-TCN), nonché l'integrazione del già esistente sistema (ECRIS), con la finalità di favorire e intensificare lo scambio di informazioni relative ai precedenti penali di soggetti condannati in uno o più Stati membri dell'Unione europea.

Il regolamento, ai sensi dell'art. 41, entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea, ma spetta alla Commissione, a norma dell'art. 35, fissare la data di avvio dell'inserimento dei dati nel sistema ECRIS-TCN da parte di ciascuno Stato membro, che coinciderà, dunque, con l'effettiva entrata in funzione del nuovo meccanismo centralizzato.

Invero, la circolazione, a livello sovranazionale, delle informazioni estratte dal casellario giudiziale trova già una compiuta disciplina all'interno delle decisioni quadro 2009/315/GAI e 2009/316/GAI, quest'ultima istitutiva di ECRIS, definito «un sistema informatico decentrato basato sulle banche dati dei casellari giudiziali di ciascuno Stato membro» (sul tema, v. G. Di Paolo, *Il riconoscimento degli effetti della condanna straniera e lo scambio di dati*, in F. Ruggieri (a cura di), *Processo penale e regole europee: atti, diritti, soggetti e decisioni*, Torino, Giappichelli, 2017, p. 211 ss.).

Tale sistema consente agli Stati membri interessati di acquisire informazioni anche sulle condanne pronunciate nei confronti di cittadini di paesi terzi, senza però delineare un'apposita procedura in grado di agevolare le competenti autorità nella raccolta di dette informazioni (considerando n. 4). Se, infatti, in relazione ai cittadini "europei", la decisione quadro 2009/315/GAI attribuisce agli Stati membri specifici obblighi di comunicazione e trasmissione reciproca dei provvedimenti di condanna pronunciati sul proprio territorio nei confronti dei rispettivi cittadini, diversamente le informazioni concernenti i cittadini di paesi terzi sono conservate esclusivamente nei casellari nazionali degli Stati membri di condanna. Ne deriva, pertanto, che lo Stato richiedente, interessato a ricevere un quadro completo sui trascorsi penali di un determinato soggetto, è tenuto a rivolgersi a tutti gli altri Stati membri (si parla, a tal proposito, di richieste c.d. "generalizzate").

È dunque evidente che una siffatta procedura, peraltro estremamente complessa e onerosa per le parti coinvolte, rappresenti un significativo ostacolo alla proficua cooperazione tra i vari Stati e comporti altresì il rischio di diffusione di informazioni incomplete e insufficienti (considerando n. 6).

Da qui sorge, pertanto, l'esigenza – per la verità già avvertita nel programma di Stoccolma in materia di libertà, sicurezza e giustizia e nel relativo Piano di azione adottato dalla Commissione nel 2010 – di creare un sistema che favorisca «uno scambio rapido ed efficace di informazioni esatte estratte dal casellario giudiziale relative ai cittadini di paesi terzi» (considerando n. 41).

Nel perseguimento di tale obiettivo, il regolamento traccia anzitutto i propri confini operativi, precisando che le norme dell'articolato si applicano al trattamento delle informazioni relative sia ai cittadini di paesi terzi, inclusi apolidi e persone di ignota cittadinanza, condannati da una giurisdizione penale dell'Unione, sia ai cittadini dell'Unione europea in possesso anche della cittadinanza di un paese terzo, che abbiano riportato una condanna negli Stati membri (art. 2).

L'estensione dell'ambito di applicazione del regolamento anche a quest'ultima categoria di soggetti pare del tutto coerente con l'intento di raggiungere il più elevato livello di completezza possibile delle informazioni destinate a circolare nello spazio europeo.

Deve, tuttavia, osservarsi che l'inserimento dei dati in ECRIS-TCN è funzionale esclusivamente all'individuazione degli Stati membri in possesso di informazioni sul casellario giudiziale dei soggetti poc'anzi indicati, in ossequio al principio di proporzionalità, che, come noto, si impone quale canone d'azione dell'Unione europea (art. 5 TUE). Per conoscere, nello specifico, i precedenti giudiziari di una determinata persona, l'autorità competente dovrà, in ogni caso, utilizzare il sistema ECRIS, allo scopo di ottenere tali informazioni dallo Stato membro che le possiede.

Dopo alcune disposizioni di carattere definitorio (artt. 3-4) – tra le quali spicca per rilevanza quella che fornisce la nozione di «condanna», intesa quale «decisione definitiva di una giurisdizione penale nei confronti di una persona fisica in relazione a un reato, nella misura in cui tale decisione sia riportata nel casellario giudiziale dello Stato membro di condanna» (art. 3 n. 1) – sono illustrate nel dettaglio le informazioni oggetto di inserimento nel *software* di interfaccia (ECRIS-TCN), tramite richiesta da compilarsi in conformità dell'apposito formulario *standard* allegato al regolamento.

Più nel dettaglio, l'art. 5 prevede, in primo luogo, la registrazione dei dati alfanumerici, operando una distinzione tra «informazioni obbligatorie» (da includere necessariamente, salvo che siano sconosciute allo Stato membro di condanna), «informazioni facoltative» (da iscrivere se inserite nel casellario giudiziale nazionale) e «informazioni supplementari» (da trasmettere se sono a disposizione dell'autorità centrale).

In sintesi, è opportuno segnalare che all'interno della prima categoria (informazioni obbligatorie) rientrano quelle relative all'identificazione del soggetto condannato (nome e cognome, data e luogo di nascita, cittadinanza, sesso, eventuali nomi precedenti), nonché il codice dello Stato membro che ha pronunciato la condanna; al secondo gruppo (informazioni facoltative) appartengono quelle concernenti i nomi dei genitori della persona condannata. Le informazioni supplementari includono, invece, il numero di identità, o tipo e numero del documento di identificazione dell'interessato, la denominazione dell'autorità di rilascio, nonché gli eventuali pseudonimi o *alias* posseduti dalla persona oggetto di richiesta.

All'interno dei registri informatici, che gli Stati membri sono tenuti a creare «automaticamente e senza ingiustificato ritardo dopo l'iscrizione della condanna nel casellario giudiziale» (art. 5 § 4), dovrebbero collocarsi anche i dati relativi alle impronte digitali, rilevati conformemente al diritto nazionale nel corso di procedimenti penali ovvero in base a criteri minimi (se il cittadino di paese terzo è stato condannato a una pena detentiva di almeno sei mesi o per un reato punibile con una pena detentiva della durata massima di almeno sei mesi), nonché le immagini del volto del soggetto da identificare (art. 6).

Con particolare riguardo all'inserimento nel sistema centrale delle immagini digitalizzate del volto, il regolamento stabilisce che queste possano essere utilizzate, in un primo momento, unicamente per confermare l'identità del cittadino di un paese terzo, non escludendo la possibilità, in futuro, di ricorrere ai dati biometrici, quale metodo specifico per identificare cittadini sprovvisti di documenti o di altro mezzo idoneo alla identificazione (considerando n. 25). La decisione di integrare le disposizioni concernenti l'uso delle immagini del volto viene rimessa alla valutazione della Commissione, la quale, in sede di adozione degli atti delegati, dovrà tener conto della concreta disponibilità degli strumenti tecnici e degli sviluppi tecnologici nel settore del *software* di riconoscimento facciale (art. 6 § 2).

Il regolamento si occupa poi di disciplinare le condizioni di utilizzo di ECRIS-TCN, non solo da parte delle autorità centrali designate da ciascuno Stato membro, ma anche da parte dell'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust), disciplinata dal regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio, dell'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), istituita dal regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, e dell'Ufficio del pubblico ministero europeo (EPPO), istituito dal regolamento (UE) 2017/1939 del Consiglio (art. 7). Le agenzie dell'UE possono, infatti, accedere al sistema centralizzato e, in caso di riscontro positivo, contattano le autorità nazionali degli Stati membri che risultino in possesso delle informazioni sui casellari giudiziali da loro richieste (art. 14 § 4). Inoltre, l'art. 17 prevede che Eurojust abbia accesso diretto al registro europeo, al fine di agire da punto di contatto tra paesi terzi ed organizzazioni internazionali.

Pur essendo i suddetti organismi sovranazionali di cooperazione giudiziaria e investigativa legittimati a interrogare il *software* di interfaccia, al pari delle autorità centrali, è tuttavia loro preclusa la possibilità di inserire, rettificare o cancellare i dati ivi contenuti. Ai sensi dell'art. 9, l'introduzione, la modifica o cancellazione dei dati registrati è infatti di esclusiva competenza degli Stati membri.

A tal proposito, si richiede che ad ogni correzione delle informazioni nei casellari giudiziali nazionali ne corrisponda un'altra di identico contenuto a livello centralizzato.

La circostanza che le vicende del casellario europeo seguano le sorti di quello nazionale si evince anche dall'art. 8, ove si stabilisce che ciascuna registrazione permanga nel sistema centrale, finché risulti iscritta nel casellario giudiziale "interno", con automatica cancellazione alla scadenza del periodo di conservazione.

In caso di presunta inesattezza o illiceità dei dati inseriti, lo Stato membro che ha provveduto alla loro registrazione è tenuto ad avviare immediatamente una procedura volta a verificare l'esattezza o la liceità dei dati in questione ovvero, se necessario, provvedere alla rettifica o cancellazione dei medesimi senza ingiustificato ritardo (art. 9 § 3).

Per ciò che attiene alle finalità dell'utilizzo di ECRIS-TCN, si è già anticipato che l'interrogazione del sistema assolve principalmente alla funzione di individuazione degli Stati membri in possesso di informazioni sui precedenti penali di cittadini di Stati terzi, ma può servire anche per ulteriori fini specifici, espressamente elencati all'art. 7, tra cui: permettere a una persona, su sua richiesta, di verificare il proprio casellario giudiziale; rilasciare nulla osta di sicurezza; ottenere una licenza o un permesso; effettuare indagini di sicurezza a fini occupazionali; effettuare indagini di sicurezza in vista di attività di volontariato, che prevedono contatti diretti e regolari con minori o persone vulnerabili; espletare procedure in materia di visti, acquisizione della cittadinanza e migrazione, comprese quelle di asilo; effettuare controlli in relazione ad appalti pubblici e concorsi pubblici.

In tali ipotesi, l'autorità responsabile della conduzione del procedimento penale può, tuttavia, esprimersi nel senso della non adeguatezza dell'uso di ECRIS-TCN rispetto alle circostanze del caso concreto (art. 7 § 2). Ciò accade, ad esempio, qualora si tratti della richiesta di informazioni relative a reati e violazioni di minore gravità, specialmente in materia di circolazione stradale o di ordine pubblico (considerando n. 18).

Diversamente, si ritiene che debba farsi sempre ricorso al sistema centrale nel caso in cui la richiesta provenga direttamente dalla persona interessata o quando è presentata per ottenere informazioni sui casellari giudiziali conformemente alla Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, in tema di abuso e sfruttamento sessuale dei minori e pornografia minorile (considerando n. 20).

Il regolamento contempla, invero, la possibilità per gli Stati membri di fare uso di ECRIS-TCN anche per fini diversi da quelli poc'anzi richiamati (art. 7 § 1), purché tali fini ed eventuali modifiche siano notificati alla Commissione, in vista della successiva pubblicazione sulla Gazzetta ufficiale dell'Unione europea, entro trenta giorni della ricezione della notifica, a garanzia di una maggior trasparenza delle modalità di utilizzo del sistema centralizzato.

Sotto un profilo meramente tecnico, l'art. 11 individua, quale responsabile della definizione della progettazione fisica, dello sviluppo e dell'attuazione di ECRIS-TCN, l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), le cui attribuzioni sono disciplinate dal regolamento (UE) 2018/1726 del 14 novembre 2018, in parte modificato dall'atto normativo in esame (art. 40). A tale scopo, il Consiglio di amministrazione di eu-

LISA istituisce un consiglio di gestione del programma composto di dieci membri, dotati di competenze specifiche (art. 11 § 5).

Oltre alle funzioni strettamente connesse alla fase di progettazione e sviluppo del sistema centrale, eu-LISA viene investita altresì del compito di monitorare e valutare il funzionamento tecnico di ECRIS-TCN, nonché di presentare relazioni al Parlamento europeo, al Consiglio e alla Commissione (art. 36). Inoltre, è previsto che l'agenzia effettui controlli periodici di qualità sui dati conservati nel sistema e riferisca i relativi risultati agli Stati membri (art. 11 § 13).

Alcune disposizioni sono riservate alla ripartizione di responsabilità tra gli Stati membri (art. 12), Eurojust, Europol, EPPO (art. 16) ed eu-LISA (art. 19), per ciò che concerne la gestione e le modalità di accesso a ECRIS-TCN, nonché l'adozione di adeguate misure che consentano la protezione e la sicurezza dei dati inseriti nella piattaforma digitale. In tema di responsabilità, occorre soffermarsi, in particolare, sulla norma di cui all'art. 20, che attribuisce alle persone interessate e agli Stati membri il diritto di chiedere il risarcimento del danno – materiale o non materiale – derivante dal trattamento illecito di dati o da qualsiasi atto adottato in violazione del regolamento in analisi. Al tal riguardo, l'azione risarcitoria può essere promossa contro lo Stato membro responsabile ovvero contro eu-LISA, nel caso in cui questa non abbia adempiuto agli obblighi prescritti dal regolamento.

Un'ampia parte del regolamento (artt. 23-31) è dedicata alla disciplina della protezione dei dati personali, dove si ribadisce che il trattamento dei dati inseriti nel sistema centrale avviene al solo fine di individuare gli Stati membri in possesso di informazioni sui casellari giudiziali relativi a cittadini di paesi terzi e si sottolinea che l'accesso a ECRIS-TCN è riservato unicamente al personale debitamente autorizzato dalle autorità centrali (art. 24).

Una specifica disciplina è poi dettata a tutela dei diritti dei cittadini di paesi terzi, ai quali è riconosciuta la facoltà di avanzare, direttamente all'autorità centrale di ogni Stato membro, richieste relative all'accesso ai dati personali, alla modifica o cancellazione degli stessi, nonché al diritto di ottenere una limitazione del trattamento (art. 25).

Il rispetto e l'effettiva attuazione di tali diritti sono garantiti dallo svolgimento di attività di cooperazione e coordinamento, non solo tra le autorità centrali competenti, ma anche e soprattutto tra le autorità nazionali di controllo e il Garante europeo della protezione dei dati (artt. 26-30). Un ulteriore strumento di tutela, attivabile in caso di lesione dei diritti di cui all'art. 25, è rappresentato dalla possibilità di presentare un reclamo o di instaurare un giudizio nello Stato membro di condanna, al fine di ottenere l'accesso ovvero la modifica o cancellazione dei dati che riguardano la persona interessata (art. 27).

L'ultimo capitolo del regolamento contiene alcune disposizioni finali, tra cui quelle relative: alle spese da sostenere per l'istituzione e il funzionamento di ECRIS-TCN (art. 33); all'entrata in funzione del sistema centrale (art. 35) e all'entrata in vigore del regolamento (art. 42); alle funzioni di monitoraggio e valutazione di eu-LISA (art. 36); all'esercizio del potere di adottare atti delegati conferito alla Commissione (art. 37), nonché alle modifiche apportate al regolamento (UE) 2018/1726 (art. 40), limitatamente alle funzioni di eu-LISA connesse alla gestione del nuovo sistema centrale.

L'art. 41 invita, infine, gli Stati membri ad attivarsi, quanto prima possibile, nell'adozione delle misure necessarie per garantire il corretto funzionamento di ECRIS-TCN, conformemente alle indicazioni fornite dal regolamento.

I regolamenti (UE) 2019/817 e 2019/818: l'interoperabilità tra sistemi di informazione dell'UE, nel settore delle frontiere e dei visti, nonché in quello della cooperazione di polizia e giudiziaria, asilo e migrazione.

I regolamenti (UE) 2019/817 e 2019/818 del Parlamento europeo e del Consiglio, entrambi del 20 maggio 2019 (in G.U.U.E., 22 maggio 2019, L 135/27 e L 135/85) e destinati a entrare in vigore decorsi venti giorni dalla pubblicazione nella Gazzetta ufficiale dell'Unione europea, istituiscono un quadro per l'interoperabilità (ossia l'interazione reciproca) tra i sistemi di informazione dell'UE, rispettivamente, nel settore delle frontiere e dei visti, e in quello della cooperazione di polizia e giudiziaria, asilo e migrazione.

Considerata l'uniformità della struttura e la sostanziale omogeneità dei contenuti – ad eccezione dei rispettivi settori di applicazione appena sopra indicati (art. 3) e delle disposizioni relative alle modifiche di altri strumenti dell'Unione (capo IX) – pare utile procedere a una trattazione unitaria di questi due regolamenti, prestando particolare attenzione alle novità di maggior rilievo, che implicano un significa-

tivo mutamento nel panorama sovranazionale, specialmente nell'ambito delle operazioni di trattamento dei dati personali e dell'identificazione delle persone fisiche.

Preme, anzitutto, rilevare che l'obiettivo, perseguito da entrambi i regolamenti, di garantire l'interoperabilità tra i sistemi di informazione e le banche dati dell'Unione europea, relative alla sicurezza, alle frontiere e alla gestione della migrazione, si pone in perfetta linea con le precedenti comunicazioni, risoluzioni e conclusioni che già avevano sollecitato un intervento in tal senso (considerando nn. 1-8), in vista di molteplici finalità.

In particolare, l'interazione reciproca tra i sistemi di informazione dell'Unione europea dovrebbe essere realizzata al fine di migliorare l'efficacia e l'efficienza dei controlli alle frontiere esterne; contribuire a prevenire e contrastare l'immigrazione illegale e assicurare un elevato livello di sicurezza sul territorio degli Stati membri; migliorare l'attuazione della politica comune in materia di visti; fornire assistenza nell'esame delle domande di protezione internazionale; contribuire alla prevenzione, all'accertamento e all'indagine di reati di terrorismo o altri gravi reati, nonché facilitare l'identificazione di persone ignote, che non sono in grado di dimostrare la propria identità, o resti umani non identificati nel caso di una catastrofe naturale, incidente o attentato terroristico (art. 2).

Dopo aver illustrato nel dettaglio le ragioni per cui si rende necessaria l'interoperabilità tra i sistemi di informazione, le norme forniscono una puntuale descrizione delle modalità da impiegare in vista della realizzazione degli obiettivi sopra richiamati. Si segnala, a titolo esemplificativo, la necessità di garantire la corretta identificazione delle persone, di contribuire a combattere la frode di identità, di migliorare la qualità dei dati e armonizzare le condizioni di sicurezza e protezione dei medesimi.

La reciproca interazione, voluta dai regolamenti "gemelli" e finalizzata ad agevolare la raccolta e lo scambio di informazioni tra Stati membri, coinvolge il sistema di ingressi e uscite (EES), il sistema di informazione visti (VIS), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), l'Eurodac, il sistema d'informazione Schengen (SIS) e il sistema europeo di informazione sui casellari giudiziali di cittadini di paesi terzi (ECRIS-TCN), neoistituito dal regolamento (UE) 2019/816, sopra esaminato.

La possibilità che tali sistemi di informazione interagiscano tra loro presuppone l'elaborazione di quelle che vengono definite «componenti dell'interoperabilità» (art. 1 § 2), in grado di delineare un nuovo e migliore approccio ai dati relativi alle frontiere, alla sicurezza interna dell'Unione e alla migrazione, nel pieno rispetto dei diritti fondamentali e dei principi dell'UE.

Si tratta, nello specifico, dell'istituzione di un portale di ricerca europeo (ESP), di un servizio comune di confronto biometrico (BMS comune), di un archivio comune di dati di identità (CIR) e di un rilevatore di identità multiple (MID), di cui si dirà meglio oltre.

È previsto, altresì, che dette componenti includano anche i dati di Europol, ma soltanto per consentire la loro consultazione simultaneamente a quella degli altri sistemi di informazione (considerando n. 11).

Prima di fissare la disciplina delle singole componenti dell'interoperabilità, i regolamenti contemplano, all'art. 5, la clausola di non discriminazione, all'interno della quale trova spazio una specifica tutela riservata ai minori, alle persone anziane, con disabilità o bisognose di protezione internazionale. Con riguardo alla categoria dei soggetti di minore età, si sottolinea la preminenza del *best interest of the child*, principio ribadito dalla recente direttiva (UE) 2016/800 del Parlamento europeo e del Consiglio sulle garanzie procedurali per i minori indagati o imputati nei procedimenti penali (per un commento, v. L. CAMALDO, *Garanzie europee per i minori autori di reato nel procedimento penale: la direttiva 2016/800/UE in relazione alla normativa nazionale*, in *Cass. pen.*, 2016, n. 12, p. 4572 ss.).

Venendo ora all'esame delle componenti destinate alla reciproca interazione, i regolamenti disciplinano, in primo luogo, il portale di ricerca europeo (ESP): si tratta di uno strumento che dovrebbe fungere da interfaccia unica o da mediatore di messaggi (*message broker*), in grado di consentire l'interrogazione parallela di tutti i sistemi di informazione dell'UE, dei dati Europol e delle banche dati Interpol, da parte degli Stati membri e delle agenzie dell'Unione, che abbiano accesso ad almeno uno dei sistemi di informazione dell'Unione (artt. 6 e 7). In conformità con le garanzie di riservatezza, le risposte fornite da ESP si riferiscono peraltro unicamente ai dati a cui l'utente abbia accesso secondo il diritto dell'Unione e nazionale (art. 9 § 6).

È poi previsto il servizio comune di confronto biometrico (BMS comune), un sistema automatizzato di identificazione dattiloscopica, istituito allo scopo di agevolare l'identificazione di una persona regi-

strata in diverse banche dati, ricorrendo all'utilizzo di una sola componente tecnologica per far corrispondere i dati biometrici di quella persona contenuti in altri sistemi. La facilitazione del confronto trasversale è resa possibile dal fatto che il BMS riunisce e conserva tutti i *template* biometrici, separati per logica in base al sistema di informazione di provenienza, in un unico luogo (considerando n. 18).

Da ultimo, si precisa che il trattamento dei dati biometrici, in quanto appartenenti alla categoria dei dati sensibili, deve essere orientato esclusivamente a identificare in modo univoco le persone interessate (considerando n. 20).

Per ciò che attiene all'archivio comune di dati di identità (CIR), esso si presenta come un contenitore comune di dati personali, compresi i dati di identità, quelli del documento di viaggio e i dati biometrici, che, operando in veste di infrastruttura centrale, consente di svolgere un'accurata verifica di identità, attraverso il confronto e l'abbinamento automatizzato dei dati già conservati separatamente nei singoli sistemi di informazione di provenienza (EES, VIS, ETIAS, Eurodac, ECRIS-TCN). Al fine di perfezionare le tecniche di identificazione e contrastare la frode di identità, è altresì opportuna la creazione di un fascicolo individuale, nel quale far confluire le informazioni relative alle identità connesse a una determinata persona, in modo tale che siano accessibili agli utenti debitamente autorizzati da ciascuno Stato membro.

A norma dell'art. 22, la consultazione dell'archivio comune è consentita qualora sussistano fondati motivi per ritenere che l'acceso ai sistemi di informazione sottostanti possa contribuire alla prevenzione, all'accertamento o all'indagine di reati di terrorismo o di altri gravi reati. In particolare, la norma in esame considera l'ipotesi in cui vi sia il sospetto che i dati dell'autore presunto o effettivo oppure della vittima di reato siano conservati nell'EES, nel VIS o nell'ETIAS.

Il CIR può essere, inoltre, oggetto di interrogazione da parte di un'autorità di polizia, in presenza di casi tassativamente individuati dall'art. 20: ad esempio, se sussistono dubbi sull'autenticità dei dati forniti da una persona o se questa si rifiuti di cooperare con le forze di polizia.

Il rilevatore di identità multiple (MID) si configura, invece, quale infrastruttura centrale e di comunicazione, deputata alla creazione e alla conservazione di collegamenti tra i dati sulle persone fisiche presenti nei vari sistemi d'informazione dell'UE (art. 25).

I dati oggetto di collegamento dovrebbero limitarsi a quelli necessari per verificare se l'interessato è registrato in maniera giustificata o ingiustificata e con identità diverse in sistemi differenti, ovvero per chiarire che due persone aventi identità simili possono non essere la stessa persona.

Al fine di agevolare le verifiche di identità per i viaggiatori in buona fede, si rende inoltre indispensabile la dotazione di misure volte a salvaguardare le persone con identità multiple lecite (considerando n. 39).

A seguito del riscontro positivo dell'interrogazione del sistema, la verifica manuale delle identità diverse compete all'autorità responsabile che ha creato o aggiornato i dati dai quali è emersa una corrispondenza (art. 29). A garanzia di una maggior trasparenza delle operazioni, si esige che l'accertamento in parola abbia luogo, se possibile, in presenza della persona interessata, alla quale è riconosciuta la facoltà, in tale sede, di fornire spiegazioni all'autorità responsabile (art. 29 § 4).

Una peculiare disciplina è dettata con riferimento ai collegamenti ottenuti attraverso il SIS, relativamente alle segnalazioni di persone ricercate per l'arresto ai fini di consegna o di estradizione, di persone scomparse o vulnerabili, di persone ricercate per partecipare a un procedimento giudiziario o da sottoporre a controlli. In tali ipotesi, si dispone infatti che l'autorità responsabile della verifica manuale delle diverse identità debba essere l'ufficio SIRENE dello Stato membro che ha generato la segnalazione. Trattandosi di segnalazioni sensibili, i risultati ottenuti dai collegamenti non dovrebbero peraltro essere condivisi con le autorità che inseriscono o aggiornano i dati ad esse collegati in uno degli altri sistemi di informazione dell'Unione (considerando n. 44).

Le successive disposizioni operano una classificazione dei collegamenti che possono instaurarsi tra i dati di due o più sistemi di informazione dell'UE, distinguendo, in particolare, tra collegamento giallo (art. 30), verde (art. 31), rosso (art. 32) e bianco (art. 33), a seconda del livello di intensità di corrispondenza delle informazioni registrate, e descrivendo i distinti casi riconducibili all'una piuttosto che all'altra tipologia di connessione.

Volendo, per esigenze di semplificazione, circoscrivere l'analisi all'ipotesi di collegamento rosso, basti qui sottolineare che esso indica l'esistenza di una persona che utilizza identità diverse in modo ingiustificato o si avvale dell'identità di un'altra persona. Tale tipo di collegamento consente l'interro-

gazione del MID alle autorità degli Stati membri e alle agenzie dell'Unione che hanno accesso ad almeno un sistema di informazione incluso nel CIR o nel SIS (considerando 46). Come si evince dall'art. 32, le persone oggetto di collegamento rosso dovrebbero ricevere informazione per iscritto, diretta a individuare l'autorità cui rivolgersi per l'esercizio dei loro diritti. Detta garanzia informativa è tuttavia destinata a soccombere a fronte delle esigenze di protezione della sicurezza e dell'ordine pubblico e di prevenzione della criminalità, ovvero a fronte del rischio di compromissione delle indagini in corso (art. 32 § 4).

In relazione ai profili strettamente tecnici, viene affidato all'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) il compito di istituire meccanismi automatizzati di controllo della qualità dei dati e di elaborare indicatori comuni, che includano norme minime di qualità per la conservazione dei dati all'interno dei sistemi di informazione dell'UE o delle componenti dell'interoperabilità.

Le norme di qualità dovrebbero permettere l'individuazione automatica dei dati palesemente errati o incoerenti e, di conseguenza, l'attivazione di una procedura di correzione. Compete a eu-LISA, inoltre, il monitoraggio periodico della qualità dei dati e la stesura di relazioni, da sottoporre alla valutazione della Commissione (art. 37).

L'art. 38 affronta poi la disciplina del formato universale dei messaggi (UMF), che funge da standard comunicativo per lo scambio transfrontaliero di dati tra i sistemi di informazione, le autorità o le organizzazioni del settore Giustizia e affari interni. Come può leggersi nel considerando n. 50, è previsto che, per le informazioni oggetto di scambio abituale, l'UMF dovrebbe definire un lessico comune e strutture logiche che favoriscano l'interoperabilità tra i vari sistemi di informazione.

I regolamenti di recente approvazione istituiscono, inoltre, l'archivio centrale di relazioni e statistiche (CRRS), finalizzato a produrre dati statistici intersistemici e relazioni analitiche a scopi strategici, operativi e di qualità dei dati, nonché a sostenere gli obiettivi dell'EES, del VIS, dell'ETIAS e del SIS, in conformità degli strumenti giuridici rispettivamente applicabili a tali sistemi (art. 39 e considerando n. 52).

Una cospicua parte dei due regolamenti in esame (artt. 40-53) è riservata alla protezione dei dati oggetto di trattamento ad opera delle componenti di interoperabilità. Apposite norme sono dettate in tema di responsabilità e sanzioni applicabili in caso di inosservanza delle disposizioni da parte degli Stati membri e delle agenzie dell'UE. Si stabilisce, inoltre, che le autorità di controllo, previste dal regolamento (UE) 2016/679 o dalla direttiva (UE) 2016/680, verifichino la legittimità del trattamento dei dati personali da parte degli Stati membri, anche in collaborazione con il Garante europeo della protezione dei dati, che è dotato di specifiche funzioni di sorveglianza (artt. 51, 52 e 53).

Sempre nell'ottica di garantire una sicura trasmissione dei dati personali, si auspica la cooperazione tra gli Stati membri ed eu-LISA, in sede di adozione di piani di sicurezza e di misure necessarie alla salvaguardia degli interessi di sicurezza sovranazionali. In particolare, eu-LISA si adopera affinché sia garantita la protezione fisica dei dati, mediante l'elaborazione di piani d'emergenza per la tutela delle infrastrutture critiche, e affinché venga impedito l'utilizzo illecito dei dati, nonché l'accesso di persone non autorizzate alle strutture utilizzate per il trattamento dei dati medesimi (art. 42 § 3).

A tutela dei diritti del singolo, l'art. 48 definisce le modalità di accesso, rettifica e cancellazione dei dati personali conservati nel MID, su richiesta della persona interessata, precisando che lo Stato membro debba rispondere senza indebito ritardo e, in ogni caso, entro 45 giorni dalla ricezione, prorogabili per ulteriori 15 giorni, tenuto conto della complessità e del numero delle richieste pervenute. Qualora la richiesta sia stata inoltrata a uno Stato membro diverso da quello competente per la verifica manuale delle identità, lo Stato, a cui è presentata la domanda, deve contattare entro 7 giorni l'autorità competente, la quale, a sua volta, è chiamata a verificare l'esattezza dei dati e la liceità del loro trattamento entro i 30 giorni successivi (art. 48 § 3).

Sotto il profilo delle responsabilità, i nuovi regolamenti distinguono la responsabilità di eu-LISA nella fase preliminare di progettazione e sviluppo (art. 54) e in quella successiva all'entrata in funzione di ciascuna componente dell'interoperabilità (art. 55) – che, com'è noto, verrà determinata dalla Commissione mediante atto di esecuzione – da quella degli Stati membri (art. 56) e, in limitate ipotesi, dell'unità centrale ETIAS.

In aggiunta a tali soggetti, il regolamento (UE) 2019/818, che è destinato ad applicarsi, tra l'altro, anche nel settore di cooperazione di polizia, pone a carico di Europol la responsabilità per la gestione e le

modalità d'uso e di accesso all'ESP e al CIR da parte del suo personale debitamente autorizzato, nonché per la creazione e l'aggiornamento periodico di un elenco di tale personale con indicazione delle relative qualifiche (art. 57 § 2).

Tralasciando l'esame delle norme relative alle modifiche degli altri strumenti dell'Unione (capo IX) e le consuete disposizioni finali (capo X), pare opportuno richiamare, per concludere, la valutazione contenuta nel considerando n. 41, ove si afferma che le nuove modalità di trattamento dei dati personali, funzionali alla corretta individuazione delle persone interessate, costituiscono indubbiamente un'ingerenza nei loro diritti fondamentali, tutelati dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Tuttavia, a tale presa di coscienza da parte del legislatore europeo, si accompagna la considerazione che una siffatta intrusione nell'altrui sfera di riservatezza appare del tutto giustificata alla luce dei preminenti obiettivi di gestione delle frontiere, di sicurezza interna dell'Unione e di efficace attuazione delle politiche europee in materia di asilo, migrazione e visti, che hanno animato l'introduzione di rinnovati meccanismi di scambio di informazioni sensibili a livello sovranazionale.