Consiglio dell'Unione europea

Bruxelles, 2 dicembre 2020
(OR. en)

5825/20

IXIM 23
ENFOPOL 41
CT 9
ENFOCUSTOM 25
CRIMORG 14
SCHENGEN 3
VISA 22
SIRIS 18
COPEN 35
ASIM 11
FRONT 22
COMIX 51
JAI 107

NOTA

Origine:	Segretariato generale del Consiglio
Destinatario:	Gruppo "Scambio di informazioni in ambito GAI" (IXIM)
n. doc. prec.:	9364/19
Oggetto:	Manuale per lo scambio di informazioni sull'attività di contrasto

1. Introduzione

Il manuale per lo scambio di informazioni sull'attività di contrasto intende integrare il manuale sulle operazioni transfrontaliere (doc. 10505/4/09 REV 4). Tanto il contenuto e la struttura del primo quanto le schede nazionali sono stati approvati dal gruppo DAPIX nel quadro della strategia di gestione delle informazioni per la sicurezza interna dell'UE, al fine di sostenere, razionalizzare e facilitare lo scambio di informazioni a livello transfrontaliero.

Per incrementare il valore pratico del manuale, saranno rese disponibili le traduzioni in tutte le lingue ufficiali dell'Unione. Inoltre, il manuale sarà aggiornato due volte all'anno, ove necessario alla luce delle novità legislative o dell'esperienza pratica.

Gli estremi di contatto nazionali sono aggiornati regolarmente dagli Stati membri e figurano nelle schede nazionali, che sono pubblicate sotto forma di addendum (ADD 1) al manuale. Tale addendum contiene informazioni sensibili e non può essere divulgato senza previa consultazione del segretariato generale del Consiglio (SGC), in linea con il regolamento (CE) n. 1049/2001[1].

2. Finalità del manuale

Il manuale è inteso principalmente come strumento destinato agli agenti di polizia che operano nel settore del collegamento internazionale e in particolare ai cosiddetti **operatori degli sportelli unici ("punti di contatto unici").** Dovrebbe pertanto essere quanto più facile da usare ed esauriente possibile.

Scopo del manuale è informare e facilitare la **cooperazione pratica quotidiana** tra le varie autorità degli Stati membri coinvolte nello scambio di informazioni di polizia a livello sia nazionale che internazionale, servire a fini di formazione e assicurare l'adozione di decisioni più informate per quanto riguarda la ricerca e lo scambio di informazioni a livello transfrontaliero.

Il manuale offre **una panoramica di tutti i sistemi, le basi giuridiche e gli strumenti di scambio di informazioni dell'UE** a disposizione delle autorità di contrasto degli Stati membri. In questo modo, all'atto di decidere in che modo ottenere o fornire informazioni a livello transfrontaliero, l'utilizzatore è pienamente informato delle opzioni disponibili.

Il manuale è completato da **schede nazionali** contenenti gli estremi e le informazioni pertinenti disponibili per lo scambio transfrontaliero. Mediante il regolare aggiornamento delle schede, gli Stati membri adempiono ai numerosi obblighi di notifica previsti dai diversi strumenti. Dette schede nazionali dovrebbero semplificare la gestione e il reperimento delle informazioni necessarie.

Il manuale incorpora le schede nazionali e le informazioni pratiche essenziali sulla decisione quadro 2006/960/GAI del Consiglio ("decisione quadro svedese") e sostituisce i precedenti orientamenti relativi a quest'ultima (doc. 9512/10 CRIMORG 90 ENFOPOL 125 ENFOCUSTOM 36 COMIX 346).

---

[1] Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione. Il regolamento stabilisce i limiti e i principi generali relativi all'accesso.

3. Contenuto del manuale

Il manuale è suddiviso in tre parti che sono redatte in modo da essere consultate separatamente l'una dall'altra secondo il volere del lettore.

La prima parte del manuale è composta da **liste di controllo** che forniscono un quadro pragmatico delle opzioni per lo scambio di informazioni e dei relativi aspetti pratici. Tali liste di controllo contribuiscono a guidare l'utilizzatore verso il punto di contatto appropriato per lo scambio di informazioni sulla base di elenchi di sistemi e metodi disponibili nei seguenti contesti operativi fondamentali:

– prevenzione dei reati (e dell'immigrazione clandestina) e relative indagini

– lotta al terrorismo

– mantenimento dell'ordine e della sicurezza pubblici

Nella seconda parte, una descrizione **generale** presenta sia gli organismi nazionali coinvolti nello scambio di informazioni che gli strumenti per tale scambio. Il manuale fa riferimento al ruolo centrale della decisione quadro 2006/960/GAI del Consiglio ("decisione quadro svedese") e della decisione 2008/615/GAI del Consiglio ("decisione di Prüm") nella più ampia sfera dello scambio di informazioni a livello dell'UE. Esso non si limita tuttavia a tali strumenti.

4. Iter

La redazione del manuale proposto figurava tra i punti di azione del terzo elenco di azioni della strategia di gestione delle informazioni e la prima versione del manuale è stata elaborata durante le presidenze irlandese, cipriota, greca, italiana e lettone.

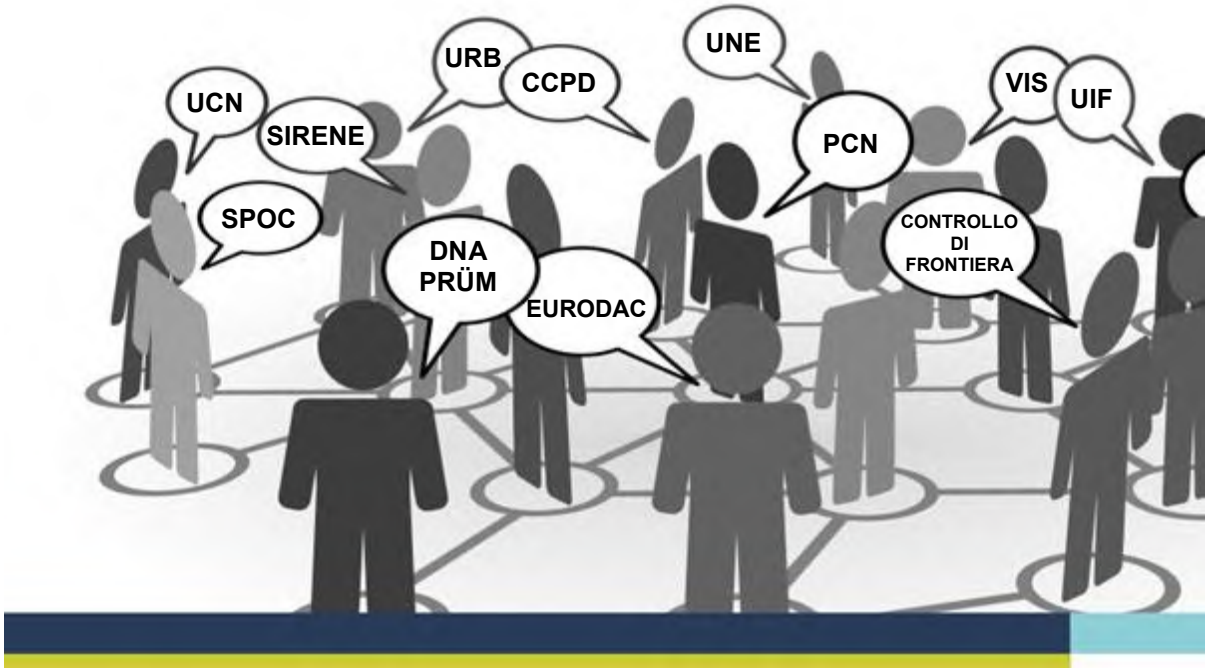
Per rendere ancora più agevole l'utilizzo del manuale per lo scambio di informazioni sull'attività di contrasto[2], le delegazioni sono invitate a distribuire la versione attuale e aggiornata del medesimo secondo le rispettive esigenze.

---

[2] Ai sensi dell'accordo sul recesso del Regno Unito di Gran Bretagna e Irlanda del Nord dall'Unione europea e dalla Comunità europea dell'energia atomica, il diritto dell'UE relativo allo scambio di informazioni nell'attività di contrasto si applica al Regno Unito e nel Regno Unito fino alla fine del periodo di transizione. Dopo la fine del periodo di transizione, solo un numero limitato di atti del diritto dell'Unione continuerà ad applicarsi allo scambio di informazioni in corso alle condizioni stabilite nell'accordo.

Consiglio dell'Unione europea
Segretariato generale
Direzione generale Giustizia e affari interni
Direzione Affari interni

Manuale per lo scambio di informazione sull'attività di contrasto



Sommario

Introduzione 10

PARTE I - Contesto operativo 12

LISTA DI CONTROLLO A: SCAMBIO DI INFORMAZIONI A FINI DELLA PREVENZIONE DEI REATI E DELLE RELATIVE INDAGINI 13

LISTA DI CONTROLLO B: SCAMBIO DI INFORMAZIONI A FINI DI LOTTA AI REATI DI TERRORISMO 22

LISTA DI CONTROLLO C: SCAMBIO DI INFORMAZIONI A FINI DI MANTENIMENTO DELL'ORDINE E DELLA SICUREZZA PUBBLICI 32

PARTE II - Informazioni generali 36

1. CANALI DI CONTATTO 37

1.1. SPOC - Sportello unico (punto di contatto unico) 37

1.2. Uffici SIRENE 41

1.3. Unità nazionale Europol (UNE) 42

1.4. Uffici centrali nazionali (UCN) INTERPOL 43

1.5. Punti di contatto nazionali "Prüm" 44

1.5.1. Punti di contatto nazionali "Prüm" - DNA e impronte digitali 44

1.5.2. Punto di contatto nazionale "Prüm" - Dati di immatricolazione dei veicoli 46

1.5.3. Punto di contatto nazionale "Prüm" per la prevenzione del terrorismo 47

1.5.4. Punti di contatto nazionali "Prüm" per eventi di rilievo 47

1.6. Punti nazionali (di polizia) d'informazione sul calcio 48

1.6.1. Il manuale per il settore calcistico 49

1.7. Punti focali nazionali Armi da fuoco (NFFP) 50

1.7.1. Orientamenti sulle migliori prassi in materia di NFFP 51

1.8. Centri di cooperazione di polizia e doganale (CCPD) 52

1.9. Ufficiali di collegamento 54

1.10. Uffici degli Stati membri per il recupero dei beni (URB) 55

1.11. Riciclaggio - Cooperazione tra unità di informazione finanziaria (FIU) 57

1.12. Convenzione di Napoli II 58

1.13. Unità d'informazione sui passeggeri (UIP) 59

1.14. Punti di accesso nazionali dell'EES 62

1.15. Unità nazionale ETIAS 64

1.16. Interoperabilità 67

1.17. Scelta del canale – Criteri usati comunemente 70

2. SISTEMI D'INFORMAZIONE 71

2.1. Sistema d'informazione Schengen – seconda generazione (SIS II) 71

2.2. SIE – Sistema di informazione Europol 74

2.3. SIENA - Applicazione di rete per lo scambio sicuro di informazioni di Europol 76

2.4. I-24/7 - Sistema globale di comunicazione di polizia di Interpol 77

2.4.1. Interpol: DNA Gateway 77

2.4.2. Banca data di impronte digitali di Interpol 78

2.4.3. Banca dati di Interpol sui documenti di viaggio rubati e smarriti 78

2.4.4. Documenti di viaggio associati a segnalazioni (TDAWN) 78

2.4.5. Tabella di riferimento delle armi da fuoco 78

2.5. ECRIS 79

2.5.1. ECRIS-TCN 80

2.6. Sistema d'informazione visti (VIS) 82

2.7. Eurodac 84

2.8. SID – Sistema d'informazione doganale 87

2.9. Documenti falsi e autentici online - FADO 88

2.10. Registro pubblico online dei documenti di identità e di viaggio autentici - PRADO 89

2.11. Sistema di ingressi/uscite (EES) 89

2.12. Sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) 92

2.13. Quadro sinottico dei sistemi informativi utilizzati nello scambio di informazioni a livello dell'UE 95

3. LEGISLAZIONE - IL CONTESTO GIURIDICO, LE NORME E GLI ORIENTAMENTI RELATIVI AI PRINCIPALI METODI E SISTEMI DI COMUNICAZIONE 103

3.1. Direttiva sulla protezione dei dati 103

3.2. La "decisione quadro svedese" 106

3.3. Accordo di Schengen 117

3.3.1. Scambio di dati all'interno e all'esterno del SIS II 117

3.3.2. Rifusione del Sistema d'informazione Schengen 121

3.4. Europol 123

3.5. Agenzia europea della guardia di frontiera e costiera (Frontex) 124

3.6. Interpol 127

3.7. Ufficiali di collegamento 128

3.8. Scambio di dati "Prüm" 130

3.9. Sistema d'informazione visti (VIS) 131

3.10. Eurodac 133

3.11. Napoli II 134

3.11.1. Sistema d'informazione doganale - SID 135

3.12. Uffici nazionali per il recupero dei beni (URB) e CARIN 136

3.13. Unità di informazione finanziaria (FIU) 138

3.14. Accordo UE/USA sul programma di controllo delle transazioni finanziarie dei terroristi (TFTP) 141

3.15. Scambio di informazioni sui casellari giudiziali (ECRIS) 142

3.15.1. Scambio di informazioni sui casellari giudiziali in ordine a cittadini di paesi terzi e apolidi (ECRIS-TCN) 144

3.16. Conservazione di dati sulle telecomunicazioni 145

3.17. Direttiva sul codice di prenotazione (PNR) 146

3.18. Informazioni anticipate sui passeggeri (API) 149

3.19. Infrazioni in materia di sicurezza stradale 150

3.20. Sistema di ingressi/uscite (EES) 151

3.21. Sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) 154

3.22. Normativa in materia di interoperabilità 156

INTRODUZIONE

Finalità del presente manuale

La cooperazione transfrontaliera tra forze di polizia dell'Unione europea si basa in larga misura sullo scambio di informazioni. Il presente manuale intende facilitare la cooperazione quotidiana al riguardo. Il suo principale destinatario è lo sportello unico (*Single Point of Contact* - SPOC) nazionale, vale a dire il punto di contatto unico incaricato di gestire il flusso di informazioni tra le diverse unità e i punti di contatto designati a livello sia nazionale che internazionale.

Il contesto della cooperazione nell'attività di contrasto[3] in Europa è caratterizzato da un aumento e un'accelerazione dello scambio di informazioni. Da un lato, esso poggia su tecnologie dell'informazione e della comunicazione in continua evoluzione. Dall'altro, è disponibile una moltitudine di banche dati a livello sia nazionale che internazionale.

Il manuale mira a rispondere alla necessità di reperire il giusto contatto o la giusta banca dati in uno specifico contesto operativo. Illustra brevemente la legislazione applicabile, senza tuttavia perdere di vista il suo obiettivo precipuo, ossia facilitare lo scambio di informazioni a livello transfrontaliero.

Struttura del manuale

Il manuale è diviso come segue:

La ***PARTE I - "Contesto operativo"*** **-** contiene una serie di tabelle o "liste di controllo" corrispondenti alle informazioni riportate nella *PARTE II* e nella *PARTE III*, con informazioni relative alla pertinente base giuridica o al punto di contatto. Le liste di controllo sono suddivise in tre aree tematiche principali:

- **prevenzione e lotta contro la criminalità (e l'immigrazione clandestina) - Lista di controllo A**
- **lotta ai reati di terrorismo - Lista di controllo B**
- **mantenimento dell'ordine pubblico - Lista di controllo C**

[3] Ai fini del presente manuale, per "attività di contrasto" si intende la prevenzione, l'accertamento o l'indagine in relazione ai reati di terrorismo quali definiti nella direttiva (UE) 2017/541 o agli altri reati gravi quali definiti all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI relativa al mandato d'arresto europeo (MAE).

Le liste di controllo servono a guidare il lettore dal punto scelto come canale o metodo di comunicazione idoneo in uno specifico contesto operativo alla fonte di informazioni di contatto o a qualsiasi disposizione legislativa, norma, regolamento e manuale di migliori pratiche pertinente.

La ***PARTE II - "Informazioni generali"*** - illustra il contesto dell'attività di contrasto con riferimento ai vari metodi e canali di comunicazione a disposizione delle forze di polizia dell'UE. Questa seconda parte si suddivide ulteriormente nelle seguenti tre aree:

- **canali di comunicazione (ossia gli organismi coinvolti nello scambio di informazioni sull'attività di contrasto)**
- **sistemi informativi e banche dati utilizzati nello scambio di dati transfrontaliero**
- **legislazione - il contesto legislativo e le norme e gli orientamenti relativi ai principali metodi e sistemi di comunicazione**

La ***PARTE III - "Schede nazionali"*** **-** figura nell'addendum alla presente nota e contiene schede nazionali con informazioni dettagliate sui punti di contatto utili per tutti gli aspetti dello scambio di informazioni transfrontaliero cui è fatto riferimento in tutto il documento. Spetta agli Stati membri notificare tempestivamente eventuali variazioni al segretariato generale del Consiglio. Mediante il regolare aggiornamento delle schede nazionali di cui all'addendum al manuale, gli Stati membri adempiono ai numerosi obblighi di notifica previsti dai diversi strumenti. Ciò dovrebbe semplificare la gestione e il reperimento di queste informazioni in futuro.

PARTE I - CONTESTO OPERATIVO

LISTA DI CONTROLLO A: SCAMBIO DI INFORMAZIONI A FINI DELLA PREVENZIONE DEI REATI E DELLE RELATIVE INDAGINI

Sistema d'informazione	Punti di accesso nazionali	Base giuridica	Manuale
Sistema d'informazione Schengen / SIS II	SIRENE (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry Bureau - Ufficio per le informazioni supplementari richieste all'ingresso nazionale)	Acquis di Schengen di cui all'articolo 1, paragrafo 2, della decisione 1999/435/CE del Consiglio del 20 maggio 1999 GU L 239 del 22.9.2000, pag. 1 Regolamento (CE) n. 1987/2006 GU L 381 del 28.12.2006, pag. 4 Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione, GU L 312 del 7.12.2018, pag. 56	Versione riveduta del catalogo aggiornato delle raccomandazioni per la corretta applicazione dell'acquis di Schengen e delle migliori pratiche, 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Decisione di esecuzione (UE) 2017/1528 della Commissione, del 31 agosto 2017, che sostituisce l'allegato della decisione di esecuzione 2013/115/UE riguardante il manuale SIRENE e altre disposizioni di attuazione per il sistema d'informazione Schengen di seconda generazione (SIS II), GU L 231 del 7.9.2017, pag. 6.

Europol / Funzione indice del sistema di informazione Europol - SIE Archivi di lavoro per fini di analisi	UNE	Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI, GU L 135 del 24.5.2016, pag. 53 (applicabile a decorrere dal 1º maggio 2017)	
Interpol / I-24/7	UCN (Ufficio centrale nazionale)	Regolamento di INTERPOL sul trattamento dei dati [III/IRPD/GA/2011(2014)] Regolamento relativo al controllo delle informazioni e all'accesso agli archivi INTERPOL [II.E/RCIA/GA/2004(2009)]	
DNA / Consultazione automatizzata di banche dati nazionali designate ai sensi della decisione di Prüm	Punto di contatto nazionale 1ª fase: consultazione automatizzata	Decisione 2008/615/GAI del Consiglio, articoli 3 e 4, GU L 210 del 6.8.2008, pag. 1	
	2ª fase: trasmissione di ulteriori dati personali e di altre informazioni	Legislazione nazionale Decisione quadro 2006/960/GAI del Consiglio ("decisione quadro svedese") GU L 386 del 29.12.2006, pag. 89 Rettifica GU L 75 del 15.3.2007, pag. 26	

Impronte digitali / Consultazione dei sistemi automatizzati di identificazione delle impronte digitali (AFIS) nazionali ai sensi della decisione di Prüm	Punto di contatto nazionale 1ª fase: consultazione automatizzata	Decisione 2008/615/GAI del Consiglio, articolo 9 GU L 210 del 6.8.2008, pag. 1	
	2ª fase: trasmissione di ulteriori dati personali e di altre informazioni	Legislazione nazionale Decisione quadro 2006/960/GAI del Consiglio ("decisione quadro svedese")	
Dati di immatricolazione dei veicoli / Consultazione automatizzata di banche dati contenenti i dati di immatricolazione dei veicoli ai sensi della decisione di Prüm	Punto di contatto nazionale per le richieste in entrata	Decisione 2008/615/GAI del Consiglio, articolo 12 GU L 210 del 6.8.2008, pag. 1	
	per le richieste in uscita	come sopra	
Dati sul codice di prenotazione (PNR)	Unità d'informazione sui passeggeri (UIP)	Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi GU L 119 del 4.5.2016, pag. 132	

Sistema di informazione visti / VIS	Punti di accesso centrale nazionali	Decisione 2004/512/CE del Consiglio GU L 213 del 15.6.2004, pag. 5 Decisione 2008/633/GAI del Consiglio GU L 218 del 13.8.2008, pag. 126 Regolamento (CE) n. 767/2008 *GU L 218 del 13.8.2008* Elenco delle autorità competenti il cui personale debitamente autorizzato ha accesso al sistema di informazione visti (Visa Information System – VIS) ai fini dell'inserimento, della modifica, della cancellazione e della consultazione dei dati (2016/C 187/04), GU C 187 del 26.5.2016, pag. 4	

Eurodac	Autorità nazionali competenti	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) GU L 180 del 29.6.2013, pag. 1 Regolamento (UE) n. 604/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide GU L 180 del 29.6.2013, pag. 31	

SID - Sistema d'informazione doganale	Punti di accesso nazionali	Decisione 2009/917/GAI del Consiglio sull'uso dell'informatica nel settore doganale GU L 323 del 10.12.2009, pag. 20	
Sistema europeo di informazione sui casellari giudiziali / ECRIS	Autorità centrale nazionale	Direttiva (UE) 2019/884 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio GU L 151 del 7.6.2019, pag. 143	ECRIS - Manuale non vincolante destinato agli operatori del settore disponibile in formato elettronico in CIRCABC https://circabc.europa.eu
Rete interagenzie Camden per il recupero dei beni (CARIN)	Ufficio per il recupero dei beni (URB)	Decisione (2007/845/GAI) del Consiglio, del 6 dicembre 2007, concernente la cooperazione tra gli uffici degli Stati membri per il recupero dei beni nel settore del reperimento e dell'identificazione dei proventi di reato o altri beni connessi GU L 332 del 18.12.2007, pag. 103	Manuale delle migliori pratiche nella lotta contro la criminalità finanziaria: una raccolta di buoni esempi di sistemi ben sviluppati negli Stati membri per combattere la criminalità finanziaria 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37

FIU.NET (rete delle unità di informazione finanziaria)	Unità di informazione finanziaria (FIU)	Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 658/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione GU L 141 del 5.6.2015, pag. 73 Le FIU sono di recente regolazione anche nella direttiva (UE) 2019/1153 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati, e che abroga la decisione 2000/642/GAI del Consiglio GU L 186 dell'11.7.2019, pag. 122	Manuale delle migliori pratiche nella lotta contro la criminalità finanziaria: una raccolta di buoni esempi di sistemi ben sviluppati negli Stati membri per combattere la criminalità finanziaria 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37

Rete dei punti focali nazionali Armi da fuoco	PUNTI FOCALI NAZIONALI ARMI DA FUOCO (NFFP)	Comunicazione della Commissione al Parlamento europeo e al Consiglio, COM(2015) 624 final. Attuazione dell'agenda europea sulla sicurezza: piano d'azione dell'UE contro il traffico e l'uso illecito di armi da fuoco ed esplosivi 14971/15 COSI 184 ENFOPOL 404 ENFOCUSTOM 142 CYBER 125 CRIMORG 129 Comunicazione congiunta al Parlamento europeo e al Consiglio JOIN (2018) 17 final. Elementi per una strategia dell'Unione europea contro le armi da fuoco, le armi leggere e le armi di piccolo calibro illegali e le relative munizioni "Mettere in sicurezza le armi, proteggere i cittadini" 11271/18 CF SP/PESC 735 CONOP 70 CODUN 26 COARM 218 Conclusioni del Consiglio sull'adozione di una strategia dell'Unione europea contro le armi da fuoco, le armi leggere e le armi di piccolo calibro illegali e le relative munizioni. 13581/18 CONOP 98 CODUN 36 COARM 289 CF SP/PESC 985 COSI 288 ENFOPOL 565	Reti e gruppi di esperti connessi al gruppo "Applicazione della legge" - Esperti europei in materia di armi da fuoco (EFE) Orientamenti sulle migliori prassi per la creazione di punti focali nazionali Armi da fuoco 8586/18 ENFOPOL 207

		Direttiva di esecuzione (UE) 2019/69 della Commissione, del 16 gennaio 2019, che stabilisce le specifiche tecniche relative alle armi d'allarme o da segnalazione a norma della direttiva 91/477/CEE del Consiglio relativa al controllo dell'acquisizione e della detenzione di armi GU L 15 del 17.1.2019, pag. 22, articolo 3 Regolamento delegato (UE) 2019/686 della Commissione, del 16 gennaio 2019, che stabilisce le modalità dettagliate, a norma della direttiva 91/477/CEE del Consiglio, per lo scambio sistematico con mezzi elettronici di informazioni relative al trasferimento di armi da fuoco nell'Unione GU L 116 del 3.5.2019, pag. 1, articolo 3	

LISTA DI CONTROLLO B: SCAMBIO DI INFORMAZIONI A FINI DI LOTTA AI REATI DI TERRORISMO

Sistema d'informazione	**Punto di accesso nazionale**	**Base giuridica**	**Manuale**
Sistema d'informazione Schengen / SIS II	SIRENE (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry Bureau - Ufficio per le informazioni supplementari richieste all'ingresso nazionale)	Acquis di Schengen di cui all'articolo 1, paragrafo 2, della decisione 1999/435/CE del Consiglio del 20 maggio 1999 GU L 239 del 22.9.2000, pag. 1 Regolamento (CE) n. 1987/2006 GU L 381 del 28.12.2006, pag. 4 Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione, GU L 312 del 7.12.2018, pag. 56	Versione riveduta del catalogo aggiornato delle raccomandazioni per la corretta applicazione dell'acquis di Schengen e delle migliori pratiche, 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Decisione di esecuzione (UE) 2015/219 della Commissione, del 29 gennaio 2015, che sostituisce l'allegato della decisione di esecuzione 2013/115/UE riguardante il manuale SIRENE e altre disposizioni di attuazione per il sistema d'informazione Schengen di seconda generazione (SIS II) (notificata con il numero C(2015) 326)

Europol / Funzione indice del sistema di informazione Europol - SIE Archivi di lavoro per fini di analisi	UNE	Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI, GU L 135 del 24.5.2016, pag. 53 (applicabile a decorrere dal 1º maggio 2017)	
Interpol / I-24/7	UCN (Ufficio centrale nazionale)	Regolamento di INTERPOL sul trattamento dei dati [III/IRPD/GA/2011(2014)] Regolamento relativo al controllo delle informazioni e all'accesso agli archivi di INTERPOL [II.E/RCIA/GA/2004(2009)]	
DNA / Consultazione automatizzata di banche dati nazionali designate ai sensi della decisione di Prüm	Punto di contatto nazionale 1ª fase: consultazione automatizzata	Decisione 2008/615/GAI del Consiglio, articoli 3 e 4, GU L 210 del 6.8.2008, pag. 1	
	2ª fase: trasmissione di ulteriori dati personali e di altre informazioni	Legislazione nazionale Decisione quadro 2006/960/GAI del Consiglio ("decisione quadro svedese") GU L 386 del 29.12.2006, pag. 89 Rettifica GU L 75 del 15.3.2007, pag. 26	

Impronte digitali / Consultazione dei sistemi automatizzati di identificazione delle impronte digitali (AFIS) nazionali ai sensi della decisione di Prüm	Punto di contatto nazionale 1ª fase: consultazione automatizzata	Decisione 2008/615/GAI del Consiglio, articolo 9 GU L 210 del 6.8.2008, pag. 1	
	2ª fase: trasmissione di ulteriori dati personali e di altre informazioni	Legislazione nazionale Decisione quadro 2006/960/GAI del Consiglio ("decisione quadro svedese")	
Dati di immatricolazione dei veicoli / Consultazione automatizzata di banche dati contenenti i dati di immatricolazione dei veicoli ai sensi della decisione di Prüm	Punto di contatto nazionale per le richieste in entrata	Decisione 2008/615/GAI del Consiglio, articolo 12 GU L 210 del 6.8.2008, pag. 1	
	per le richieste in uscita	come sopra	
DNA / Consultazione automatizzata di banche dati nazionali designate ai sensi della decisione di Prüm	Punto di contatto nazionale 1ª fase: consultazione automatizzata	Decisione 2008/615/GAI del Consiglio, articoli 3 e 4, GU L 210 del 6.8.2008, pag. 1	*Guida all'attuazione - Scambio di dati sul DNA* 7148/15 DAPIX 40 CRIMORG 25 ENFOPOL 61
Rete "Prüm" per la trasmissione di dati personali e informazioni specifiche per la prevenzione dei reati di terrorismo	Punto di contatto nazionale "Prüm" per la lotta al terrorismo	Decisione 2008/615/GAI del Consiglio, articolo 16 GU L 210 del 6.8.2008, pag. 1	

Dati sul codice di prenotazione (PNR)	Unità d'informazione sui passeggeri (UIP)	Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi GU L 119 del 4.5.2016, pag. 132	
Sistema di informazione visti / VIS	Punti di accesso centrale nazionali	Decisione 2004/512/CE del Consiglio GU L 213 del 15.6.2004, pag. 5 Decisione 2008/633/GAI del Consiglio GU L 218 del 13.8.2008, pag. 126 Regolamento (CE) n. 767/2008 GU L 218 del 13.8.2008 Elenco delle autorità competenti il cui personale debitamente autorizzato ha accesso al sistema di informazione visti (Visa Information System – VIS) ai fini dell'inserimento, della modifica, della cancellazione e della consultazione dei dati (2016/C 187/04), GU C 187 del 26.5.2016, pag. 4	

Eurodac	Autorità nazionali competenti	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) GU L 180 del 29.6.2013, pag. 1 Regolamento (UE) n. 604/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide GU L 180 del 29.6.2013, pag. 31	

Sistema europeo di informazione sui casellari giudiziali / ECRIS	Autorità centrale nazionale	Direttiva (UE) 2019/884 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio GU L 151 del 7.6.2019, pag. 143	ECRIS - Manuale non vincolante destinato agli operatori del settore disponibile in formato elettronico in CIRCABC https://circabc.europa.eu

Sistema europeo di informazione sui casellari giudiziali in ordine a cittadini di paesi terzi e apolidi (ECRIS-TCN)	Autorità centrale nazionale	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 cittadini 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 GU L 135 del 22.5.2019, pag. 1 Direttiva (UE) 2019/884 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio GU L 151 del 7.6.2019, pag. 143	
Rete interagenzie Camden per il recupero dei beni (CARIN)	Ufficio per il recupero dei beni (URB)	Decisione (2007/845/GAI) del Consiglio, del 6 dicembre 2007, concernente la cooperazione tra gli uffici degli Stati membri per il recupero dei beni nel settore del reperimento e dell'identificazione dei proventi di reato o altri beni connessi GU L 332 del 18.12.2007, pag. 103	

FIU.NET (rete delle unità di informazione finanziaria)	Unità di informazione finanziaria (FIU)	Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 658/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione GU L 141 del 5.6.2015, pag. 73 Le FIU sono di recente regolazione anche nella direttiva (UE) 2019/1153 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati, e che abroga la decisione 2000/642/GAI del Consiglio GU L 186 dell'11.7.2019, pag. 122	

Rete dei punti focali nazionali Armi da fuoco	PUNTI FOCALI NAZIONALI ARMI DA FUOCO (NFFP)	Comunicazione della Commissione al Parlamento europeo e al Consiglio, COM(2015) 624 final. Attuazione dell'agenda europea sulla sicurezza: piano d'azione dell'UE contro il traffico e l'uso illecito di armi da fuoco ed esplosivi 14971/15 Comunicazione congiunta al Parlamento europeo e al Consiglio JOIN (2018) 17 final. Elementi per una strategia dell'Unione europea contro le armi da fuoco, le armi leggere e le armi di piccolo calibro illegali e le relative munizioni "Mettere in sicurezza le armi, proteggere i cittadini" 11271/18 Conclusioni del Consiglio sull'adozione di una strategia dell'Unione europea contro le armi da fuoco, le armi leggere e le armi di piccolo calibro illegali e le relative munizioni. 13581/18 Direttiva di esecuzione (UE) 2019/69 della Commissione, del 16 gennaio 2019, che stabilisce le specifiche tecniche relative alle armi d'allarme o da segnalazione a norma della direttiva 91/477/CEE del Consiglio relativa al controllo dell'acquisizione e della detenzione di armi, GU L 15 del 17.1.2019, pag. 22, articolo 3	Reti e gruppi di esperti connessi al gruppo "Applicazione della legge" - Esperti europei in materia di armi da fuoco (EFE) Orientamenti sulle migliori prassi per la creazione di punti focali nazionali Armi da fuoco 8586/18 ENFOPOL 207

		Regolamento delegato (UE) 2019/686 della Commissione, del 16 gennaio 2019, che stabilisce le modalità dettagliate, a norma della direttiva 91/477/CEE del Consiglio, per lo scambio sistematico con mezzi elettronici di informazioni relative al trasferimento di armi da fuoco nell'Unione, GU L 116 del 3.5.2019, pag. 1, articolo 3	

LISTA DI CONTROLLO C: SCAMBIO DI INFORMAZIONI A FINI DI MANTENIMENTO DELL'ORDINE E DELLA SICUREZZA PUBBLICI

Sistema d'informazione	**Punto di accesso nazionale**	**Base giuridica**	
Rete dei punti di contatto permanenti in materia di ordine pubblico	Punti di contatto nazionali	Azione comune (97/339/GAI) del 26 maggio 1997 adottata dal Consiglio in base all'articolo K.3 del trattato sull'Unione europea in materia di cooperazione nel settore dell'ordine pubblico e della pubblica sicurezza, articolo 3, lettera b) GU L 147 del 5.6.1997, pag. 1	
Rete "Prüm" per la trasmissione di dati personali e non personali per la prevenzione dei reati e il mantenimento dell'ordine e della sicurezza pubblici durante eventi di rilievo a dimensione transfrontaliera	Punto di contatto nazionale "Prüm" / Eventi di rilievo	Decisione 2008/615/GAI del Consiglio, articolo 15 GU L 210 del 6.8.2008, pag. 1 Legislazione nazionale	

Rete dei punti nazionali d'informazione sul calcio	Punti nazionali d'informazione sul calcio / PNIC	Decisione (2002/348/GAI) del Consiglio, del 25 aprile 2002, concernente la sicurezza in occasione di partite di calcio internazionali GU L 121 dell'8.5.2002, pag. 1 Decisione (2007/412/GAI) del Consiglio, del 12 giugno 2007, che modifica la decisione 2002/348/GAI concernente la sicurezza in occasione di partite di calcio internazionali GU L 155 del 15.6.2007, pag. 76	Raccomandazione (2007/C 314/02) del Consiglio, del 6 dicembre 2007, relativa a un manuale per le autorità di polizia e di sicurezza concernente la cooperazione in occasione di eventi importanti di dimensione internazionale GU C 314 del 22.12.2007, pag. 4 Risoluzione del Consiglio, del 3 giugno 2010, concernente un manuale aggiornato di raccomandazioni per la cooperazione internazionale tra forze di polizia e misure per prevenire e combattere la violenza e i disordini in occasione delle partite di calcio di dimensione internazionale alle quali è interessato almeno uno Stato membro GU C 165 del 24.6.2010, pag. 1

Rete dei punti focali nazionali Armi da fuoco	PUNTI FOCALI NAZIONALI ARMI DA FUOCO (NFFP)	Comunicazione della Commissione al Parlamento europeo e al Consiglio, COM(2015) 624 final. Attuazione dell'agenda europea sulla sicurezza: piano d'azione dell'UE contro il traffico e l'uso illecito di armi da fuoco ed esplosivi 14971/15 Comunicazione congiunta al Parlamento europeo e al Consiglio JOIN (2018) 17 final. Elementi per una strategia dell'Unione europea contro le armi da fuoco, le armi leggere e le armi di piccolo calibro illegali e le relative munizioni "Mettere in sicurezza le armi, proteggere i cittadini" 11271/18 Conclusioni del Consiglio sull'adozione di una strategia dell'Unione europea contro le armi da fuoco, le armi leggere e le armi di piccolo calibro illegali e le relative munizioni. 13581/18 Direttiva di esecuzione (UE) 2019/69 della Commissione, del 16 gennaio 2019, che stabilisce le specifiche tecniche relative alle armi d'allarme o da segnalazione a norma della direttiva 91/477/CEE del Consiglio relativa al controllo dell'acquisizione e della detenzione di armi, GU L 15 del 17.1.2019, pag. 22, articolo 3	Reti e gruppi di esperti connessi al gruppo "Applicazione della legge" - Esperti europei in materia di armi da fuoco (EFE) Orientamenti sulle migliori prassi per la creazione di punti focali nazionali Armi da fuoco 8586/18 ENFOPOL 207

		Regolamento delegato (UE) 2019/686 della Commissione, del 16 gennaio 2019, che stabilisce le modalità dettagliate, a norma della direttiva 91/477/CEE del Consiglio, per lo scambio sistematico con mezzi elettronici di informazioni relative al trasferimento di armi da fuoco nell'Unione, GU L 116 del 3.5.2019, pag. 1, articolo 3	
Rete europea di protezione delle personalità	Punti di accesso nazionali	Decisione 2009/796/GAI del Consiglio, del 4 giugno 2009, recante modifica della decisione 2002/956/GAI relativa all'istituzione di una rete europea di protezione delle personalità GU L 283 del 30.10.2009, pag. 62	Manuale della rete europea di protezione delle personalità 10478/13 ENFOPOL 173
Centri di cooperazione di polizia e doganale	CCPD	Accordi bilaterali	

PARTE II - INFORMAZIONI GENERALI

1. CANALI DI CONTATTO[4]

1.1. SPOC - Sportello unico (punto di contatto unico)

Numerosi punti di contatto nazionali

Gli Stati membri, sia richiesti che richiedenti, fanno fronte al crescente flusso transfrontaliero di informazioni migliorando l'efficienza delle reti e delle strutture operative a livello sia nazionale che europeo. Molti strumenti giuridici dell'UE relativi alla cooperazione transfrontaliera nell'attività di contrasto richiedono l'istituzione di specifici organismi/uffici/autorità competenti o di punti di contatto nazionali (PCN). La polizia, le dogane o altre autorità competenti autorizzate dalla legislazione nazionale devono scambiarsi informazioni attraverso tali punti di contatto nazionali designati, i quali, all'interno di un determinato Stato membro, possono collocarsi in diversi dipartimenti delle forze di polizia o persino in diversi ministeri. Per fornire una visione d'insieme, nella parte III del presente documento il segretariato generale del Consiglio pubblica e aggiorna regolarmente elenchi di specifici punti di contatto nazionali per lo scambio, a livello UE, di informazioni su dati inerenti all'attività di contrasto.

Principio di disponibilità - Decisione quadro svedese

Lo scambio di informazioni e analisi (intelligence) di rilevanza transfrontaliera sull'attività di contrasto[5] dovrebbe soddisfare le condizioni derivanti dal "principio di disponibilità" attuato dalla "decisione quadro svedese". Ciò implica che:

- un agente di un servizio di contrasto di uno Stato membro che ha bisogno di informazioni nell'esercizio delle sue funzioni può ottenere tali informazioni da un altro Stato membro e che
- le autorità di contrasto dell'altro Stato membro che dispone di tali informazioni sono tenute a trasmettergliele per i fini dichiarati, tenendo conto delle esigenze delle indagini in corso in detto Stato membro, e che

---

4 Organismi nazionali coinvolti nello scambio di informazioni sull'attività di contrasto.

5 Ai fini del presente manuale, per "attività di contrasto" si intende la prevenzione, l'accertamento o l'indagine in relazione ai reati di terrorismo quali definiti nella direttiva (UE) 2017/541 o agli altri reati gravi quali definiti all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI relativa al mandato d'arresto europeo (MAE), se punibili conformemente al diritto nazionale con una pena detentiva o una misura di sicurezza privativa della libertà personale per un periodo massimo di almeno tre anni.

- una volta che in uno Stato membro siano disponibili informazioni di polizia, queste sono condivise a livello transfrontaliero alle stesse condizioni che disciplinano la condivisione di informazioni a livello nazionale, il che significa che le norme applicate in un caso transfrontaliero non sono più rigorose di quelle applicate allo scambio di dati a livello nazionale ("principio dell'accesso equivalente").

Sportello unico (punto di contatto unico - SPOC)

La combinazione tra i rigorosi requisiti della decisione quadro svedese e l'esistenza di diverse strategie nazionali per gestire le varie iniziative per lo scambio di informazioni esige un approccio più semplice e uniforme a livello di Stato membro al fine di garantire un trattamento efficace ed efficiente di tutte le richieste di informazioni tra servizi di contrasto dell'UE.

Le conclusioni del Consiglio sul modello europeo di scambio di informazioni (EIXM)[6], adottate nel giugno 2013, hanno riconosciuto la potenzialità di un punto di contatto unico (o sportello unico) per lo scambio di informazioni all'interno di ciascuno Stato membro di contribuire a snellire il processo in un contesto giuridico e operativo sempre più complesso.

Sebbene la definizione di SPOC sembri differire da uno Stato membro all'altro, la prassi che quasi tutti gli Stati membri hanno adottato consiste nell'effettuare il più possibile lo scambio di informazioni attraverso uno sportello unico (punto di contatto unico - SPOC). Le linee guida relative ad uno sportello unico[7] suggeriscono come strutturare gli SPOC al fine di ottimizzare l'uso delle risorse, evitare sovrapposizioni e rendere la cooperazione con gli altri Stati membri più efficiente, utile e trasparente.

Tra le linee guida, gli Stati membri dovrebbero scegliere la soluzione adatta allo loro situazione nell'ottica dell'obiettivo comune e concordato di migliorare la cooperazione internazionale e dovrebbero valutare modi appropriati per informare gli altri Stati membri della soluzione scelta ai fini dello scambio di migliori pratiche.

---

6 Conclusioni del Consiglio facenti seguito alla comunicazione della Commissione sul modello europeo di scambio di informazioni (EIXM), doc. 9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146.

7 Progetto di linee guida relative ad uno sportello unico per lo scambio internazionale di informazioni sull'attività di contrasto, docc. 10492/14 DAPIX 75 ENFOPOL 157 e 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1.

Idealmente, lo SPOC:

- ha accesso alla più vasta gamma di banche dati nazionali, europee e internazionali pertinenti sull'attività di contrasto ai fini di una celere gestione dello scambio diretto di informazioni fra le autorità nazionali competenti;

- ospita le unità nazionali SIRENE, Europol e INTERPOL;

- ospita il punto di contatto per gli ufficiali di collegamento, i punti di contatto designati a norma della decisione quadro svedese e delle "decisioni di Prüm" e, se del caso, i punti di contatto per gli uffici regionali e bilaterali;

- è inserito in un ambiente di lavoro protetto ed è dotato di personale sufficiente e adeguato, comprese capacità di interpretazione e traduzione, per operare 24 ore su 24 e 7 giorni su 7. Per quanto possibile, tutto il personale dovrebbe essere formato e attrezzato per/incaricato di svolgere tutti i tipi di compiti all'interno dello SPOC. Qualora ciò non sia possibile, si dovrebbe assicurare che tutti i compiti possano essere svolti 24 ore su 24 e 7 giorni su 7 dai funzionari di turno;

- è un organismo interservizi composto da personale proveniente da/appartenente a diversi servizi e/o ministeri, comprese la polizia criminale, le guardie di frontiera, le dogane e le autorità giudiziarie.

Struttura tipica dell'ufficio di uno sportello unico (punto di contatto unico - SPOC) nazionale

Unità centrale per la cooperazione operativa di polizia,

Piattaforma per lo scambio di informazioni

La S.C.C.O.Pol (Section Centrale de Coopération Opérationnelle de Police - Sezione centrale di cooperazione operativa di polizia) è una struttura ***interministeriale*** *composta da 67 poliziotti, gendarmi e agenti doganali. I magistrati del B.E.P.I. (Bureau de l'entraide pénale internationale - Ufficio di mutua assistenza penale internazionale) del Ministero della giustizia svolgono inoltre, negli stessi locali, un servizio di base volto a convalidare le richieste francesi di emissione di mandati di arresto europei e l'iscrizione nel registro nazionale delle persone ricercate delle richieste di arresto e degli avvisi rossi pervenuti dall'estero.*

Per garantire la necessaria ***trasversalità*** *dei tre canali di cooperazione, nell'agosto del 2004 è stato designato presso la S.C.C.O.Pol un punto di contatto centrale incaricato principalmente di assistere i servizi di contrasto francesi nella scelta del miglior strumento di cooperazione di polizia a seconda della natura e della complessità dell'indagine in corso. Esso verifica la liceità della richiesta, effettua i primi controlli incrociati e inoltra la richiesta verso il canale di cooperazione più adatto in base alla richiesta degli inquirenti. Soltanto le richieste relative a una segnalazione Schengen rientrano nella competenza esclusiva del S.I.R.E.N.E. Francia.*

Grazie ad una proficua messa in comune delle risorse, la S.C.C.O.Pol tratta, operando ***24 ore su 24****, quasi* ***350 000 messaggi all'anno****, su una* ***piattaforma sicura unica*** *e con personale limitato.*

La competenza della S.C.C.O.Pol per più canali di cooperazione le consente di rappresentare la Francia in seno a gruppi europei (SIS/VIS, SIS/SIRENE, capi delle UNE) o gruppi INTERPOL (riunione degli ufficiali di contatto di INTERPOL, gruppo "Avvisi"), nonché di apportare un punto di vista operativo pertinente all'unità DRI (Division des relations internationales - Divisione per le relazioni internazionali) responsabile in Francia del monitoraggio degli organi di governance di INTERPOL e di Europol.

1.2. Uffici SIRENE

Gli uffici SIRENE sono essenziali per le operazioni SIS e lo scambio di informazioni. In ogni Stato membro sono istituiti, nel quadro dell'*acquis* di Schengen[8], uffici SIRENE (**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry - Informazioni supplementari richieste all'ingresso nazionale) permanenti quali autorità designate cui è conferita la responsabilità centrale per la sezione nazionale del sistema d'informazione Schengen (SIS II). Essi costituiscono il punto di contatto per gli uffici SIRENE delle altre parti contraenti e il collegamento con le autorità e i servizi nazionali. SIS II è un sistema di risconto positivo o negativo ("hit/no hit") basato su ricerche. Gli uffici scambiano dati relativi alle segnalazioni SIS II[9] 24 ore su 24 e 7 giorni su 7. Una segnalazione è un insieme di dati che consente alle autorità di identificare persone o oggetti al fine di intraprendere l'azione appropriata.

Per "informazioni supplementari" s'intendono informazioni non memorizzate nel SIS II ma connesse alle segnalazioni del SIS II, che devono essere scambiate, a livello bilaterale o multilaterale, mediante formulari:

i) per permettere agli Stati membri di consultarsi o informarsi a vicenda quando introducono una segnalazione;

ii) in caso di "hit", al fine di consentire l'azione appropriata;

iii) quando non è possibile procedere all'azione richiesta;

iv) con riguardo alla qualità dei dati SIS II;

v) con riguardo alla compatibilità e alla priorità delle segnalazioni;

vi) con riguardo ai diritti di accesso.

---

8 Cfr. Convenzione di applicazione dell'accordo di Schengen, GU L 239 del 22.9.2000.

9 Cfr. decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II), GU L 205 del 7.8.2007, pag. 63.

Le informazioni devono essere scambiate conformemente alle disposizioni del manuale SIRENE[10] e per il tramite dell'infrastruttura di comunicazione.[11] SIS II[12] dispone di funzionalità migliorate rispetto al suo predecessore, come la possibilità di inserire impronte digitali, e fotografie, nonché nuovi tipi di oggetti rubati (aeromobili, natanti, container, mezzi di pagamento) e la possibilità, per il titolare della segnalazione, di creare connessioni fra le segnalazioni. SIS II contiene copie dei mandati di arresto europei allegate direttamente alle segnalazioni delle persone interessate.

Gli uffici SIRENE facilitano la cooperazione su questioni di polizia e possono anche svolgere un ruolo nello scambio di informazioni al di fuori dell'ambito del SIS II in virtù delle disposizioni precedentemente comprese negli articoli 39 e 46 della convenzione di applicazione dell'accordo di Schengen (CAS), che sono state sostituite dalla **"decisione quadro svedese"**. A norma dell'articolo 12, paragrafo 1, della "decisione quadro svedese", le disposizioni dell'articolo 39, paragrafi 1, 2 e 3, e dell'articolo 46 della CAS sono sostituite dalle disposizioni della decisione quadro nella misura in cui riguardano lo scambio di informazioni e di analisi (intelligence) ai fini dello svolgimento di indagini o di operazioni di intelligence criminale da essa previsto.

1.3. Unità nazionale Europol (UNE)

Ogni Stato membro dispone di un'unità nazionale Europol (UNE) designata che costituisce l'organo di collegamento tra Europol e le autorità nazionali competenti. Gli ufficiali di collegamento delle UNE distaccati presso Europol dovrebbero assicurare un collegamento in tempo reale, 24 ore su 24 e 7 giorni su 7, tra la sede centrale di Europol all'Aia e le UNE presenti nei 28 Stati membri. Europol ospita inoltre ufficiali di collegamento di 10 paesi non UE e organizzazioni. La rete è supportata da canali di comunicazione sicuri forniti da Europol.

---

10 Decisione di esecuzione della Commissione, del 26 febbraio 2013, riguardante il manuale Sirene e altre disposizioni di attuazione per il sistema d'informazione Schengen di seconda generazione (SIS II) [notificata con il numero C(2013) 1043], GU L 71 del 14.3.2013, pag. 1.

11 A causa della chiusura della rete di posta SISnet, gli uffici SIRENE possono ora utilizzare il servizio di posta sTESTA. Altri scambi di informazioni possono svolgersi tramite i canali di comunicazione della rete sTESTA, di SIENA o di I-24/7.

12 Relazione della Commissione al Parlamento europeo e al Consiglio sulla valutazione del sistema d'informazione Schengen di seconda generazione (SIS II) ai sensi dell'articolo 24, paragrafo 5, dell'articolo 43, paragrafo 3, e dell'articolo 50, paragrafo 5, del regolamento (CE) n. 1987/2006 e ai sensi dell'articolo 59, paragrafo 3, e dell'articolo 66, paragrafo 5, della decisione 2007/533/GAI; 15810/16 SIRIS 175 COMIX 860

Europol[13] sostiene le autorità di contrasto degli Stati membri nella prevenzione e nella lotta contro la criminalità organizzata, le forme gravi di criminalità internazionale e il terrorismo laddove siano coinvolti due o più Stati membri. Per raccogliere, conservare, trattare e analizzare dati personali e scambiare informazioni e analisi (intelligence), Europol dipende dai dati forniti dagli Stati membri. Il regolamento Europol stabilisce i diversi compiti d'informazione e le norme relative all'uso dei dati e allo scambio di dati con terzi sulla base di un solido regime di protezione e sicurezza dei dati.

1.4. Uffici centrali nazionali (UCN) INTERPOL

Gli **uffici centrali nazionali (UCN)** presso la sede centrale della polizia nazionale svolgono un ruolo cruciale per quanto riguarda il trattamento, nel sistema d'informazione Interpol, dei dati forniti dai loro paesi. Essi sono autorizzati ad accedere direttamente al sistema, tra l'altro a fini di:

- registrazione, aggiornamento e cancellazione di dati direttamente nelle banche dati di polizia dell'organizzazione, nonché creazione di collegamenti fra dati;
- consultazione diretta di tali banche dati;
- uso di avvisi e circolari di Interpol per la trasmissione di richieste di cooperazione e di segnalazioni internazionali.

Gli UCN possono effettuare rapidamente ricerche e controlli incrociati di dati con un accesso diretto, 24 ore su 24 e 7 giorni su 7, a banche dati contenenti informazioni su persone sospettate di terrorismo, persone ricercate, impronte digitali, profili DNA, documenti di viaggio smarriti o rubati, veicoli a motore rubati, opere d'arte rubate, ecc.

[13] Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI, GU L 135 del 24.5.2016, pag. 53 (applicabile a decorrere dal 1º maggio 2017).

Per quanto possibile, gli UCN dovrebbero consentire alle autorità di polizia giudiziaria dei rispettivi paesi coinvolte nella cooperazione internazionale di polizia di accedere al sistema d'informazione Interpol. Essi controllano il livello di accesso di altri utenti autorizzati dei loro paesi ai servizi Interpol e possono chiedere di essere informati in merito alle ricerche effettuate nelle loro banche dati nazionali da altri paesi.

1.5. Punti di contatto nazionali "Prüm"

Le "decisioni di Prüm"[14] hanno aperto una nuova dimensione transfrontaliera della lotta alla criminalità prevedendo il reciproco accesso in linea transfrontaliero a banche dati nazionali designate del DNA, ai sistemi automatizzati di identificazione delle impronte digitali (AFIS) e alle banche dati contenenti i dati di immatricolazione dei veicoli. Per la fornitura di dati, in ogni Stato membro partecipante[15] è designato uno specifico punto di contatto nazionale per ogni tipo di scambio di dati. Le disposizioni in materia di protezione dei dati e quelle appositamente previste per la sicurezza dei dati tengono in particolare considerazione la specificità dell'accesso in linea a queste banche dati. La fornitura di dati personali richiede un adeguato livello di protezione e sicurezza dei dati che sia reciprocamente testato e concordato dagli Stati membri prima che sia avviato lo scambio.

1.5.1. Punti di contatto nazionali "Prüm" - DNA e impronte digitali

Nel caso di dati sul DNA e sulle impronte digitali, il raffronto automatizzato di dati indicizzati biometrici si basa su un sistema di risconto positivo o negativo ("hit/no hit"). I dati indicizzati non consentono l'immediata identificazione della persona interessata. In caso di "hit", il punto di contatto nazionale dello Stato membro che effettua la ricerca può dunque chiedere ulteriori dati personali specifici. La fornitura di tali dati supplementari deve essere richiesta mediante procedure di assistenza reciproca, comprese quelle adottate ai sensi della "decisione quadro svedese", ed è disciplinata dalla legislazione nazionale dello Stato membro richiesto, ivi incluse le norme relative all'assistenza giudiziaria.

---

14 Decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, GU L 210 del 6.8.2008, pag. 1. Decisione 2008/616/GAI del Consiglio, del 23 giugno 2008, relativa all'attuazione della decisione 2008/615/GAI sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, GU L 210 del 6.8.2008, pag. 12.

15 5010/15 JAI 1 DAPIX 1 ENFOPOL 1 CRIMORG 1.

1.5.1.1. Linee guida sulle migliori pratiche per la ricerca di impronte digitali

Qualora utilizzi il sistema automatizzato "Prüm" di ricerca delle impronte digitali, lo Stato membro richiedente dovrebbe seguire le raccomandazioni formulate nel documento *Good Practices for consulting Member States' databases* (Buone prassi per la consultazione delle banche dati degli Stati membri) (doc. 14885/1/08 REV 1), il quale riconosce le capacità di ricerca limitate delle **banche dati dattiloscopiche** e raccomanda la promozione, a livello operativo, delle seguenti prassi:

- l'opportunità di consultare o meno banche dati di impronte digitali degli Stati membri e l'ordine in cui tali consultazioni sono effettuate e ripetute costituiscono decisioni investigative prese caso per caso e non dovrebbero essere sistematicamente predeterminati;
- in linea di principio, non si dovrebbero consultare le banche dati di impronte digitali di altri Stati membri finché non siano state consultate quelle dello stesso Stato richiedente;
- la decisione di consultare una o più banche dati degli Stati membri dovrebbe tener conto, in particolare, dei seguenti elementi:
  - la gravità del caso,
  - e/o i filoni d'indagine esistenti, in particolare informazioni che puntino nella direzione di uno Stato membro o un gruppo di Stati membri,
  - e/o le esigenze specifiche dell'indagine;
- si dovrebbe procedere a ricerche generali solo dopo aver seguito tutte le buone prassi di cui ai punti da 1 a 3.

Esempi di scambio automatizzato di dati ai sensi delle decisioni di Prüm del Consiglio

Nel 2011, durante l'indagine su un omicidio, è stato inserito materiale genetico nella banca dati nazionale del DNA della Repubblica ceca. L'indagine era condotta nei confronti di un sospetto che era fuggito all'estero e il materiale genetico era stato prelevato da un mozzicone di sigaretta trovato in un posacenere nell'appartamento in cui era stato commesso il crimine. Effettuando una ricerca nella banca dati del DNA austriaca nel 2014, si è scoperto che lo stesso profilo era stato trattato in Austria. Gli SPOC di entrambi i paesi si sono scambiati ulteriori dati personali attraverso la cooperazione di polizia. Successivamente, mediante l'assistenza giudiziaria in materia penale, si è contattato il dipartimento di giustizia penale austriaco e lo si è invitato a consegnare il sospetto alla Repubblica ceca al fine di procedere nei suoi confronti.

Nel 2005, durante l'indagine su una rapina, è stato inserito un profilo DNA nella banca dati nazionale del DNA della Repubblica ceca. Nel 2014, consultando la banca dati del DNA austriaca è stato identificato un sospetto. La parte austriaca è stata invitata a trasmettere una foto attuale e altri dati personali tramite gli SPOC.

1.5.2. Punto di contatto nazionale "Prüm" - Dati di immatricolazione dei veicoli

Per quanto riguarda i dati di immatricolazione dei veicoli, le ricerche possono essere effettuate con un numero completo di telaio in uno o in tutti gli Stati membri partecipanti, o con un numero completo di immatricolazione in un determinato Stato membro. Le informazioni saranno scambiate dai punti di contatto nazionali designati sia per le richieste in entrata che per quelle in uscita. Gli Stati membri si concedono reciprocamente l'accesso in linea ai dati nazionali di immatricolazione dei veicoli per ottenere:

a) i dati relativi ai proprietari o agli utenti, e

b) i dati relativi ai veicoli.

Per effettuare tali ricerche, gli Stati membri utilizzano una versione dell'applicazione software del sistema europeo d'informazione sui veicoli e le patenti di guida (EUCARIS) appositamente progettata per le finalità della decisione di Prüm. Le ricerche relative ai dati di immatricolazione dei veicoli differiscono da quelle relative al DNA e alle impronte digitali poiché in caso di "hit" producono sia dati personali che dati indicizzati. Come per altre consultazioni automatizzate, resta inteso che la trasmissione di dati personali è subordinata all'applicazione di un adeguato livello di protezione dei dati da parte degli Stati membri riceventi.

1.5.3. Punto di contatto nazionale "Prüm" per la prevenzione del terrorismo

Su richiesta o di propria iniziativa, i punti di contatto nazionali designati possono scambiarsi informazioni su persone sospettate di aver commesso reati di terrorismo. I dati comprendono cognome, nome, data e luogo di nascita del sospetto, nonché una descrizione delle circostanze dalle quali deriva la presunzione che l'interessato intenda commettere reati legati ad attività terroristiche.

Lo Stato membro che trasmette i dati può, nel rispetto della legislazione nazionale, fissare le condizioni relative all'utilizzo di tali dati e informazioni da parte dello Stato membro ricevente, il quale è da esse vincolato.

1.5.4. Punti di contatto nazionali "Prüm" per eventi di rilievo

Gli Stati membri che ospitano eventi di rilievo di dimensione internazionale devono garantire la sicurezza dell'evento sia sotto il profilo dell'ordine pubblico che sotto quello dell'antiterrorismo. In funzione della natura dell'evento (politico, sportivo, sociale, culturale o di altro tipo), un profilo può rivelarsi più rilevante dell'altro. Occorre tuttavia prendere in considerazione entrambi gli aspetti, anche se eventualmente trattati da autorità diverse. Un'attenzione particolare è rivolta al fenomeno dei delinquenti violenti itineranti, in particolare per quanto riguarda le partite di calcio internazionali.

Al fine di prevenire reati e mantenere l'ordine e la sicurezza pubblici in relazione a eventi di rilievo e analoghi assembramenti di massa (di natura politica, sportiva, sociale, culturale o di altro tipo), catastrofi e gravi incidenti con ripercussioni transfrontaliere, i punti di contatto nazionali designati si trasmettono, su richiesta o di propria iniziativa:

- dati non personali, o
- dati personali, qualora condanne definitive o altre circostanze facciano presupporre che le persone interessate commetteranno reati in occasione di questi eventi o costituiranno una minaccia per l'ordine e la sicurezza pubblici.

I dati personali possono essere trattati solo ai suddetti fini e per gli eventi specifici per i quali sono stati trasmessi. I dati trasmessi devono essere cancellati immediatamente non appena tali fini siano stati raggiunti e in ogni caso al massimo entro un anno. Le informazioni sono trasmesse conformemente alla legislazione nazionale dello Stato membro che le trasmette.

1.5.4.1. Manuale concernente la cooperazione in occasione di eventi importanti di dimensione internazionale[16]

Il manuale contiene orientamenti e suggerimenti per le autorità di contrasto che hanno il compito di garantire la pubblica sicurezza in occasione di eventi importanti, come i giochi olimpici o altri grandi eventi sportivi, o di eventi sociali o incontri politici di alto livello.

Esso è costantemente modificato e adattato in funzione dell'evoluzione delle migliori pratiche e contiene orientamenti in materia di gestione delle informazioni e degli eventi, nonché di valutazione connessa all'evento e di valutazione strategica. I moduli standard ivi allegati riguardano:

- le richieste di ufficiali di collegamento;
- l'analisi del rischio riguardo a manifestanti potenziali ed altri gruppi;
- lo scambio di informazioni sulle persone che costituiscono una minaccia terroristica;
- un elenco di testi di riferimento;
- una tabella contenente punti di contatto permanenti in materia di ordine pubblico.

1.6. Punti nazionali (di polizia) d'informazione sul calcio[17]

Oltre al punto di contatto nazionale "Prüm" per eventi di rilievo e con particolare riferimento alle partite di calcio internazionali, in ogni Stato membro un punto nazionale d'informazione sul calcio è incaricato di scambiare informazioni pertinenti e di sviluppare una cooperazione di polizia transfrontaliera. Il punto nazionale d'informazione sul calcio può utilizzare a fini propri o trasmettere alle autorità o ai servizi di polizia competenti informazioni tattiche, strategiche e operative.

Il coordinamento e, laddove necessario, l'organizzazione dei contatti tra i servizi di polizia dei diversi paesi coinvolti in un evento sono affidati al punto nazionale d'informazione sul calcio. Il sito web del Centro informazioni sul teppismo negli stadi (CIV) per i punti nazionali d'informazione sul calcio (www.nfip.eu) diffonde informazioni e indicazioni utili sulle opzioni giuridiche e di altro genere disponibili per quanto concerne la sicurezza in occasione delle partite di calcio.

---

16 Raccomandazione 2007/C 314/02 del Consiglio, del 6 dicembre 2007, relativa a un manuale per le autorità di polizia e di sicurezza concernente la cooperazione in occasione di eventi importanti di dimensione internazionale, GU C 314 del 22.12.2007, pag. 4.

17 Decisione 2002/348/GAI del Consiglio, del 25 aprile 2002, concernente la sicurezza in occasione di partite di calcio internazionali, GU L 121 dell'8.5.2002, pag. 1.

Il punto nazionale d'informazione sul calcio coordina il trattamento di informazioni sui tifosi ad alto rischio al fine di predisporre e adottare misure appropriate per il mantenimento dell'ordine pubblico in occasione di un evento calcistico. Dette informazioni includono, in particolare, dati su persone che rappresentano una minaccia reale o potenziale per l'ordine e la sicurezza pubblici. Le informazioni dovrebbero essere scambiate mediante i formulari[18] contenuti nell'appendice del manuale per il calcio.

1.6.1. Il manuale per il settore calcistico[19]

Il manuale per il settore calcistico è allegato alla risoluzione 2016/C 444/01 del Consiglio e fornisce esempi di come la polizia dovrebbe cooperare a livello internazionale al fine di prevenire e combattere la violenza e i disordini in occasione delle partite di calcio. Il contenuto è costituito, in particolare, da raccomandazioni riguardanti:

- la gestione delle informazioni da parte delle forze di polizia;
- l'organizzazione della cooperazione tra forze di polizia;
- un elenco di controllo per la politica in materia di media e la strategia di comunicazione (polizia/autorità).

---

18 Decisione 2007/412/GAI del Consiglio, del 12 giugno 2007, che modifica la decisione 2002/348/GAI concernente la sicurezza in occasione di partite di calcio internazionali, GU L 155 del 15.6.2007, pag. 76.

19 Risoluzione del Consiglio concernente un manuale aggiornato di raccomandazioni per la cooperazione internazionale tra forze di polizia e misure per prevenire e combattere la violenza e i disordini in occasione delle partite di calcio di dimensione internazionale alle quali è interessato almeno uno Stato membro ("manuale UE per il settore calcistico" (2016/C 444/01), GU C 444 del 29.11.2016, pag. 1.

1.7. Punti focali nazionali Armi da fuoco (NFFP)

Nel dar seguito al piano d'azione dell'UE del 2 dicembre 2015 (COM(2015) 624 final), la Commissione, sotto il punto "Elaborare un migliore quadro di intelligence", ha invitato tutti gli Stati membri a istituire punti focali nazionali interconnessi in materia di armi da fuoco per sviluppare le competenze e migliorare l'analisi e la stesura strategica di relazioni sul traffico illecito di armi da fuoco, in particolare attraverso l'uso combinato dell'intelligence balistica e criminale.

La strategia dell'Unione europea contro le armi da fuoco, le armi leggere e le armi di piccolo calibro illegali e le relative munizioni "Mettere in sicurezza le armi, proteggere i cittadini"[20] afferma al punto "Rispetto delle norme attraverso il monitoraggio e le attività di contrasto -cooperazione operativa-" che "l'Unione migliorerà la cooperazione transfrontaliera tra le autorità giudiziarie e di contrasto, incoraggerà le competenti autorità degli Stati membri, comprese le autorità doganali, a istituire punti focali nazionali sulle armi da fuoco, a produrre migliori analisi di tutte le informazioni disponibili nel settore delle armi da fuoco illegali e a garantire la piena partecipazione allo scambio di informazioni con Europol nel settore del traffico delle armi da fuoco". Ciò è stato approvato dal Consiglio che ne ha fatto una vera e propria strategia dell'Unione europea.[21]

La rete dei punti focali nazionali Armi da fuoco (NFFP) raccoglie, analizza e migliora il flusso di informazioni sull'uso delle armi da fuoco a fini criminali e sul loro traffico illegale verso gli Stati membri e all'interno degli stessi e attraverso tutta l'UE a livello strategico e operativo mediante una raccolta e una condivisione coordinate delle informazioni per migliorare il quadro di intelligence e informare meglio i servizi di contrasto. Le informazioni dovrebbero essere scambiate conformemente agli orientamenti sulle migliori prassi dei responsabili EMPACT in materia di armi da fuoco e degli esperti europei in materia di armi da fuoco (EFE).

---

20 JOIN(2018) 17 final, dell'1.6.2018.

21 Conclusioni del Consiglio del 19 novembre 2018 - Documento 13581/18.

1.7.1. Orientamenti sulle migliori prassi in materia di NFFP

Gli orientamenti sulle migliori prassi[22] per la creazione di NFFP forniscono esempi sul modo in cui i punti focali nazionali Armi da fuoco dovrebbero svolgere i seguenti compiti:

- creare un archivio per l'intelligence criminale e balistica in materia di armi da fuoco,
- creare un archivio per tutte le armi da fuoco smarrite, rubate e recuperate,
- tracciare tutte le armi da fuoco sequestrate, dal fabbricante fino all'ultimo legittimo proprietario,
- analizzare i dati sulle armi da fuoco tracciate per individuarne il tipo, la marca, il modello, il calibro e il paese di fabbricazione,
- fornire dati, statistiche, informazioni, valutazioni e relazioni da usare all'interno degli Stati membri,
- fungere da punto di contatto tecnico con l'UNODC,
- soddisfare i requisiti del questionario delle Nazioni Unite sui flussi illeciti (UN-IAQF),
- promuovere la cooperazione internazionale.

Grazie all'accesso alle pertinenti banche dati, tra cui il sistema d'informazione Europol (SIE), il sistema d'informazione Schengen (SIS2) e iARMS, e in linea con gli orientamenti sulle migliori prassi, i punti focali nazionali Armi da fuoco sarebbero in grado di avviare e di assicurare lo scambio di informazioni, di trattare le domande di ricerca interne e in entrata, di sostenere e coordinare le azioni operative mantenendo nel contempo un controllo sufficiente dell'intelligence, dei dati e delle informazioni a livello nazionale così da consentire la tempestiva e regolare trasmissione di tali dati a Europol e ad altri organi e autorità di contrasto, come l'UNODC.

[22] 8586/18

1.8. Centri di cooperazione di polizia e doganale (CCPD)

I CCPD sono istituiti sulla base di accordi bilaterali o multilaterali conformemente all'articolo 39, paragrafo 4, della convenzione di applicazione dell'accordo di Schengen (CAS). In tali accordi, le parti contraenti definiscono la base della loro cooperazione transfrontaliera, compresi i compiti, il quadro giuridico e le procedure istitutive e di funzionamento dei centri. I CCPD riuniscono personale proveniente dai paesi vicini e sono strettamente legati agli organismi nazionali preposti alla cooperazione internazionale (punti di contatto nazionali, UCN Interpol, UNE, uffici SIRENE).

Essi forniscono consulenza e sostegno non operativo alla polizia, alle dogane e ad altri servizi operativi nazionali nella regione di frontiera in cui si trovano. Il personale dei CCPD è incaricato di fornire rapidamente le informazioni richieste in conformità della decisione 2006/960/GAI del Consiglio ("decisione quadro svedese").

Alla fine del 2016, 8 dei 59 CCPD esistenti erano connessi a SIENA, l'applicazione di rete per lo scambio sicuro di informazioni di Europol. Lo scambio di informazioni attraverso i CCPD riguarda principalmente la piccola e media criminalità, i flussi d'immigrazione clandestina e i problemi di ordine pubblico. Può trattarsi di informazioni concernenti l'identificazione di conducenti o l'accertamento dell'idoneità e dell'autenticità di documenti d'identità e di viaggio.

Le parti contraenti possono convenire di trasformare un CCPD in un centro operativo di coordinamento regionale a disposizione di tutti i servizi interessati, segnatamente in caso di incidenti di portata regionale (catastrofi naturali) o di eventi di rilievo (giochi olimpici, campionato mondiale di calcio, ecc.).

Se riceve informazioni di competenza dell'unità centrale nazionale, il CCPD è tenuto a trasmetterle senza indugio allo SPOC o all'unità centrale. Qualora il CCPD riceva informazioni di palese interesse per Europol, le può trasmettere all'UNE situata presso lo SPOC, il quale le inoltra a Europol.

Esempio di scambio di informazioni attraverso un CCPD

EPICC (Euregio Police Information and Cooperation Centre - Centro di cooperazione e informazione di polizia euregionale) è l'acronimo del CCPD Heerlen.

È stato creato ad hoc (senza uno specifico strumento giuridico) nel 2005 su iniziativa della NeBeDeAgPol, un'associazione di capi di polizia dell'eurregione Mosa-Reno, situata nella regione di frontiera tra Paesi Bassi, Belgio e Germania, una delle zone frontaliere più densamente popolate dell'Unione europea.

In questo CCPD circa trenta agenti di polizia belgi, tedeschi e olandesi lavorano insieme su un'unica piattaforma.

Detti agenti dispongono di un accesso in loco alla maggior parte dei contenuti delle banche dati dei rispettivi paesi, il che consente loro di fornire, entro un tempo brevissimo, risposte precise, complete e attendibili alle richieste di informazioni da parte della polizia riguardanti Belgio, Germania o Paesi Bassi. Lo scambio di informazioni tra le tre delegazioni di EPICC avviene tramite l'applicazione SIENA di Europol.

EPICC raccoglie e analizza le informazioni di polizia disponibili nella regione di frontiera al fine di individuare, descrivere e seguire problemi di sicurezza alle frontiere (nuovi fenomeni o modalità operative, bande di criminali che agiscono nella regione di frontiera, eventi o persone che richiedono una particolare attenzione, ecc.).

Grazie alle sue speciali competenze e alla sua composizione mista, il CCPD Heerlen può fornire un sostegno efficiente durante la preparazione e l'esecuzione di operazioni, indagini o misure di sorveglianza transfrontaliere.

1.9. Ufficiali di collegamento

Ai sensi dell'articolo 47 della convenzione di applicazione dell'accordo di Schengen (CAS), gli Stati membri "*possono concludere accordi bilaterali che consentono il distacco, a tempo determinato o indeterminato, di funzionari di collegamento di un[o] [Stato membro] presso i servizi di polizia dell'altr[o] [Stato membro]*". Il ruolo degli ufficiali di collegamento è stabilire e mantenere contatti diretti per favorire e accelerare la cooperazione ai fini della lotta alla criminalità, in particolare fornendo assistenza. Gli ufficiali di collegamento non hanno il potere di eseguire autonomamente misure di polizia. Essi garantiscono una cooperazione rapida ed efficace basata sul contatto personale e sulla fiducia reciproca:

- facilitando e accelerando la raccolta e lo scambio di informazioni;
- eseguendo le richieste di mutua assistenza giudiziaria e fra polizie in materia penale;
- organizzando e assicurando operazioni transfrontaliere.

Gli ufficiali di collegamento possono essere distaccati presso altri Stati membri, paesi terzi, agenzie dell'UE o organizzazioni internazionali. Il compendio[23] sugli ufficiali di collegamento dei servizi di contrasto, aggiornato annualmente dal segretariato generale del Consiglio, illustra il lavoro e i compiti degli ufficiali di collegamento e contiene elenchi di ufficiali di collegamento con i relativi estremi.

Sulla base delle esperienze passate e in corso in vari paesi ospitanti e al fine di conseguire una maggiore messa in comune delle attività degli Stati membri nei confronti dei paesi terzi per quanto riguarda sia il lavoro degli ufficiali di collegamento che la cooperazione tecnica, sono state individuate alcune buone prassi, che sono riportate nel compendio. Si propone che gli ufficiali di collegamento degli Stati membri e le loro autorità competenti le applichino ogniqualvolta sia opportuno.

---

[23] "*Update of the Compendium on law enforcement liaison officers (2018)*" (Aggiornamento del compendio sugli ufficiali di collegamento dei servizi di contrasto 2018), doc. 10095/1/18 REV 1 ENFOPOL 397 JAIEX 84 COMIX 422.

Esempi tipici di scambio di informazioni tra ufficiali di collegamento

- *Gli ufficiali di collegamento possono essere incaricati di assicurare i contatti al fine di stabilire una cooperazione diretta in casi specifici, come i reati connessi agli stupefacenti.*
- *Gli ufficiali di collegamento possono fornire informazioni specifiche sulle norme e la legislazione nazionali in materia di cooperazione internazionale di polizia o di assistenza giudiziaria in materia penale.*
- *In alcuni casi, gli ufficiali di collegamento tengono aggiornati elenchi delle autorità competenti del loro Stato membro.*
- *In alcuni Stati membri, gli ufficiali di collegamento hanno anche il compito di trattare le richieste di cooperazione ai sensi dell'articolo 17 della decisione di Prüm (operazioni congiunte). Ad esempio, l'ufficiale di collegamento danese presso Europol è stato invitato dalla Repubblica ceca a trasmettere una richiesta alla Danimarca ai fini dell'assegnazione di 4 agenti di polizia danesi per fornire assistenza in un caso che coinvolgeva entrambi gli Stati membri.*

1.10. Uffici degli Stati membri per il recupero dei beni (URB)

La criminalità finanziaria include un'ampia gamma di attività quali la contraffazione, la corruzione e la frode (ad esempio la frode con carta di credito, lo stellionato, la frode medica, la contraffazione di bolli, la corruzione o l'appropriazione indebita, il riciclaggio, il furto d'identità e l'evasione fiscale). Si raggiunge una migliore cooperazione tramite una collaborazione transfrontaliera più stretta tra gli uffici per il recupero dei beni (URB), le unità di informazione finanziaria (FIU) e le autorità di polizia e doganali[24].

[24] Manuale delle migliori pratiche nella lotta contro la criminalità finanziaria: una raccolta di buoni esempi di sistemi ben sviluppati negli Stati membri per combattere la criminalità finanziaria, 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144.

In seguito all'adozione della decisione 2007/845/GAI del Consiglio, del 6 dicembre 2007, concernente la cooperazione tra gli uffici degli Stati membri per il recupero dei beni nel settore del reperimento e dell'identificazione dei proventi di reato o altri beni connessi[25], tutti gli Stati membri hanno istituito e designato uffici per il recupero dei beni (URB). Tali unità specializzate si sono evolute in una stretta rete di specialisti che possono scambiarsi direttamente informazioni su questioni relative al recupero dei beni tramite il sistema SIENA. Sotto l'egida della Commissione europea e di Europol, la rete degli URB facilita la cooperazione tra gli URB degli Stati membri, la discussione strategica e lo scambio di migliori pratiche. L'Ufficio Europol per i proventi criminali (Europol Criminal Assets Bureau - ECAB) funge da punto focale per il recupero dei beni nell'UE.

Le disposizioni di cui alla direttiva 2014/42/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa al congelamento e alla confisca dei beni strumentali e dei proventi da reato nell'Unione europea[26] miglioreranno ulteriormente l'efficacia della cooperazione tra gli uffici per il recupero dei beni nell'Unione europea. Gli Stati membri sono tenuti a recepire la direttiva entro il 4 ottobre 2016.

La **rete interagenzie Camden per il recupero dei beni (CARIN)**, istituita nel 2004 per sostenere l'identificazione, il congelamento, il sequestro e la confisca a livello transfrontaliero dei beni connessi a reati, promuove lo scambio reciproco di informazioni relative ai diversi approcci nazionali anche al di là dell'UE.

Dal 2015 la rete CARIN include operatori di 53 giurisdizioni e 9 organizzazioni internazionali che fungono da punti di contatto ai fini del rapido scambio di informazioni a livello transfrontaliero, su richiesta o spontaneamente. Gli URB nazionali cooperano tra loro o con le altre autorità che facilitano il reperimento e l'identificazione dei proventi di reato. Sebbene tutti gli Stati membri abbiano istituito un URB, tra essi esistono notevoli differenze in termini di assetto organizzativo, risorse e attività.

---

25 Decisione 2007/845/GAI del Consiglio, del 6 dicembre 2007, concernente la cooperazione tra gli uffici degli Stati membri per il recupero dei beni nel settore del reperimento e dell'identificazione dei proventi di reato o altri beni connessi, GU L 332 del 18.12.2007, pag. 103.

26 Direttiva 2014/42/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa al congelamento e alla confisca dei beni strumentali e dei proventi da reato nell'Unione europea, GU L 127 del 29.4.2014, pag. 39.

Le informazioni scambiate possono essere utilizzate in conformità delle disposizioni in materia di protezione dei dati dello Stato membro ricevente e sono soggette a norme di protezione dei dati identiche a quelle applicabili se fossero raccolte nello Stato membro ricevente. Occorre promuovere lo scambio spontaneo di informazioni in linea con la presente decisione, applicando le procedure e le tempistiche previste dalla decisione quadro svedese.

1.11. Riciclaggio - Cooperazione tra unità di informazione finanziaria (FIU)[27] [28]

Le informazioni pertinenti su qualsiasi fatto che possa rappresentare un indizio di riciclaggio o di finanziamento del terrorismo dovrebbero essere riferite alle unità di informazione finanziaria (FIU) nazionali. Le FIU analizzano le informazioni ricevute caso per caso, allo scopo di individuare le connessioni tra le operazioni sospette e l'attività criminosa sottostante per prevenire e combattere il riciclaggio e il finanziamento del terrorismo. Le FIU fungono da unità nazionale centrale per la ricezione, l'analisi e l'inoltro alle autorità competenti dei risultati delle proprie analisi. Indipendenti e autonome a livello operativo, le FIU svolgono le proprie funzioni liberamente, incluse quelle di decidere in modo autonomo di analizzare, richiedere e comunicare informazioni specifiche.

Le FIU fungono altresì da punti di contatto nazionali per lo scambio di informazioni a livello transfrontaliero. Analogamente alle agenzie per il recupero dei beni, variano considerevolmente da uno Stato membro all'altro per quanto concerne l'assetto organizzativo, le funzioni e le risorse. Sono poste sotto l'egida di autorità giudiziarie, in seno a organi di polizia oppure sono create come "ibridi", con una combinazione di competenze della polizia e della magistratura. Talvolta questa diversità può intralciare la cooperazione internazionale.

---

27 Direttiva (UE) 2019/1153 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati e che abroga la decisione 2000/642/GAI del Consiglio, GU L 186 dell'11.7.2019, pag. 122.

28 Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 658/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione, GU L 141 del 5.6.2015, pag. 73.

Tuttavia, tenendo conto della natura transnazionale del riciclaggio e del finanziamento del terrorismo, il coordinamento e la cooperazione tra le FIU sono estremamente importanti. Al fine di migliorare tali coordinamento e cooperazione e, in particolare, per assicurare che le segnalazioni delle operazioni sospette pervengano alla FIU dello Stato membro in cui la segnalazione sarebbe più utile, nella direttiva (UE) 2015/849 sono stabilite norme dettagliate. Nell'ottica di fornire in maniera rapida, costruttiva ed efficace la massima cooperazione transfrontaliera possibile, gli Stati membri dovrebbero in particolare provvedere affinché le loro FIU scambino informazioni liberamente, spontaneamente o su richiesta, con le unità di informazione finanziaria dei paesi terzi.

È importante migliorare lo scambio di informazioni tra le FIU dell'Unione e utilizzare strutture protette, in particolare la rete informatica decentralizzata FIU.NET. Tutte le 28 FIU sono connesse alla rete FIU.NET. Negli ultimi anni, da strumento di base sicuro per lo scambio bilaterale strutturato di informazioni, si è trasformata in uno strumento sicuro multifunzionale per lo scambio multilaterale di informazioni, con funzionalità di gestione dei fascicoli nonché una standardizzazione semiautomatica dei processi. Su FIU.NET ogni nuova caratteristica e ogni nuovo processo automatizzato sono opzionali e non soggetti a condizioni. Le singole FIU possono decidere quali possibilità e caratteristiche offerte da FIU.NET utilizzare; ricorrono soltanto alle caratteristiche che ritengono convenienti ed escludono quelle di cui non hanno bisogno o che non desiderano utilizzare.

1.12. Convenzione di Napoli II[29]

Gli Stati membri si assistono reciprocamente nel quadro della convenzione di Napoli II al fine di prevenire e accertare le violazioni delle disposizioni doganali nazionali nonché perseguire e punire le violazioni delle disposizioni doganali comunitarie e nazionali. Per quanto concerne le indagini penali, la convenzione introduce procedure che consentono alle amministrazioni doganali di agire in comune e di scambiarsi dati, spontaneamente o su richiesta, relativi ai traffici illeciti.

Le domande sono presentate per iscritto in una delle lingue ufficiali dello Stato membro dell'autorità richiesta o in una lingua concordata con quest'ultima. In un formulario è definita la norma per la comunicazione delle informazioni. Le autorità interessate comunicano tutte le informazioni che possono fornire assistenza alla prevenzione, all'accertamento e al perseguimento delle violazioni. Si scambiano dati personali, vale a dire qualsiasi informazione concernente una persona fisica identificata o identificabile.

---

29 Atto del Consiglio, del 18 dicembre 1997, che stabilisce la convenzione, in base all'articolo K.3 del trattato sull'Unione europea, relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali, GU C 24 del 23.1.1998, pag. 1.

Nell'assistenza da fornire, l'autorità richiesta o l'autorità competente cui quest'ultima si rivolge procede come se agisse per conto proprio o su richiesta di un'altra autorità del proprio Stato membro.

Il prontuario della convenzione relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali (convenzione di Napoli II) si divide in tre parti, che contengono:

- le disposizioni generali (doc. 13615/05 ENFOCUSTOM 61 + COR 1 (CZ));
- le schede nazionali aggiornate al 2016 (doc. 15429/16 JAI 1082 ENFOCUSTOM 238);
- gli allegati, compresi i formulari standard per la comunicazione di informazioni (doc. 13615/05 ENFOCUSTOM 61 ADD 1).

1.13. Unità d'informazione sui passeggeri (UIP)

Nell'ambito della direttiva 2016/681[30] ciascuno Stato membro istituisce o designa un'unità d'informazione sui passeggeri (UIP). Tali unità sono competenti in materia di trattamento dei dati sul codice di prenotazione (PNR) ricevuti dai vettori aerei[31] e rappresentano inoltre il principale canale per lo scambio di informazioni tra gli Stati membri e con Europol. Due o più Stati membri possono istituire o designare una stessa autorità che agisca in qualità di UIP comune.

Il trattamento dei dati PNR serve principalmente per la valutazione dei passeggeri aerei allo scopo di identificare quelli da sottoporre a ulteriore verifica da parte delle autorità nazionali competenti a fini di prevenzione, accertamento, indagine e perseguimento di reati di terrorismo e altri reati gravi. La direttiva si applica ai voli extra-UE e, se uno Stato membro lo decide, può essere applicata anche ai voli intra-UE.

---

30 Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, GU L 119 del 4.5.2016, pag. 132.

31 La direttiva non pregiudica la possibilità che gli Stati membri istituiscano, ai sensi del diritto nazionale, un sistema di raccolta e trattamento dei dati PNR provenienti da operatori economici diversi dai vettori aerei, come le agenzie di viaggio e gli operatori turistici, che forniscono servizi connessi ai viaggi, fra cui la prenotazione di voli per i quali raccolgono e trattano dati PNR, o da imprese di trasporto diverse da quelle previste nella direttiva, purché tale diritto nazionale sia conforme al diritto dell'Unione.

La valutazione dei dati PNR facilita l'identificazione di persone mai sospettate di reati di terrorismo o di altri reati gravi prima di tale valutazione. In linea con la politica dell'UE in materia di protezione dei dati, il trattamento di tali dati dovrebbe essere pertinente e necessario, nonché proporzionato agli obiettivi specifici di sicurezza perseguiti dalla direttiva.

Le UIP sono incaricate:

- a livello nazionale, di raccogliere i dati PNR presso i vettori aerei, conservare, trattare e trasferire tali dati, o i risultati del trattamento, alle autorità nazionali competenti;
- a livello dell'Unione, di scambiare i dati PNR e i risultati del trattamento di tali dati

    a) tra di loro; tuttavia, in casi di emergenza e a determinate condizioni, le sopracitate autorità nazionali competenti possono chiedere all'UIP di un altro Stato membro di trasmettere loro direttamente dati PNR conservati nella sua banca dati; e

    b) con Europol che, entro i limiti delle sue competenze e per l'adempimento dei suoi compiti, ha diritto di chiedere tali dati alle UIP.

Le UIP svolgono i loro compiti esclusivamente in un luogo sicuro all'interno del territorio di uno Stato membro. I dati PNR forniti alle UIP devono essere conservati in una banca dati per un periodo di cinque anni dal loro trasferimento all'UIP dello Stato membro di arrivo o di partenza. A sei mesi dal trasferimento, tuttavia, tutti i dati PNR devono essere resi anonimi mediante mascheratura degli elementi dei dati definiti dalla direttiva e che potrebbero servire a identificare direttamente l'interessato. I risultati del trattamento sono conservati presso l'UIP soltanto per il tempo necessario a informare le pertinenti autorità nazionali competenti e le UIP di altri Stati membri di un riscontro positivo.

L'UIP tratta solo i dati elencati nell'allegato I della direttiva ai fini di:

- valutare i passeggeri prima dell'arrivo previsto nello Stato membro o della partenza prevista dallo Stato membro per identificare quelli da sottoporre a ulteriore verifica da parte delle autorità nazionali e, se richiesto, di Europol;

- rispondere, caso per caso, a una richiesta da parte delle autorità competenti di trasmettere e trattare dati PNR in casi specifici, e di comunicare i risultati di tale trattamento alle stesse autorità competenti o, se del caso, a Europol;

- analizzare i dati PNR per aggiornare i criteri esistenti o definire nuovi criteri da applicare al fine di identificare i passeggeri che potrebbero essere implicati in reati di terrorismo o in altri reati gravi.

Nell'effettuare tali valutazioni, l'UIP può confrontare i dati PNR rispetto a banche dati pertinenti a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e di altri reati gravi e conformemente alle norme dell'Unione, internazionali e nazionali applicabili a tali banche dati oppure può trattare i dati PNR sulla base di criteri prestabiliti. Tali criteri prestabiliti devono essere mirati, proporzionati e specifici. Spetta alle UIP stabilire, e rivedere regolarmente, tali criteri in cooperazione con le pertinenti autorità competenti. I criteri non devono essere basati su dati personali sensibili quali l'origine razziale o etnica, le opinioni politiche, la religione o le convinzioni filosofiche, l'appartenenza sindacale, lo stato di salute, la vita sessuale o l'orientamento sessuale.

Con riguardo alle persone identificate, l'UIP trasmette tutti i dati PNR pertinenti e necessari o i risultati del loro trattamento alle corrispondenti UIP degli altri Stati membri, le quali trasmetteranno le informazioni ricevute alle rispettive autorità competenti.

Il responsabile della protezione dei dati nominato dall'UIP è incaricato di sorvegliare il trattamento dei dati PNR. Gli interessati hanno il diritto di contattare il responsabile della protezione dei dati, che funge da punto di contatto unico, in merito a tutte le questioni connesse al trattamento dei dati PNR che li riguardano.

Tutti i trasferimenti di dati PNR dai vettori aerei alle UIP devono essere effettuati con un mezzo elettronico che garantisca la sicurezza tecnica. A tal fine, sono definiti a livello dell'UE sia i protocolli comuni che i vettori aerei saranno tenuti a rispettare nel trasferimento dei dati, sia i formati di dati supportati che garantiscano la leggibilità dei dati per tutte le parti interessate[32].

[32] Decisione di esecuzione (UE) 2017/759 della Commissione, del 28 aprile 2017, sui protocolli comuni e i formati dei dati che i vettori aerei devono utilizzare per trasferire i dati PNR alle Unità di informazione sui passeggeri, GU L 113 del 29.4.2017, pag. 48.

1.14. Punti di accesso nazionali dell'EES

Il sistema di ingressi/uscite (EES)[33] mira principalmente a migliorare la gestione delle frontiere esterne dell'Unione ed è utilizzato a tal fine dalle autorità di frontiera e dalle autorità competenti per l'immigrazione e i visti[34]. Il sistema registra elettronicamente l'ora e il luogo di ingresso e di uscita di taluni cittadini di paesi terzi ammessi per un soggiorno di breve durata nel territorio degli Stati membri e calcola la durata del loro soggiorno autorizzato. L'EES è operativo presso le frontiere esterne. Gli Stati membri che applicano integralmente l'*acquis* di Schengen introducono l'EES alle loro frontiere interne con gli Stati membri che non applicano ancora integralmente l'*acquis* di Schengen, indipendentemente dal fatto che l'EES sia o meno operativo in tali Stati membri. Gli Stati membri che non applicano integralmente l'*acquis* di Schengen non introducono funzionalità biometriche.

Oltre alle autorità di frontiera e alle autorità competenti per l'immigrazione e i visti, l'EES può essere consultato, alle condizioni stabilite nel regolamento, anche dalle "autorità designate" nazionali a fini di contrasto e per consentire l'acquisizione di informazioni ai fini delle indagini relative a reati di terrorismo o ad altri reati gravi, compresa l'identificazione degli autori, dei sospettati e delle vittime di tali reati che hanno attraversato le frontiere esterne.

Gli Stati membri designano le autorità che sono autorizzate a consultare l'EES a fini di contrasto. Inoltre, ciascuno Stato membro designa un punto di accesso centrale all'EES. Il punto di accesso centrale è distinto dalle "autorità designate", agisce in modo del tutto indipendente da esse e non dovrebbe ricevere istruzioni dalle stesse in merito al risultato della verifica, vale a dire il procedimento di confronto di serie di dati al fine di verificare la validità di una identità dichiarata, in modo da garantire che tale verifica si svolga in modo indipendente. Solo il personale debitamente autorizzato del punto di accesso centrale è autorizzato ad accedere all'EES.

---

33 Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite (EES) per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011, GU L 327 del 9.12.2017, pag. 20.

34 La Commissione determinerà la data a partire dalla quale l'EES entrerà in funzione una volta soddisfatte le condizioni di cui all'articolo 66 del regolamento (UE) 2017/2226.

Le unità operative in seno alle "autorità designate" sono autorizzate a richiedere l'accesso ai dati dell'EES attraverso i punti di accesso centrale. A tal fine l'unità operativa deve presentare una richiesta motivata in formato elettronico o cartaceo a un punto di accesso centrale per l'accesso ai dati dell'EES. Il punto di accesso centrale verifica se le condizioni di accesso prescritte dal regolamento siano soddisfatte e, in caso affermativo, tratta la richiesta. I dati dell'EES sono quindi trasmessi a un'unità operativa in modo da non compromettere la sicurezza dei dati.

Le condizioni da soddisfare per l'accesso all'EES a fini di contrasto sono le seguenti:

- l'accesso per consultazione è necessario a fini di contrasto;
- l'accesso per consultazione è necessario e proporzionato in un caso specifico;
- esistono prove o ragionevoli motivi per ritenere che la consultazione dei dati dell'EES contribuisca alla prevenzione, all'accertamento o all'indagine di uno dei reati in questione, in particolare laddove sussista il sospetto fondato che la persona sospettata, l'autore o la vittima di un reato di terrorismo o un altro reato grave rientri in una delle categorie contemplate dal regolamento.

Inoltre, l'accesso all'EES come strumento per identificare una persona sospettata, un autore o una vittima di tali reati è consentito quando sono soddisfatte le seguenti condizioni:

- è stata effettuata una precedente interrogazione delle banche dati nazionali;
- nel caso di interrogazioni con impronte digitali, una precedente interrogazione è stata avviata ai sensi della decisione 2008/615/GAI ("decisione Prüm"), qualora i confronti delle impronte digitali siano tecnicamente disponibili e tale interrogazione sia stata effettuata pienamente oppure non sia stata effettuata pienamente entro due giorni dal suo avvio.

In parallelo a una richiesta di consultazione dell'EES può essere presentata una richiesta di consultazione del VIS su uno stesso soggetto interessato conformemente alle condizioni stabilite nella decisione 2008/633/GAI del Consiglio[35].

Infine, l'accesso all'EES come strumento per consultare lo storico dei viaggi o i periodi di soggiorno nel territorio degli Stati membri di una persona sospettata conosciuta, un autore conosciuto o una vittima presunta conosciuta di un reato di terrorismo o altro reato grave è consentito quando i principi di cui sopra sono rispettati.

1.15. Unità nazionale ETIAS[36]

Il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) sostiene[37] lo scambio di informazioni a fini di gestione delle frontiere, di contrasto e di lotta al terrorismo. Scopo dell'ETIAS è determinare l'ammissibilità dei cittadini di paesi terzi esenti dall'obbligo del visto prima che si rechino nello spazio Schengen e prima del loro arrivo ai valichi di frontiera esterni. L'ETIAS rilascia un'autorizzazione ai viaggi, che per sua natura è diversa da un visto ma costituisce una condizione per l'ingresso e il soggiorno, e indica che il richiedente non presenta un rischio per la sicurezza, di immigrazione illegale o un alto rischio epidemico.

L'ETIAS consta degli elementi seguenti:

- il sistema d'informazione dell'ETIAS, compreso l'elenco di controllo ETIAS;
- l'unità centrale ETIAS, che è parte dell'Agenzia europea della guardia di frontiera e costiera;
- le unità nazionali ETIAS.

---

35 Decisione 2008/633/GAI del Consiglio, del 23 giugno 2008, relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi, GU L 218 del 13.8.2008, pag. 129.

36 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, GU L 236 del 19.9.2018, pag. 1.
Regolamento (UE) 2018/1241 del Parlamento europeo e del Consiglio, del 12 settembre 2018, recante modifica del regolamento (UE) 2016/794 ai fini dell'istituzione di un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), GU L 236 del 19.9.2018, pag. 72.

37 La Commissione determinerà la data a partire dalla quale l'ETIAS entrerà in funzione una volta soddisfatte le condizioni di cui all'articolo 88 del regolamento (UE) 2018/1240.

Se dal trattamento automatizzato della domanda emerge una corrispondenza (riscontro positivo) tra i dati contenuti nel fascicolo di domanda e i dati registrati nel sistema d'informazione dell'ETIAS, gli indicatori di rischio specifici o le segnalazioni nei sistemi di informazione dell'UE consultati, l'unità centrale ETIAS è incaricata di verificare tale riscontro positivo e, se la corrispondenza è confermata o persistono dubbi, di avviare il trattamento manuale della domanda nello Stato membro individuato.

Dopodiché spetta all'unità nazionale ETIAS dello Stato membro interessato trattare manualmente la domanda in questione. A tal fine, ha accesso al fascicolo di domanda e agli eventuali fascicoli di domanda collegati, nonché a tutti i riscontri positivi emersi dal trattamento automatizzato. Al termine del trattamento manuale, l'unità nazionale responsabile decide se rilasciare o rifiutare l'autorizzazione ai viaggi, conformemente alle disposizioni del regolamento. A tal fine, l'unita nazionale può richiedere informazioni o documenti aggiuntivi.

L'autorizzazione ai viaggi è rifiutata se il richiedente:

- ha utilizzato un documento di viaggio segnalato come smarrito, rubato, altrimenti sottratto o invalidato nel SIS;
- presenta un rischio per la sicurezza;
- presenta un rischio di immigrazione illegale;
- presenta un alto rischio epidemico;
- è oggetto di una segnalazione inserita nel SIS ai fini del rifiuto d'ingresso o di soggiorno;
- non risponde a una richiesta di informazioni o documenti aggiuntivi o non si presenta al colloquio.

Spetta alle unità nazionali ETIAS esaminare le domande e decidere se rilasciare o rifiutare, annullare o revocare le autorizzazioni ai viaggi. A tal fine, le unità nazionali dovrebbero cooperare tra loro e con Europol per valutare le domande.

Un'unità nazionale può decidere di rifiutare o annullare un'autorizzazione ai viaggi qualora risulti che le condizioni di rilascio della stessa non erano soddisfatte al momento del rilascio, o può decidere di revocare un'autorizzazione ai viaggi qualora risulti che le condizioni di rilascio della stessa non sono più soddisfatte. I richiedenti interessati hanno il diritto di presentare ricorso. I ricorsi devono essere proposti nello Stato membro che ha preso la decisione sul rifiuto, sull'annullamento o sulla revoca e conformemente alla legislazione nazionale di quello Stato membro. L'unità nazionale competente è incaricata di fornire ai richiedenti le informazioni sulla procedura di ricorso.

Le autorità di frontiera competenti ad effettuare verifiche di frontiera ai valichi esterni consultano il sistema centrale ETIAS usando i dati contenuti nella zona a lettura ottica del documento di viaggio. Le autorità competenti in materia di immigrazione sono abilitate a eseguire interrogazioni del sistema centrale ETIAS al fine di accertare o verificare se siano soddisfatte le condizioni d'ingresso o di soggiorno nel territorio degli Stati membri.

Solo in casi specifici e soltanto quando è necessario a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi, le autorità di contrasto designate degli Stati membri sono autorizzate a chiedere la consultazione dei dati personali registrati nel sistema centrale ETIAS. La direttiva (UE) 2016/680 ("direttiva polizia") si applica al trattamento di tali dati personali da parte delle autorità designate degli Stati membri, ai sensi del regolamento ETIAS.

1.16. Interoperabilità

L'obiettivo principale del "pacchetto interoperabilità"[38] è quello di migliorare l'architettura di gestione dei dati dell'Unione per la gestione delle frontiere e la sicurezza allo scopo di agevolare la corretta identificazione delle persone che non sono cittadini europei ma cittadini di paesi terzi. L'interoperabilità tra l'EES (cfr. punto 3.20), il VIS (cfr. punto 3.9), l'ETIAS (cfr. punto 3.21), l'Eurodac (cfr. punto 3.10), il SIS (cfr. punto 3.3) e l'ECRIS-TCN (cfr. punto 3.15.1) mira a fare in modo che tali sistemi di informazione dell'UE si integrino a vicenda. A tal fine saranno istituiti un portale di ricerca europeo (ESP), un servizio comune di confronto biometrico (BMS comune), un archivio comune di dati di identità (CIR) e un rilevatore di identità multiple (MID)[39].

a) Per garantire l'utilizzo sistematico dei suddetti sistemi di informazione dell'UE, le autorità designate autorizzate ad avere accesso ad almeno uno di essi, al CIR e al MID, ai dati Europol o alle banche dati SLTD e TDAWN (cfr. punto 2.4) dovrebbero usare l'ESP, che consente l'interrogazione simultanea di tali sistemi di informazione.

b) L'archivio comune di dati di identità (CIR) crea un fascicolo individuale per ciascuna persona registrata in tali sistemi di informazione e funge da contenitore comune per i dati di identità, i dati del documento di viaggio e i dati biometrici delle persone ivi registrate. Il CIR dovrebbe rientrare nell'architettura tecnica di tali sistemi e fungere da componente comune tra di essi ai fini della conservazione e dell'interrogazione dei dati di identità, dei dati del documento di viaggio e dei dati biometrici che trattano.

---

[38] Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27.
Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85.

[39] La Commissione determinerà la data a partire dalla quale si applicheranno le disposizioni dei regolamenti relativi all'ESP, al BMS comune, al CIR e al MID.

L'accesso al CIR è concesso per fini quali:

- la corretta identificazione delle persone registrate nei sistemi di informazione dell'UE o, se necessario,

- per assistere le autorità di contrasto nelle attività di prevenzione, accertamento e indagine di reati di terrorismo o di altri reati gravi.

Se, per due ragioni diverse, un'autorità di polizia non è in grado di identificare una persona, tale autorità può interrogare il CIR. A tal fine, gli Stati membri autorizzano appositamente le proprie autorità competenti, in virtù della legislazione nazionale, e stabiliscono le procedure, le condizioni e i criteri di tali verifiche. L'interrogazione è effettuata sulla base delle impronte digitali recenti dell'interessato oppure, se ciò non è possibile, sulla base dei suoi dati di identità combinati con i dati del documento di viaggio.

Se dall'interrogazione emerge che nel CIR sono conservati dati relativi all'interessato, l'autorità di polizia ne ottiene cognome, nome, data e luogo di nascita, cittadinanza, genere, nomi precedenti e, ove disponibili, pseudonimi, come pure, ove disponibili, informazioni sui documenti di viaggio. Inoltre, se autorizzata dalla legislazione nazionale, l'autorità di polizia può interrogare il CIR usando dati biometrici, in caso di catastrofe naturale, incidente o attacco terroristico e unicamente ai fini dell'identificazione di persone ignote che non sono in grado di dimostrare la propria identità o resti umani non identificati.

Nell'effettuare interrogazioni a fini di contrasto, in particolare laddove sussista il sospetto che i dati dell'autore presunto o effettivo oppure della vittima di reati di terrorismo o di altri reati gravi siano conservati nei sistemi di informazione, le autorità designate e Europol possono consultare il CIR per sapere se sono conservati dati su una determinata persona. In caso affermativo, in esito alla verifica automatica della presenza di un riscontro positivo nel sistema (la cosiddetta funzione di segnalazione "match/no match"), il CIR fornisce un riferimento al sistema di informazione che contiene i corrispondenti dati. La segnalazione di un riscontro dovrebbe essere utilizzata soltanto per presentare una richiesta di accesso ai sistemi di informazione sottostanti dell'UE; non dovrebbe rivelare i dati personali dell'interessato ma limitarsi a indicare che questi sono conservati in uno dei sistemi.

L'utente finale autorizzato non dovrebbe assumere alcuna decisione sfavorevole all'interessato basandosi unicamente sulla segnalazione di un riscontro positivo. L'accesso dell'utente finale a tale segnalazione è pertanto considerata un'ingerenza molto limitata nel diritto alla protezione dei dati personali dell'interessato, consentendo allo stesso tempo alle autorità designate di richiedere l'accesso ai dati personali in modo più efficace. Il pieno accesso ai dati a fini di contrasto rimane soggetto alle condizioni e procedure previste nel regolamento Eurodac (cfr. punto 2.7).

c) Il rilevatore di identità multiple (MID) crea e conserva i collegamenti tra i dati presenti nei vari sistemi di informazione dell'UE. A fini di contrasto, il MID nel CIR e nel SIS è attivato quando è creata o aggiornata una segnalazione su una persona nel SIS o quando un registro dei dati nell'ECRIS-TCN è creato o modificato. La procedura è avviata unicamente per confrontare i dati disponibili in un sistema di informazione dell'UE con i dati disponibili in un altro sistema di informazione dell'UE. La verifica manuale di identità diverse spetta al rispettivo ufficio SIRENE o alle rispettive autorità centrali.

La Commissione:

- determinerà la data a partire dalla quale si applicheranno le disposizioni dei regolamenti relativi all'ESP, al BMS comune, al CIR e al MID;

- in stretta cooperazione con gli Stati membri, eu-LISA e altre agenzie pertinenti dell'Unione, mette a disposizione un manuale pratico per l'implementazione e la gestione delle componenti dell'interoperabilità. Il manuale pratico fornisce orientamenti tecnici e operativi, raccomandazioni e migliori prassi.

1.17. Scelta del canale – Criteri usati comunemente

In uno Stato membro, lo SPOC[40] svolge un ruolo cruciale nella determinazione del canale più appropriato e pertinente raccogliendo tutte le richieste (sia in entrata che in uscita) gestite dall'unità. In nome dell'efficienza, le autorità nazionali consentono agli inquirenti una notevole autonomia nella scelta del canale ritenuto più appropriato per le indagini. I canali di comunicazione più comunemente usati sono i seguenti:

- SIRENE tramite i punti di contatto per ciascuno Stato Schengen per il SIS
- EUROPOL tramite le unità nazionali Europol / gli ufficiali di collegamento Europol
- INTERPOL tramite gli uffici centrali nazionali presso la sede centrale della polizia nazionale
- Ufficiali di collegamento
- Canali di mutua assistenza utilizzati tra le autorità doganali (Napoli II)
- Canali bilaterali basati su accordi di cooperazione a livello nazionale, regionale e locale (CCPD)

Le norme generali prevedono che una richiesta sia trasmessa soltanto attraverso un canale. Nondimeno, in casi eccezionali, una richiesta può essere trasmessa simultaneamente attraverso diversi canali. In tali casi ciò dovrebbe essere segnalato chiaramente a tutte le parti in modo opportuno. Analogamente, un cambiamento di canale deve essere comunicato a tutte le parti, insieme alla relativa motivazione.

Al fine di evitare sovrapposizioni tematiche o situazioni in cui le richieste sono trasmesse inutilmente più di una volta attraverso diversi canali, il desk officer pertinente (SIS, Europol, Interpol, ufficiale di collegamento bilaterale) nello Stato membro richiedente può determinare la rotta più adatta per una domanda di informazioni sulla base dei seguenti criteri:

---

[40] Linee guida relative ad uno sportello unico, docc. 10492/14 DAPIX 75 ENFOPOL 157 e 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1.

- criteri geografici, cioè la cittadinanza/residenza/origine della persona od oggetto in questione sono noti e la richiesta concerne la comunicazione di informazioni dettagliate (indirizzo, numero telefonico, impronte digitali, DNA, immatricolazione, ecc.);

- criteri tematici, cioè criminalità organizzata, reati gravi, terrorismo; riservatezza/sensibilità; canale utilizzato per richieste precedenti collegate;

- criteri tecnici, cioè la necessità di canali informatici protetti;

- criteri di urgenza, cioè rischio immediato per l'integrità fisica di una persona, perdita immediata di prove, richiesta di operazioni o sorveglianza transfrontaliere urgenti.

2. SISTEMI D'INFORMAZIONE

2.1. Sistema d'informazione Schengen – seconda generazione (SIS II)[41]

Attualmente, il sistema d'informazione Schengen di seconda generazione ("SIS II") è operativo in 26 Stati membri dell'UE nonché nei quattro paesi non membri dell'UE che sono associati alla cooperazione Schengen: Norvegia, Islanda, Svizzera e Liechtenstein. Esso sostiene la cooperazione operativa tra le autorità giudiziarie e di polizia in materia penale. Dal momento che il SIS è sia un sistema di cooperazione di polizia che di controllo delle frontiere, può essere consultato dagli agenti di polizia designati, dalle guardie di frontiera, dagli agenti doganali, dalle autorità competenti per i visti e dalle autorità giudiziarie di tutto lo spazio Schengen[42].

I dati SIS II possono essere consultati (conformemente a rigorose norme in materia di protezione dei dati) 24 ore su 24 e 7 giorni su 7 attraverso punti di accesso presso gli uffici SIRENE, ai punti di controllo delle frontiere, sul territorio nazionale e presso i consolati all'estero. La banca dati registra dati sia su **persone** che su **oggetti** e permette lo scambio dei dati ai fini della prevenzione della criminalità e della lotta all'immigrazione irregolare. Tramite le ricerche online su SIS il funzionario che effettua la consultazione determina rapidamente, su base "hit/no hit", se la persona oggetto di un controllo è citata nella banca dati o no.

---

41 Decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II), GU L 205 del 7.8.2007, pag. 63.

42 Un elenco delle autorità nazionali competenti che godono del diritto di accedere alle segnalazioni è pubblicato ogni anno nella *Gazzetta ufficiale dell'Unione europea*.

I dati sono denominati segnalazioni, le quali contengono solo le informazioni necessarie per identificare una persona o un oggetto e per l'azione da intraprendere. La rete unica di uffici SIRENE nazionali provvede allo scambio di informazioni supplementari conformemente alle disposizioni del manuale SIRENE. Una segnalazione è un insieme di dati che consente alle autorità di identificare persone od oggetti al fine di intraprendere azioni appropriate.

Le segnalazioni su **persone** riguardano sia cittadini dell'UE che cittadini non UE. Esse facilitano misure quali:

– l'arresto a fini di consegna sulla base di un mandato d'arresto europeo o di accordi conclusi tra l'UE e paesi terzi, o a fini di estradizione;

– la ricerca del luogo di soggiorno di persone scomparse;

– inviti a comparire davanti a un tribunale nel contesto di un procedimento penale o dell'esecuzione di una sentenza che preveda la reclusione;

– sorveglianza discreta e controlli specifici a fini di repressione di reati, prevenzione di minacce alla sicurezza pubblica o prevenzione di minacce alla sicurezza nazionale;

– non ammissione sul territorio Schengen per cittadini o stranieri in seguito a una decisione amministrativa o giudiziaria, per motivi di minaccia all'ordine pubblico o alla sicurezza nazionale o per motivi di mancato rispetto delle normative nazionali in materia di ingresso e soggiorno degli stranieri.

Le segnalazioni SIS II su **oggetti** sono inserite a fini di controlli discreti o specifici, di sequestro, di prova in un procedimento penale o di sorveglianza. Tali segnalazioni possono riguardare:

– veicoli, natanti, aeromobili, container;

– armi da fuoco;

– documenti rubati;

– banconote;

– proprietà rubate come opere d'arte, natanti, navi.

Il personale di Europol specificatamente autorizzato ha il diritto, nei limiti del proprio mandato, di accedere e consultare direttamente i dati inseriti nel SIS II e può chiedere ulteriori informazioni allo Stato membro interessato.

I membri nazionali di Eurojust e i loro assistenti hanno il diritto, nei limiti del proprio mandato, di accedere e consultare i dati inseriti nel SIS II.

Tre anni dopo l'entrata in funzione del SIS II, la Commissione ha svolto una valutazione del sistema. I tre recenti nuovi regolamenti SIS (rifusione del SIS) tengono conto di tale valutazione e mirano a una maggiore efficienza nella lotta contro il terrorismo e le forme gravi di criminalità, in particolare attraverso un migliore scambio di informazioni tra le autorità competenti. Sostengono inoltre la gestione delle frontiere e della migrazione e preparano il SIS all'interoperabilità con i sistemi IT dell'UE su larga scala, quali VIS, Eurodac, ETIAS ed EES. I regolamenti che modificano il quadro giuridico e operativo del SIS II sono i seguenti:

- il regolamento (UE) 2018/1860 relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare[43];

- il regolamento (UE) 2018/1861 sull'istituzione, l'esercizio e l'uso del SIS nel settore delle verifiche di frontiera[44]; e

- il regolamento (UE) 2018/1862 sull'istituzione, l'esercizio e l'uso del SIS nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale[45].

---

43 Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare, GU L 312 del 7.12.2018, pag. 1.

44 Regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006, GU L 312 del 7.12.2018, pag. 14.

45 Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione, GU L 312 del 7.12.2018, pag. 56.

I tre regolamenti SIS riveduti sono entrati in vigore nel dicembre 2019 e saranno pienamente operativi a partire dal dicembre 2021. Le nuove funzionalità del SIS sono in corso di realizzazione in fasi diverse, con l'obbligo di completare i lavori entro il 2021. Nel marzo 2018 è stato introdotto nel SIS un sistema automatico per il riconoscimento delle impronte digitali (AFIS) che consentirà di effettuare interrogazioni basate sulle impronte digitali a partire dal 2021.

I regolamenti contengono disposizioni specifiche per gli Stati membri che godono di uno status speciale per quanto riguarda Schengen e le misure nello spazio di libertà, sicurezza e giustizia del TFUE, ossia Danimarca, Irlanda, Croazia, Bulgaria, Romania e Cipro. Inoltre, i regolamenti (UE) 2018/1861 e (UE) 2018/1860 forniscono la base giuridica per consentire ai membri delle squadre della guardia di frontiera e costiera europea di accedere direttamente ai dati del SIS ai fini delle verifiche di frontiera e del rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare. I membri delle squadre della guardia di frontiera e costiera europea, nell'ambito dei rispettivi mandati e a condizione che siano autorizzati a effettuare controlli e abbiano ricevuto la formazione necessaria, eserciteranno tale diritto tramite l'interfaccia tecnica che sarà istituita e gestita dall'Agenzia europea della guardia di frontiera e costiera (Frontex) e che permetterà un collegamento diretto con il SIS II centrale.

2.2. SIE – Sistema di informazione Europol[46]

Il regolamento Europol introduce un nuovo concetto per il trattamento dei dati, comunemente indicato come concetto di gestione integrata dei dati (Integrated Data Management Concept - IDMC). L'IDMC può essere definito come la possibilità di utilizzare le informazioni relative alla criminalità per molteplici fini commerciali quali indicati dal proprietario dei dati, consentendone una gestione e un trattamento integrati e tecnologicamente neutrali. In base alla decisione del Consiglio che istituiva Europol, il trattamento dei dati era strutturato attorno a sistemi. Il regolamento Europol non contiene più riferimenti a sistemi, ma richiede invece l'indicazione delle finalità del trattamento. Per agevolare una transizione fluida, gli utenti possono continuare a operare con i sistemi esistenti in un modo che sia conforme al nuovo quadro giuridico.

[46] Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI, GU L 135 del 24.5.2016, pag. 53 (applicabile a decorrere dal 1º maggio 2017).

Il sistema di informazione Europol (SIE), di cui alla decisione Europol, è un sistema centralizzato ospitato da Europol che permette agli Stati membri e ai partner di cooperazione di Europol di conservare, condividere e sottoporre a controlli incrociati i dati relativi a indagati, condannati o "futuri criminali potenziali" coinvolti in reati che rientrano nel mandato di Europol (forme gravi di criminalità, criminalità organizzata o terrorismo). Permette di conservare l'intera gamma di dati e di prove relativa a tali reati/persone, ad esempio persone con pseudonimi, società, numeri di telefono, indirizzi e-mail, veicoli, armi da fuoco, DNA, fotografie, impronte digitali, bombe ecc. Il SIE, che serve in primo luogo come sistema di sostegno ai controlli incrociati, offre un accesso basato sul risconto positivo o negativo ("hit/no hit"). Il regolamento Europol prevede il pieno accesso ai dati trasmessi a fini di analisi strategiche e tematiche, ma soltanto un accesso basato sul riscontro positivo o negativo per i dati presentati a fini di analisi operative.

Il SIE è, di fatto, un sistema di riferimento che aiuta a verificare se le informazioni cercate sono disponibili in uno degli Stati membri dell'UE, presso i partner di cooperazione o presso Europol. È direttamente disponibile in tutti gli Stati membri e per il personale di Europol debitamente autorizzato. Attualmente si distinguono tre modalità di caricamento dei dati da parte degli Stati membri:

a) inserimento manuale dei dati nel SIE o tramite SIENA;

b) trasferimento semi-automatizzato effettuando un caricamento a blocchi nel SIE;

c) trasferimento automatizzato dei dati utilizzando un caricatore di dati.

La grande maggioranza dei dati contenuti nel sistema di informazione Europol (SIE) è inserita mediante sistemi automatici di caricamento dati. L'approccio degli Stati membri alla raccolta dei dati è cambiato: l'attenzione in materia di trasmissione dei dati si è spostata verso le entità che possono essere oggetto di controlli incrociati, come persone, veicoli, numeri di telefono e armi da fuoco.

I paesi terzi non possono inserire direttamente o effettuare controlli incrociati dei dati nel SIE; tuttavia, conformemente all'articolo 23, paragrafo 5, del regolamento Europol, possono inviarli a Europol, il quale valuterà innanzitutto se i dati rientrino nel suo mandato e solo allora li accetterà e ne effettuerà il controllo incrociato.

Il SIE, che consente la condivisione di informazioni estremamente sensibili, dispone di un solido sistema che assicura riservatezza e sicurezza. La sicurezza è garantita, ad esempio, dai codici di gestione specifici, che indicano cosa è possibile fare con le informazioni in questione e chi vi ha accesso. I codici di gestione sono progettati per proteggere la fonte delle informazioni e garantire che il trattamento delle informazioni avvenga conformemente agli auspici del loro proprietario e al diritto nazionale degli Stati membri. Il SIE è accreditato per il trattamento di dati fino al livello RESTREINT UE/EU RESTRICTED incluso.

2.3. SIENA - Applicazione di rete per lo scambio sicuro di informazioni di Europol

SIENA è il sistema di comunicazione sicura di Europol utilizzato dagli Stati membri, da Europol e dai suoi partner di cooperazione per lo scambio di informazioni e analisi (intelligence) operative e strategiche relative ai reati, compresi dati operativi di carattere personale. SIENA è un sistema di messaggistica che offre vari tipi di messaggi per varie finalità, incluso lo scambio di dati ai sensi della "decisione quadro svedese".

Nella progettazione e nel funzionamento di SIENA è stato posto un accento notevole sulla sicurezza, la protezione dei dati e la riservatezza. SIENA è accreditata per lo scambio di informazioni CONFIDENTIEL UE/EU CONFIDENTIAL. Lo scambio di dati tramite SIENA comporta chiare responsabilità in termini di trattamento di dati. Per ogni messaggio SIENA trasmesso devono essere indicati la classificazione (riservatezza), i codici di gestione e l'affidabilità della fonte e delle informazioni.

L'interfaccia utente di SIENA ha l'inglese come lingua predefinita ma l'interfaccia è plurilingue e permette agli operatori SIENA di lavorare nella propria lingua nazionale/ nelle proprie lingue nazionali. Oltre a scambiare messaggi, gli operatori SIENA possono effettuare ricerche ed elaborare relazioni statistiche sui dati scambiati tramite SIENA.

SIENA sostiene lo scambio bilaterale di dati tra Stati membri e permette loro di scambiare dati che esulano dal mandato di Europol. Quando nello scambio di dati si rivolgono a uno dei partner di cooperazione di Europol, gli Stati membri ricevono una notifica tramite SIENA relativa al fatto che lo scambio dovrebbe aver luogo solo se riguarda reati rientranti nel mandato di Europol.

Europol gestirà le informazioni scambiate via SIENA ai fini del trattamento dei dati operativi soltanto se è incluso come destinatario nello scambio di dati. A fini di audit, tutti i dati scambiati tramite SIENA sono a disposizione del responsabile della protezione dei dati di Europol e delle autorità di controllo nazionali.

SIENA supporta lo scambio strutturato di dati sulla base del formato universale dei messaggi (UMF). Attualmente l'entità UMF PERSON può essere creata/mostrata nella stessa applicazione web SIENA. L'intero modello dati UMF è già supportato dal servizio web SIENA.

2.4. I-24/7 - Sistema globale di comunicazione di polizia di Interpol

La rete globale I-24/7 per lo scambio di informazioni di polizia collega il segretariato generale di Interpol a Lione (Francia), gli uffici centrali nazionali (UCN) in 190 paesi e gli uffici regionali.

Il sistema d'informazione Interpol consente la comunicazione tramite messaggi diretti tra UCN. Tutte le banche dati Interpol (eccetto la banca dati di immagini di sfruttamento sessuale di minori) sono accessibili in tempo reale tramite il sistema globale di comunicazione di polizia I-24/7. Il sistema I-24/7, inoltre, permette ai paesi membri di accedere reciprocamente alle banche dati nazionali utilizzando una connessione business-to-business (B2B). I paesi membri gestiscono e mantengono i rispettivi dati nazionali di natura penale e ne controllano la trasmissione, l'accesso da parte di altri paesi e la distruzione conformemente alle normative nazionali. Hanno anche l'opzione di renderli accessibili alla comunità internazionale delle autorità di contrasto tramite I-24/7.

2.4.1. Interpol: DNA Gateway

La banca dati di Interpol sul DNA include una banca dati internazionale sul DNA, un modulo di richiesta di ricerca internazionale per lo scambio bilaterale e uno strumento di trasferimento elettronico sicuro standardizzato. Non si conservano dati nominali che collegano un profilo DNA a un individuo. Il DNA Gateway è compatibile con lo scambio automatizzato di dati nel quadro di Prüm.

I paesi membri possono accedere alla banca dati e, su richiesta, l'accesso può essere esteso, oltre agli uffici centrali nazionali dei paesi membri, ai centri e ai laboratori di scienza forense. La polizia nei paesi membri può trasmettere il profilo DNA di autori di reati, scene del crimine, persone scomparse e corpi non identificati.

2.4.2. Banca data di impronte digitali di Interpol

Gli utenti autorizzati nei paesi membri possono visualizzare, trasmettere e sottoporre a controlli incrociati i dati tramite un sistema automatico per il riconoscimento delle impronte digitali (AFIS). I dati sono salvati e scambiati nel formato definito dall'Istituto nazionale per gli standard e la tecnologia (NIST). Gli orientamenti relativi alla trasmissione di impronte digitali e gli orientamenti relativi alla trasmissione delle tracce di impronte digitali rinvenute sulla scena del crimine forniscono un contributo ai paesi membri per migliorare la qualità e la quantità dei dati relativi a impronte digitali trasmessi all'AFIS di Interpol.

2.4.3. Banca dati di Interpol sui documenti di viaggio rubati e smarriti

La banca dati di Interpol sui documenti di viaggio rubati e smarriti contiene informazioni su più di 45 milioni di documenti di viaggio segnalati come rubati o smarriti da 166 paesi. Questa banca dati permette agli UCN di Interpol e alle altre autorità di contrasto autorizzate (come i funzionari preposti all'immigrazione e al controllo delle frontiere) di accertare la validità di un documento di viaggio sospetto. Al fine di prevenire e combattere la criminalità organizzata e le forme gravi di criminalità, le autorità di contrasto competenti degli Stati membri scambiano dati relativi ai passaporti con Interpol[47].

2.4.4. Documenti di viaggio associati a segnalazioni (TDAWN)

La banca dati TDAWN contiene informazioni su documenti di viaggio relative a individui oggetto di un avviso Interpol.

2.4.5. Tabella di riferimento delle armi da fuoco

La tabella di riferimento INTERPOL delle armi da fuoco permette agli inquirenti di identificare in modo adeguato un'arma da fuoco utilizzata in un reato (marca, modello, calibro ecc.). Contiene più di 250 000 riferimenti ad armi da fuoco e 57 000 immagini di alta qualità. La rete di informazione balistica di INTERPOL è una piattaforma per la condivisione e il confronto internazionale su vasta scala dei dati balistici e contiene più di 150 000 voci.

Il sistema di INTERPOL per la registrazione e la tracciabilità delle armi da fuoco illegali (iARMS) è un'applicazione informatica che facilita lo scambio di informazioni e la cooperazione tra le autorità di contrasto per quanto concerne i reati connessi ad armi da fuoco.

---

[47] Posizione comune 2005/69/GAI del Consiglio sullo scambio con l'Interpol di alcuni dati, GU L 27 del 29.1.2005, pag. 61.

2.5. ECRIS[48]

Il sistema informatico europeo di informazione sui casellari giudiziali (ECRIS)[49] fornisce gli strumenti elettronici per lo scambio tra gli Stati membri delle informazioni relative alle condanne in un formato standardizzato. ECRIS è utilizzato per notificare agli Stati membri le condanne dei loro cittadini e per inviare richieste di informazioni relative alle condanne a fini di procedimenti penali e ad altri fini, come quelli amministrativi od occupazionali. È anche possibile avanzare richieste relative a cittadini di paesi terzi, se vi sono motivi di ritenere che lo Stato membro richiesto disponga di azioni sulla persona in questione.

Le richieste ECRIS devono ricevere una risposta entro 10 giorni lavorativi, se sono a fini di procedimenti penali o a fini occupazionali, ed entro 20 giorni lavorativi se la richiesta proviene da un privato per sua informazione.

ECRIS non si prefigge di istituire una banca dati centralizzata di casellari giudiziali e si basa su un'architettura informatica decentrata in cui tutti i casellari giudiziali sono conservati unicamente nelle banche dati gestite dagli Stati membri. I dati sono scambiati in via elettronica tra le autorità centrali designate degli Stati membri.

Le informazioni devono essere trasmesse dagli Stati membri in conformità alle norme convenute e ai formati standard, e devono essere il più possibile complete al fine di consentire allo Stato membro che le riceve di trattarle in modo adeguato e identificare la persona. I messaggi sono inviati nelle lingue ufficiali degli Stati membri interessati o in un'altra lingua accettata da entrambi gli Stati membri.

---

48 Decisione quadro 2009/315/GAI del Consiglio, del 26 febbraio 2009, relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario, GU L 93 del 7.4.2009, pag. 23.

49 Direttiva (UE) 2019/884 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio, GU L 151 del 7.6.2019, pag. 143.

Il segretariato generale del Consiglio pubblica un manuale non vincolante destinato agli operatori del settore - disponibile in formato elettronico sul sito web del Consiglio e sul sito CIRCABC ospitato dalla Commissione europea all'indirizzo https://circabc.europa.eu - che definisce le procedure di scambio delle informazioni e coordina le loro azioni per lo sviluppo e il funzionamento di ECRIS. Le richieste di accesso al manuale vanno trasmesse al segretariato del Consiglio. Le richieste di accesso al gruppo di interesse ristretto "ECRIS Business and Technical Support" vanno trasmesse alla Commissione europea.

2.5.1. ECRIS-TCN[50]

Il quadro giuridico di ECRIS non risponde sufficientemente alle caratteristiche delle richieste riguardanti cittadini di paesi terzi. All'interno dell'Unione le informazioni sui cittadini di paesi terzi non sono raccolte come avviene per i cittadini degli Stati membri negli Stati membri di cittadinanza, ma sono solo conservate negli Stati membri in cui le condanne sono state pronunciate. Mediante l'ECRIS-TCN[51] l'autorità centrale nazionale può individuare quale altro Stato membro è in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo. Il quadro ECRIS può pertanto essere utilizzato per richiedere tali informazioni a quegli Stati membri conformemente alla decisione quadro 2009/315/GAI.

Il regolamento prevede norme che istituiscono un sistema centralizzato a livello di Unione contenente dati personali e norme sulla ripartizione delle responsabilità tra gli Stati membri e sull'organizzazione responsabile dello sviluppo e della manutenzione del sistema centralizzato. Esso prevede globalmente un livello adeguato di protezione e sicurezza dei dati e di salvaguardia dei diritti fondamentali degli interessati.

---

50 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 cittadini 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, GU L 135 del 22.5.2019, pag. 1.
Direttiva (UE) 2019/884 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio, GU L 151 del 7.6.2019, pag. 143.

51 La Commissione determinerà la data a partire dalla quale l'ECRIS-TCN entrerà in funzione una volta soddisfatte le condizioni di cui all'articolo 35 del regolamento (UE) 2019/816.

Gli Stati membri dovrebbero creare nell'ECRIS-TCN registri di dati concernenti i cittadini di paesi terzi condannati. Ove possibile, ciò dovrebbe essere fatto automaticamente e senza ingiustificato ritardo dopo l'iscrizione della condanna nel casellario giudiziale nazionale. Gli Stati membri dovrebbero, conformemente al regolamento, inserire nel sistema centrale i dati alfanumerici e i dati relativi alle impronte digitali relativamente alle condanne pronunciate dopo la data d'inizio dell'inserimento dei dati nell'ECRIS-TCN. A decorrere dalla stessa data, e in qualsiasi momento successivo, gli Stati membri dovrebbero poter inserire immagini del volto nel sistema centrale.

L'ECRIS-TCN prevede il trattamento dei dati relativi alle impronte digitali allo scopo di individuare gli Stati membri in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo. Esso dovrebbe inoltre consentire il trattamento delle immagini del volto allo scopo di confermarne l'identità. È essenziale che l'inserimento e l'utilizzo dei dati relativi alle impronte digitali e delle immagini del volto non eccedano quanto strettamente necessario per raggiungere l'obiettivo perseguito, rispettino i diritti fondamentali, come pure l'interesse superiore del minore, e siano conformi alle norme applicabili dell'Unione in materia di protezione dei dati.

Eurojust, Europol ed EPPO dovrebbero avere accesso all'ECRIS-TCN al fine di individuare gli Stati membri in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo, ai fini dello svolgimento dei loro compiti statutari.

L'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA) è incaricata dello sviluppo e del funzionamento dell'ECRIS-TCN.

2.6. Sistema d'informazione visti (VIS)[52]

Il Sistema d'informazione visti (VIS) è principalmente un sistema di controllo dell'immigrazione. Si tratta di uno strumento utilizzato per facilitare la consultazione a livello di consolati e il controllo delle frontiere tramite la verifica elettronica e lo scambio, tra Stati membri, di dati relativi ai visti. In quanto tale, riguarda i cittadini stranieri con l'obbligo del visto. Le autorità designate degli Stati membri (ossia, gli uffici consolari, i valichi di frontiera, le autorità di polizia e preposte all'immigrazione)[53] ed Europol[54], nel quadro dei suoi compiti, sono autorizzate a consultare il VIS[55] ai fini della prevenzione, dell'individuazione e dell'investigazione di:

- reati di terrorismo, vale a dire i reati che, ai sensi della legislazione nazionale, corrispondono o sono equivalenti ai reati di cui agli articoli da 1 a 4 della decisione quadro 2002/475/GAI del Consiglio, del 13 giugno 2002, sulla lotta contro il terrorismo, e di

- reati gravi, vale a dire le forme di reato che corrispondono o sono equivalenti a quelle di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI ("mandato d'arresto europeo").

---

52 Decisione del Consiglio dell'8 giugno 2004 che istituisce il sistema di informazione visti (VIS) (2004/512/CE), GU L 213 del 15.6.2004, pag. 5.

53 Elenco delle autorità competenti il cui personale debitamente autorizzato ha accesso al sistema di informazione visti (Visa Information System – VIS) ai fini dell'inserimento, della modifica, della cancellazione e della consultazione dei dati (2016/C 187/04), GU C 187 del 26.5.2016, pag. 4.

54 Decisione 2008/633/GAI del Consiglio relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi, GU L 218 del 13.8.2008, pag. 129; Decisione del Consiglio che fissa la data di decorrenza degli effetti della decisione 2008/633/GAI relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi (2013/392/UE), GU L 198 del 23.7.2013, pag. 45.

55 Il 16 aprile 2015 la Corte di giustizia ha annullato la decisione 2013/392/UE del Consiglio, del 22 luglio 2013, che fissa la data di decorrenza degli effetti della decisione 2008/633/GAI relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi. Ciononostante, la Corte ha dichiarato che gli effetti della decisione 2013/392 dovevano essere mantenuti fino all'entrata in vigore di un nuovo atto diretto a sostituirla.

Ai sensi della decisione quadro svedese, le informazioni contenute nel VIS possono essere fornite al Regno Unito e all'Irlanda dalle autorità competenti degli Stati membri le cui autorità designate hanno accesso al VIS, e le informazioni conservate nei registri nazionali dei visti del Regno Unito e dell'Irlanda possono essere fornite alle autorità di contrasto competenti degli altri Stati membri.

Il VIS si basa su un'architettura centralizzata e su una piattaforma comune con il SIS II. I dati VIS sono trattati in due fasi. Nella prima fase essi includono dati alfanumerici e fotografie. Nella seconda fase sono trattati e inseriti nel VIS i dati biometrici e i documenti scannerizzati. Il VIS contiene dati relativi alle domande di visto, fotografie, impronte digitali, decisioni correlate delle autorità per il visto e collegamenti tra domande connesse. Il VIS ricorre a un sistema di confronto biometrico per garantire confronti affidabili delle impronte digitali a fini di:

- verifica, vale a dire un controllo della corrispondenza delle impronte digitali scannerizzate al valico di frontiera con quelle associate ai documenti biometrici allegati al visto, oppure

- identificazione, vale a dire un confronto delle impronte digitali rilevate al valico di frontiera con il contenuto dell'intera banca dati.

In termini tecnici, il VIS consiste di tre livelli, ovvero quello centrale, quello nazionale e quello locale; quest'ultimo include gli uffici consolari, i valichi di frontiera e le autorità preposte all'immigrazione e di polizia.
Nel maggio 2018 la Commissione ha presentato una proposta legislativa di modifica del regolamento VIS allo scopo, tra l'altro, di garantire l'interoperabilità tra altre banche dati del settore della giustizia e degli affari interni. Il VIS potenziato non dovrebbe essere operativo prima della fine del 2021.

2.7. Eurodac[56] [57]

Il sistema automatico europeo per il riconoscimento delle impronte digitali (Eurodac) assiste in primo luogo nella determinazione dello Stato membro responsabile dell'esame delle domande di asilo presentate in uno degli Stati membri, nonché nella facilitazione dell'applicazione della convenzione di Dublino. L'accesso a Eurodac a fini di prevenzione, rilevamento o indagine di reati terroristici o altri reati gravi è concesso esclusivamente in casi ben definiti.

Il regolamento Eurodac n. 603/2013 detta disposizioni in ordine alla trasmissione all'unità centrale dei dati relativi alle impronte digitali, alla registrazione, nella banca dati centrale pertinente, di tali dati e di altri dati pertinenti, alla loro memorizzazione, al loro confronto con altri dati relativi a impronte digitali, nonché in ordine alla trasmissione dei risultati di tali confronti e al congelamento e alla cancellazione dei dati registrati.

L'architettura del sistema Eurodac consta di a) una banca dati centrale informatizzata per le impronte digitali ("sistema centrale") costituita da un'unità centrale e un piano e un sistema di continuità operativa, e b) un'infrastruttura di comunicazione tra il sistema centrale e gli Stati membri, dotata di una rete virtuale cifrata dedicata ai dati Eurodac ("infrastruttura di comunicazione").

Ciascuno Stato membro dispone di un unico punto di accesso nazionale.

---

56 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, GU L 316 del 15.12.2000, pag. 1.

57 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).

"eu-LISA", istituita dal regolamento (UE) n. 1077/2011[58], è responsabile della gestione operativa dell'Eurodac e, in cooperazione con gli Stati membri, provvede a che in qualsiasi momento siano utilizzate, previa analisi costi/benefici, le migliori e più sicure tecnologie e tecniche disponibili per il sistema centrale.

Ogni Stato membro può trasmettere impronte digitali all'unità centrale al fine di controllare se uno straniero di almeno 14 anni di età trovato illegalmente sul suo territorio ha già presentato una domanda di asilo in un altro Stato membro. L'unità centrale confronta tali impronte digitali con i dati relativi alle impronte digitali trasmessi dagli altri Stati membri e già memorizzati nella banca dati centrale. L'unità informa lo Stato membro che ha trasmesso i dati dell'esistenza di una risposta pertinente, vale a dire il risultato di un confronto tra le impronte digitali registrate e quelle trasmesse. Tale Stato membro controlla il risultato e procede all'identificazione definitiva in cooperazione con lo Stato membro interessato.

Gli Stati membri devono garantire la liceità, l'accuratezza e la sicurezza dei dati Eurodac. Le persone e gli Stati membri che hanno subito un danno in conseguenza del mancato rispetto delle disposizioni Eurodac hanno diritto di ottenere un risarcimento dallo Stato membro responsabile del pregiudizio.

Il regolamento (UE) n. 603/2013 prevede l'accesso ai dati Eurodac da parte delle autorità designate degli Stati membri e di Europol a fini di contrasto. Ai sensi del regolamento, le autorità designate possono presentare una richiesta motivata in formato elettronico per il confronto dei dati relativi alle impronte digitali con i dati conservati nel sistema centrale soltanto se il confronto con le seguenti banche dati non ha consentito di stabilire l'identità dell'interessato:

– le banche nazionali dei dati dattiloscopici;

[58] Regolamento (UE) n. 1077/2011 del Parlamento europeo e del Consiglio, del 25 ottobre 2011, che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, GU L 286 dell'1.11.2011, pag. 1.

– i sistemi automatizzati d'identificazione dattiloscopica (AFIS) di tutti gli altri Stati membri ai sensi della decisione 2008/615/GAI ("decisione di Prüm"), qualora il confronto sia tecnicamente disponibile, a meno che non sussistano fondati motivi per ritenere che un confronto con tali sistemi non consentirebbe di stabilire l'identità dell'interessato. Tali fondati motivi sono inclusi nella richiesta motivata di confronto con i dati Eurodac presentata in formato elettronico dall'autorità designata all'autorità di verifica;

– il sistema di informazione visti (VIS), purché siano soddisfatte le condizioni per il confronto previste dalla decisione 2008/633/GAI.

Devono inoltre essere soddisfatte tutte le seguenti condizioni nel loro insieme:

a) il confronto è necessario a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi, vale a dire esiste un interesse prevalente di sicurezza pubblica tale da rendere proporzionata l'interrogazione della banca dati;

b) il confronto è necessario in un caso specifico (vale a dire non si eseguono confronti sistematici);

c) esistono fondati motivi per ritenere che il confronto contribuisca in misura sostanziale alla prevenzione, all'individuazione o all'investigazione di uno dei reati in questione. Tali fondati motivi ricorrono in particolare laddove sussista il sospetto fondato che l'autore presunto o effettivo oppure la vittima di un reato di terrorismo o di un altro reato grave rientri in una delle categorie contemplate dal regolamento (UE) n. 603/2013.

2.8. SID – Sistema d'informazione doganale[59]

Il sistema d'informazione doganale integra la convenzione "Napoli II"[60]. Il sistema mira a rafforzare l'amministrazione doganale degli Stati membri attraverso un rapido scambio di informazioni al fine di prevenire, accertare e perseguire gravi infrazioni del diritto nazionale e comunitario. Il SID istituisce inoltre un archivio d'identificazione dei fascicoli a fini doganali (FIDE) per prestare assistenza alle indagini doganali.

Il SID è un sistema di informazione centralizzato gestito dalla Commissione e accessibile tramite terminali situati in ogni Stato membro e presso la Commissione, Europol ed Eurojust. Ai dati SID possono accedere le autorità nazionali doganali, tributarie, agricole, sanitarie e di polizia, Europol ed Eurojust. Soltanto le autorità designate dagli Stati membri[61] e la Commissione hanno accesso diretto ai dati contenuti nel SID. Al fine di rafforzare la complementarità, Europol ed Eurojust hanno un accesso in sola lettura al SID e al FIDE.

Il SID comprende dati personali raggruppati secondo le seguenti categorie: merci, mezzi di trasporto, imprese, persone e merci e denaro contante bloccati, sequestrati o confiscati. I dati personali immessi nel SID possono essere copiati in altri sistemi di trattamento dei dati soltanto a fini di gestione dei rischi o di analisi operativa e possono essere consultati soltanto dagli analisti designati dagli Stati membri.

Il FIDE consente alle autorità nazionali preposte alle indagini doganali, quando istruiscono un fascicolo, di individuare le altre autorità che possono aver indagato sulle persone o sulle imprese in questione.

---

59 Decisione 2009/917/GAI del Consiglio, del 30 novembre 2009, sull'uso dell'informatica nel settore doganale, GU L 323 del 10.12.2009, pag. 20.

60 Convenzione stabilita in base all'articolo K.3, del trattato sull'Unione europea relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali, GU C 24 del 23.1.1998, pag. 2.

61 Attuazione dell'articolo 7, paragrafo 2, e dell'articolo 8, paragrafo 3, della decisione 2009/917/GAI del Consiglio, del 30 novembre 2009, sull'uso dell'informatica nel settore doganale - elenchi aggiornati delle autorità competenti, doc. 13394/11 ENFOCUSTOM 85.

2.9. Documenti falsi e autentici online - FADO[62]

Un sistema informatizzato di archiviazione delle immagini che include documenti falsi e autentici basato sulla tecnologia Internet permette uno scambio rapido e sicuro di informazioni tra il segretariato generale del Consiglio dell'Unione europea e il personale preposto al controllo dei documenti in tutti gli Stati membri nonché in Islanda, Norvegia e Svizzera. Il sistema consente un confronto su schermo tra l'originale e un documento falso o contraffatto. In primo luogo contiene documenti degli Stati membri nonché documenti di paesi terzi da cui si registra un'emigrazione abituale verso gli Stati membri. La banca dati istituita da FADO contiene i seguenti dati:

- immagini di documenti autentici
- informazioni sulle tecniche di sicurezza (elementi di sicurezza)
- immagini di documenti tipici contraffatti e falsi
- informazioni sulle tecniche di falsificazione
- statistiche sui documenti falsi e contraffatti individuati e sulle frodi d'identità

Il sistema utilizza linee speciali per la trasmissione dei dati tra il segretariato generale del Consiglio e i servizi centrali degli Stati membri. Negli Stati membri il sistema è consultato da un'unità centrale attraverso una connessione Internet crittografata. Uno Stato membro può usare il sistema a livello nazionale, ossia collegare diverse stazioni di lavoro situate ai suoi diversi posti di frontiera o presso altre autorità competenti. Ciononostante, non vi sono collegamenti diretti tra una stazione di lavoro diversa dall'unità centrale nazionale ed il punto centrale installato presso il segretariato generale.

FADO è disponibile al momento in 22 lingue ufficiali dell'Unione europea. I documenti sono inseriti da esperti di documenti in una delle lingue e le descrizioni standardizzate sono tradotte automaticamente. Di conseguenza, i documenti sono immediatamente disponibili in tutte le lingue supportate. Le ulteriori informazioni a testo libero contenute sono tradotte in seguito da linguisti specializzati del segretariato generale del Consiglio.

---

[62] Azione comune (98/700/GAI) del 3 dicembre 1998 adottata dal Consiglio in base all'articolo K.3 del Trattato sull'Unione europea, relativa alla creazione di un sistema europeo di archiviazione delle immagini (FADO), GU L 333 del 9.12.1998, pag. 4.

2.10. Registro pubblico online dei documenti di identità e di viaggio autentici - PRADO

Mentre l'accesso a FADO è limitato al personale preposto al controllo dei documenti e agli usi governativi, il registro pubblico online dei documenti di identità e di viaggio autentici (PRADO) del Consiglio dell'Unione europea contiene una parte delle informazioni FADO messe a disposizione del pubblico. Il sito web[63] è pubblicato nelle lingue ufficiali dell'UE dal segretariato generale del Consiglio dell'Unione europea per motivi di trasparenza e fornisce un servizio importante a numerosi utenti in Europa, in particolare alle organizzazioni non governative con la necessità o l'obbligo legale di verificare l'identità.

Il sito web contiene descrizioni tecniche, incluse informazioni sugli elementi di sicurezza, di documenti di identità e di viaggio autentici. Le informazioni sono selezionate e fornite da esperti di documenti degli Stati membri, dell'Islanda, della Norvegia e della Svizzera.

Su PRADO gli utenti possono inoltre trovare link a siti web con informazioni su numeri di documenti non validi fornite da alcuni Stati membri nonché da paesi terzi e altre informazioni utili relative all'identità, al controllo dei documenti e alle frodi.

2.11. Sistema di ingressi/uscite (EES)

Il sistema di ingressi/uscite[64] (EES) mira principalmente a migliorare la gestione delle frontiere esterne dell'Unione[65]. Registra elettronicamente l'ora e il luogo di ingresso e di uscita di taluni cittadini di paesi terzi ammessi per un soggiorno di breve durata nel territorio degli Stati membri e calcola la durata del loro soggiorno autorizzato.

Le autorità di contrasto nazionali possono inoltre consultare l'EES, soltanto alle condizioni di cui al regolamento, a fini di prevenzione, accertamento o indagine di reati di terrorismo e altri reati gravi.

---

63 http://www.prado.consilium.europa.eu/

64 Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite (EES) per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011, GU L 327 del 9.12.2017, pag. 20.

65 La Commissione determinerà la data a partire dalla quale l'EES entrerà in funzione una volta soddisfatte le condizioni di cui all'articolo 66 del regolamento (UE) 2017/2226.

Il regolamento stabilisce rigorose norme relative all'accesso all'EES. Stabilisce inoltre i diritti individuali di accesso, rettifica, completamento, cancellazione e ricorso, in particolare il diritto a un ricorso giurisdizionale, e il controllo del trattamento dei dati da parte di autorità pubbliche indipendenti. Il regolamento rispetta i diritti fondamentali ed è conforme ai principi riconosciuti dalla Carta dei diritti fondamentali dell'UE.

L'EES è composto da:

- un sistema centrale (sistema centrale dell'EES) che gestisce una banca dati centrale informatizzata di dati biometrici (impronte digitali e immagini del volto) e alfanumerici;
- un'interfaccia uniforme nazionale in ciascuno Stato membro;
- un'infrastruttura di comunicazione sicura e criptata tra il sistema centrale dell'EES e l'interfaccia uniforme nazionale;
- un canale di comunicazione sicuro fra il sistema centrale dell'EES e il sistema centrale di informazione visti (VIS) a fini di consultazione.

Il regolamento specifica quali autorità nazionali possano essere autorizzate ad accedere all'EES per inserire, modificare, cancellare o consultare dati ai fini specifici dell'EES e nella misura necessaria all'assolvimento dei loro compiti. Ogni trattamento dei dati dell'EES dovrebbe essere proporzionato agli obiettivi perseguiti e necessario all'assolvimento dei compiti delle autorità competenti.

Le condizioni di accesso all'EES da parte delle autorità di contrasto nazionali sono tali da permettere a queste ultime di occuparsi di casi di sospetti che usano identità multiple. Malgrado l'impatto sulla vita privata del viaggiatore, l'uso specifico di dati biometrici conservati nell'EES è giustificato per identificare viaggiatori sprovvisti di documenti di viaggio o di altri documenti identificativi. Tuttavia, tali dati possono anche essere utilizzati per raccogliere prove risalendo alle rotte di viaggio di una persona sospettata di aver commesso un reato o di una vittima di reato.

L'accesso ai dati nell'EES a fini di contrasto costituisce un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono trattati nell'EES. Il trattamento di tali dati è disciplinato dalle disposizioni della direttiva (UE) 2016/680 ("direttiva polizia")[66].

Nello svolgimento dei loro compiti, le autorità di contrasto nazionali possono confrontare una traccia dattiloscopica rilevata in una scena del crimine ("impronte digitali latenti") con dati relativi alle impronte digitali conservati nell'EES, ove vi siano motivi ragionevoli per ritenere che i dati relativi all'autore o alla vittima siano conservati nell'EES. Tuttavia, l'accesso all'EES a fini di contrasto per identificare una persona sospettata sconosciuta, un autore sconosciuto o una vittima sconosciuta di un reato di terrorismo o altro reato grave è concesso solo qualora le banche dati nazionali siano state consultate e la consultazione in base alle impronte digitali ai sensi della decisione del Consiglio 2008/615/GAI[67] ("decisione Prüm") sia stata interamente effettuata oppure non sia stata interamente effettuata entro due giorni dal suo avvio.

Analogamente alle procedure e alle condizioni di accesso da parte delle autorità nazionali di contrasto, i dati dell'EES sono a disposizione anche di Europol, nel quadro dei suoi compiti e alle condizioni e limitazioni stabilite nel regolamento. Europol tratta le informazioni ottenute da una consultazione dei dati dell'EES soggetta all'autorizzazione dello Stato membro d'origine. Tale autorizzazione è ottenuta attraverso l'unità nazionale Europol di detto Stato membro. Il Garante europeo della protezione dei dati dovrebbe monitorare il trattamento dei dati da parte di Europol e garantire la piena conformità alle norme applicabili in materia di protezione dei dati.

---

66 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2019, 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, GU L 119 del 4.5.2016, pag. 89.

67 Decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, GU L 210 del 6.5.2008, pag. 1.

2.12. Sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)[68]

Lo scambio di informazioni nel settore della gestione delle frontiere, del contrasto e della lotta al terrorismo sarà sostenuto dall'ETIAS[69]. Scopo del sistema è determinare l'ammissibilità dei cittadini di paesi terzi esenti dall'obbligo del visto prima che si rechino nello spazio Schengen e prima del loro arrivo ai valichi di frontiera esterni. L'ETIAS rilascia un'autorizzazione ai viaggi, che per sua natura è diversa da un visto ma costituisce una condizione per l'ingresso e il soggiorno, e indica che il richiedente non presenta un rischio per la sicurezza, di immigrazione illegale o un alto rischio epidemico. Le autorizzazioni ai viaggi rilasciate dovrebbero essere annullate o revocate non appena risulti ovvio che le condizioni del loro rilascio non sono state o non sono più rispettate.

L'ETIAS consta degli elementi seguenti:

- un sistema IT su larga scala, ossia il sistema d'informazione dell'ETIAS, che è progettato, sviluppato e gestito tecnicamente da eu-LISA;
- l'unità centrale ETIAS, che è parte dell'Agenzia europea della guardia di frontiera e costiera;
- le unità nazionali ETIAS, competenti per l'esame delle domande e la decisione se rilasciare o rifiutare, annullare o revocare le autorizzazioni ai viaggi. A tal fine, le unità nazionali dovrebbero cooperare tra loro e con Europol per valutare le domande.

---

68 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, GU L 236 del 19.9.2018, pag. 1.
Regolamento (UE) 2018/1241 del Parlamento europeo e del Consiglio, del 12 settembre 2018, recante modifica del regolamento (UE) 2016/794 ai fini dell'istituzione di un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), GU L 236 del 19.9.2018, pag. 72.

69 La Commissione determinerà la data a partire dalla quale l'ETIAS entrerà in funzione una volta soddisfatte le condizioni di cui all'articolo 88 del regolamento (UE) 2018/1240.

L'ETIAS tratta i dati personali forniti dal richiedente al solo scopo di valutare se il suo ingresso nell'Unione possa presentare un rischio per la sicurezza, di immigrazione illegale o un alto rischio epidemico nell'Unione. Ai fini della valutazione dei rischi, i dati personali forniti dovrebbero essere confrontati con i dati contenuti in una cartella, un fascicolo o una segnalazione registrati in un sistema d'informazione o in una banca dati dell'UE (sistema centrale ETIAS, SIS, sistema di informazione visti (VIS), sistema di ingressi/uscite (EES) o Eurodac), nei dati Europol o nelle banche dati Interpol (banca dati di Interpol sui documenti di viaggio rubati e smarriti (SLTD) o banca dati Interpol sui documenti di viaggio associati a segnalazioni (TDAWN). I dati personali dovrebbero essere confrontati anche con l'elenco di controllo ETIAS e con indicatori di rischio specifici.

Tale confronto avviene con l'ausilio di processi automatizzati. In caso di riscontro positivo, ovvero di corrispondenza tra i dati personali contenuti nella domanda e indicatori di rischio specifici o i dati personali contenuti in una cartella, un fascicolo o una segnalazione presenti in uno dei suddetti sistemi d'informazione o nell'elenco di controllo, la domanda dovrebbe essere trattata manualmente dall'unità nazionale dello Stato membro competente. Tale valutazione dovrebbe permettere di decidere se rilasciare o meno l'autorizzazione ai viaggi.

Il conseguimento degli obiettivi generali di ETIAS implica il trattamento di quantità significative di dati personali. Il regolamento rispetta i diritti fondamentali ed è conforme ai principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea. Garanzie adeguate tendono pertanto a limitare l'ingerenza nel diritto al rispetto della vita privata e nel diritto alla protezione dei dati di carattere personale a quanto necessario e proporzionato in una società democratica. Per lo stesso motivo, i criteri usati per definire gli indicatori di rischio specifici non dovrebbero in alcun caso essere basati su dati personali sensibili.[70]

[70] Cfr. il 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, GU L 119 del 4.5.2016, pag. 1.

L'accesso ai dati personali nell'ETIAS dovrebbe essere limitato al personale strettamente autorizzato e in nessun caso l'accesso dovrebbe essere utilizzato per giungere a decisioni basate su una qualche forma di discriminazione. Per quanto riguarda le autorità di contrasto, il trattamento dei dati conservati nel sistema centrale ETIAS dovrebbe avvenire solo in casi specifici e solo quando necessario a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi. Le autorità designate ed Europol dovrebbero chiedere l'accesso all'ETIAS soltanto quando abbiano fondati motivi per ritenere che tale accesso fornisca informazioni che contribuiranno alla prevenzione, all'accertamento o all'indagine di reati di terrorismo o altri reati gravi.

2.13. Quadro sinottico dei sistemi informativi utilizzati nello scambio di informazioni a livello dell'UE

Sistemi IT e banche dati	Base giuridica	Finalità	Persone interessate	Condivisione dei dati
Sistema d'informazione Schengen di seconda generazione **SIS II**	Decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) GU L 205 del 7.8.2007, pag. 63	• Sicurezza interna • Controllo delle frontiere • Cooperazione giudiziaria • Indagini sui reati	• Cittadini dell'UE • Cittadini di paesi terzi	• VIS • Europol • Eurojust • Interpol
	Regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) GU L 381 del 23.12.2006, pag. 4	• Rifiuto di ingresso o di soggiorno • Politiche di asilo, immigrazione e rimpatrio	• Cittadini di paesi terzi che non godono di diritti di libera circolazione equivalenti a quelli dei cittadini dell'UE	
	Regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006 GU L 312 del 7.12.2018, pag. 14.	• Rifiuto di ingresso o di soggiorno • Controllo delle frontiere • Indagini sui reati	• Cittadini di paesi terzi	• Europol • Agenzia europea della guardia di frontiera e costiera (Frontex)

	Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare GU L 312 del 7.12.2018, pag. 1.	• Politiche in materia di migrazione e rimpatrio	• Cittadini di paesi terzi	• Europol • Agenzia europea della guardia di frontiera e costiera (Frontex)
	Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione GU L 312 del 7.12.2018, pag. 56.	• Sicurezza interna • Controllo delle frontiere • Cooperazione giudiziaria • Indagini sui reati		
Europol **SIE**	Decisione 2009/371/GAI del Consiglio, del 6 aprile 2009, che istituisce l'Ufficio europeo di polizia (Europol), articoli da 11 a 13 GU L 121 del 15.5.2009, pag. 37	• Reati gravi • Immigrazione • Sicurezza interna • Lotta al terrorismo	• Cittadini dell'UE • Cittadini di paesi terzi	• SIS II
Interpol **I-24/7**	Costituzione di Interpol		• Cittadini dell'UE • Cittadini di paesi terzi	• SIS II • Europol • VIS

Interpol **Documenti di viaggio smarriti/rubati (SLTD)**	Posizione comune 2005/69/GAI del Consiglio sullo scambio con l'Interpol di alcuni dati GU L 27 del 29.1.2005, pag. 61	• Criminalità internazionale e criminalità organizzata • Sicurezza interna	• Cittadini dell'UE • Cittadini di paesi terzi	
ECRIS	Direttiva (UE) 2019/884 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio GU L 151 del 7.6.2019, pag. 143	• Procedimenti penali	• Cittadini dell'UE • Cittadini di paesi terzi	
ECRIS-TCN	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 cittadini 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 GU L 135 del 22.5.2019, pag. 1. Direttiva (UE) 2019/884 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio GU L 151 del 7.6.2019, pag. 143	• Procedimenti penali	• Cittadini di paesi terzi	• Europol • Eurojust • EPPO

VIS	Decisione 2004/512/CE del Consiglio, dell'8 giugno 2004, che istituisce il sistema di informazione visti (VIS) GU L 213 del 15.6.2004, pag. 5 Decisione 2008/633/GAI del Consiglio relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi GU L 218 del 13.8.2008, pag. 129 Decisione 2013/392/UE del Consiglio che fissa la data di decorrenza degli effetti della decisione 2008/633/GAI relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi GU L 198 del 23.7.2013, pag. 45	• Reati gravi • Sicurezza interna • Lotta al terrorismo	• Cittadini di paesi terzi	• SIS II • Europol • Interpol

Eurodac	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) GU L 180 del 29.6.2013, pag. 1 Regolamento (UE) n. 604/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide GU L 180 del 29.6.2013, pag. 31	• Immigrazione • Reati gravi • Sicurezza interna • Lotta al terrorismo	• Cittadini di paesi terzi	• Europol

Codice di prenotazione **(PNR)**	Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi GU L 119 del 4.5.2016, pag. 132	• Reati gravi • Sicurezza interna • Lotta al terrorismo	• Cittadini dell'UE • Cittadini di paesi terzi	• Europol
Informazioni anticipate sui passeggeri (API)	Direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate GU L 261 del 6.8.2004, pag. 24	• Controllo delle frontiere • Immigrazione	• Cittadini di paesi terzi	
ETIAS	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[71] GU L 236 del 19.9.2018, pag. 1 Regolamento (UE) 2018/1241 del Parlamento europeo e del Consiglio, del 12 settembre 2018, recante modifica del regolamento (UE) 2016/794 ai fini dell'istituzione di un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) GU L 236 del 19.9.2018, pag. 72	• Controllo delle frontiere • Immigrazione • Reati gravi • Sicurezza interna • Lotta al terrorismo	• Cittadini di paesi terzi	• SIS • VIS • EES • Eurodac • Europol • Interpol • Elenco di controllo ETIAS

[71] La Commissione determinerà la data a partire dalla quale l'ETIAS entrerà in funzione una volta soddisfatte le condizioni di cui all'articolo 88 del regolamento.

EES	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 GU L 327 del 9.12.2017, pag. 1 Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite (EES) per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011[72] GU L 327 del 9.12.2017, pag. 20	• Gestione delle frontiere • Reati gravi • Lotta al terrorismo	• Cittadini di paesi terzi	• VIS • Europol • Decisione Prüm
SID	Decisione 2009/917/GAI del Consiglio, del 30 novembre 2009, sull'uso dell'informatica nel settore doganale GU L 323 del 10.12.2009, pag. 20	• Lotta ai traffici illeciti	• Cittadini europei • Cittadini di paesi terzi	• Europol

[72] La Commissione determinerà la data a partire dalla quale l'EES entrerà in funzione una volta soddisfatte le condizioni di cui all'articolo 66 del regolamento.

FADO	Azione comune (98/700/GAI) del 3 dicembre 1998 adottata dal Consiglio in base all'articolo K.3 del Trattato sull'Unione europea, relativa alla creazione di un sistema europeo di archiviazione delle immagini (FADO) GU L 333 del 9.12.1998, pag. 4	• Lotta ai documenti falsi • Politica d'immigrazione • Cooperazione di polizia	• Cittadini europei • Cittadini di paesi terzi	

3. LEGISLAZIONE - IL CONTESTO GIURIDICO, LE NORME E GLI ORIENTAMENTI RELATIVI AI PRINCIPALI METODI E SISTEMI DI COMUNICAZIONE

3.1. Direttiva sulla protezione dei dati[73]

La direttiva (UE) 2016/680, che abroga la decisione quadro 2008/977/GAI del Consiglio[74], stabilisce le norme specifiche in materia di:

- protezione delle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, con riguardo al trattamento, con l'ausilio di strumenti automatizzati o in altro modo, dei dati personali da parte della polizia o di altre autorità di contrasto nell'ambito delle loro attività;

- scambio di dati personali, all'interno dell'Unione, da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Mira a garantire il medesimo livello di protezione alle persone fisiche stabilendo diritti azionabili in tutta l'Unione e a prevenire disparità che possono ostacolare lo scambio di dati personali tra le autorità competenti.

È previsto che gli Stati membri recepiscano la direttiva entro il 6 maggio 2018; in via eccezionale tuttavia, nei casi in cui ciò comporti sforzi sproporzionati, possono disporre l'attuazione entro il 6 maggio 2023 delle pertinenti disposizioni di monitoraggio delle operazioni nei sistemi di trattamento automatizzato istituiti anteriormente al 6 maggio 2016.

---

73 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, GU L 119 del 4.5.2016, pag. 89.

74 Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, GU L 350 del 30.12.2008, pag. 60. La decisione quadro è abrogata a decorrere dal 6 maggio 2018.

Il termine "autorità competenti" comprende autorità pubbliche quali le autorità giudiziarie, la polizia o altre autorità di contrasto, come pure qualsiasi altro organismo o entità incaricati dal diritto di uno Stato membro di esercitare l'autorità pubblica e i poteri pubblici ai fini della direttiva. Le attività svolte dalle autorità di contrasto vertono principalmente sulla prevenzione, l'indagine, l'accertamento o il perseguimento di reati. Tali attività possono comprendere attività di polizia in occasione di manifestazioni, grandi eventi sportivi e sommosse, come pure il mantenimento dell'ordine pubblico quale compito conferito a tali autorità ove necessario per la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica e agli interessi fondamentali della società che possono dar luogo a reati.

Il trattamento dei dati personali per fini che non rientrano nell'ambito delle attività sopracitate e di cui le autorità di contrasto possono essere ulteriormente incaricate dagli Stati membri e il trattamento dei dati personali, nella misura in cui ricada nell'ambito di applicazione del diritto dell'Unione, sono disciplinati dal regolamento (UE) 2016/679[75]. Inoltre la direttiva (UE) 2016/680 non disciplina il trattamento dei dati personali con riguardo ad attività concernenti la sicurezza nazionale, attività delle agenzie o unità che si occupano di questioni connesse alla sicurezza nazionale o il trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività attinenti alla politica estera e di sicurezza comune[76].

Ai fini della direttiva sulla protezione dei dati si intende per:

- **"dati personali"** qualsiasi informazione riguardante una persona fisica (l'"interessato") identificata o identificabile, direttamente o indirettamente, in particolare con riferimento a un 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.

  Gli Stati membri dispongono che le autorità competenti che trattano dati personali, se del caso e nella misura del possibile, operino una chiara distinzione tra i dati personali delle diverse categorie di interessati, quali a) indiziati, b) condannati, c) vittime di reato e d) altri parti rispetto a un reato, quali i testimoni;

---

75 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), GU L 119 del 4.5.2016, pag. 1.

76 Titolo V, capo 2, del trattato sull'Unione europea (TUE).

- **"trattamento"** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

I dati personali devono essere trattati in maniera lecita e corretta e perseguire unicamente fini specifici previsti dalla legge. Per essere lecito, tale trattamento dovrebbe essere necessario per l'esecuzione di un compito svolto da un'autorità competente ai fini di contrasto di cui sopra. Il principio di trattamento corretto proprio della protezione dei dati è una nozione distinta dal diritto a un giudice imparziale sancito nell'articolo 47 della Carta e nell'articolo 6 della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. I dati personali devono essere adeguati e pertinenti alle finalità del trattamento.

Il trattamento di dati personali particolarmente sensibili, che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici unicamente intesi a identificare una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale è autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto a condizioni ben definite e restrittive.

La designazione di autorità di controllo nazionali che possano agire in totale indipendenza è un elemento essenziale della tutela delle persone fisiche con riguardo al trattamento dei loro dati. Le autorità di controllo dovrebbero sorvegliare l'applicazione delle disposizioni adottate a norma della direttiva e contribuire alla loro coerente applicazione in tutta l'Unione. La tutela dei diritti e delle libertà degli interessati così come la responsabilità generale delle autorità nazionali competenti e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara attribuzione delle responsabilità.

Il trasferimento transfrontaliero di dati personali potrebbe compromettere la capacità della persona fisica di tutelarsi da usi o divulgazioni illeciti di tali dati. Allo stesso tempo, le autorità di controllo possono concludere di non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività condotte oltre frontiera. I loro sforzi di collaborazione nel contesto transfrontaliero possono anche essere ostacolati da poteri insufficienti per prevenire e correggere e da ordinamenti giuridici incoerenti. Pertanto vi è la necessità di promuovere una più stretta cooperazione tra le autorità di controllo della protezione dei dati affinché possano scambiare informazioni con le loro controparti all'estero.

3.2. La "decisione quadro svedese"[77]

Come sviluppo dell'*acquis* di Schengen, la decisione quadro 2006/960/GAI del Consiglio ("decisione quadro svedese") stabilisce in particolare le norme relative ai termini e ai formulari standard per lo scambio di informazioni a livello transfrontaliero[78], su richiesta preventiva o spontaneamente, tra le competenti autorità di contrasto designate degli Stati membri, allo scopo di:

- prevenire, individuare e indagare su reati o attività criminali che corrispondono o sono equivalenti a quelli enunciati nel mandato d'arresto europeo[79], o
- prevenire un pericolo grave e immediato per la sicurezza pubblica.

Le autorità designate sono tenute a rispondere, entro un massimo di otto ore nei casi urgenti, nella misura in cui le informazioni o le analisi (intelligence) richieste siano direttamente accessibili alle autorità di contrasto. È possibile non fornire informazioni se:

- è in gioco la sicurezza nazionale;
- sono messe a repentaglio indagini in corso;

---

77 Decisione quadro 2006/960/GAI del Consiglio, del 18 dicembre 2006, relativa alla semplificazione dello scambio di informazioni e analisi (intelligence) tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge, GU L 386 del 29.12.2006, pag. 89, modificata dalla rettifica pubblicata nella GU L 75 del 15.3.2007, pag. 26.

78 Cfr. figura 1 in appresso.

79 8216/2/08 REV 2 (Versione definitiva del manuale europeo sull'emissione del mandato di arresto europeo). L'articolo 2 della decisione quadro 2002/584/GAI del Consiglio relativa al mandato d'arresto europeo definisce il campo di applicazione dello stesso.

- la richiesta riguarda un reato passibile di una pena privativa della libertà di un anno o meno a norma della legislazione dello Stato membro richiesto;

- l'autorità giudiziaria competente nega l'accesso alle informazioni.

Per "informazioni e/o analisi (intelligence)" si intendono le due seguenti categorie:

– qualsiasi tipo di informazioni o dati detenuti da autorità di contrasto;

– qualsiasi tipo di informazioni o dati detenuti da autorità pubbliche o da enti privati che siano a disposizione delle autorità di contrasto senza il ricorso a mezzi coercitivi.

Il contenuto di tali categorie dipende dalla legislazione nazionale. Il tipo di informazioni disponibili per ogni Stato membro è riportato nelle schede nazionali allegate al presente manuale.

Devono essere scambiati dati con Europol nella misura in cui le informazioni o le analisi (intelligence) oggetto dello scambio riguardino un reato o un'attività criminale di competenza di Europol. Le informazioni e le analisi (intelligence) saranno trattate secondo i pertinenti codici di gestione Europol. L'applicazione di rete per lo scambio sicuro di informazioni (SIENA) di Europol sostiene lo scambio di informazioni conformemente alla "decisione quadro svedese".

Gli Stati membri garantiscono che le condizioni per lo scambio di informazioni a livello transfrontaliero non siano più rigorose di quelle applicabili a un caso interno. Le autorità di contrasto competenti non sono, in particolare, obbligate a richiedere un accordo o un'autorizzazione giudiziari preliminari allo scambio di informazioni a livello transfrontaliero, se le informazioni richieste sono disponibili a livello nazionale senza tale accordo o autorizzazione. Se tuttavia è richiesta un'autorizzazione giudiziaria, nel pronunciare la sua decisione l'autorità giudiziaria deve applicare al caso transfrontaliero le medesime norme applicabili a un caso meramente interno. Le informazioni per cui è richiesta un'autorizzazione giudiziaria sono indicate nelle schede nazionali.

Poiché gli operatori hanno ritenuto troppo complicato il formulario di richiesta standard, è stato elaborato un formulario di richiesta di informazioni e analisi (intelligence)[80] non obbligatorio. Quando non sia possibile avvalersi di questo formulario semplificato, si consiglia di usare un formulario diverso o del testo libero non strutturato.

[80] Cfr. figura 2 in appresso.

Tuttavia, tali richieste rispettano comunque i requisiti dell'articolo 5 della decisione quadro svedese e contengono almeno i seguenti elementi obbligatori:

- informazioni amministrative: Stato membro e autorità richiedenti, data, numero/i di riferimento, Stato o Stati membri richiesti;
- eventuale urgenza e, nel caso, motivazione;
- descrizione delle informazioni o analisi (intelligence) richieste;
- identità (se nota) o identificazione della persona/delle persone, dell'oggetto/degli oggetti su cui si incentra l'indagine penale o l'operazione di intelligence criminale alla base della richiesta di informazioni o intelligence (ad es. descrizione del reato, circostanze, ecc.);
- finalità della richiesta di informazioni e analisi (intelligence);
- nesso tra la finalità e la persona oggetto delle informazioni e dell'intelligence;
- motivi che fanno ritenere che le informazioni o l'intelligence siano nello Stato membro richiesto;
- eventuali restrizioni all'uso delle informazioni contenute nella richiesta ("codici di gestione").

Lo Stato membro richiedente può scegliere tra i canali esistenti della comunicazione internazionale in materia di attività di contrasto (SIRENE, Europol, Interpol, punti di contatto bilaterali). Lo Stato membro che invia la risposta di norma impiega lo stesso canale usato per la richiesta. Se tuttavia lo Stato membro richiesto risponde, per motivi legittimi, tramite un altro canale, ne informa l'autorità richiedente. La lingua utilizzata per la richiesta e la fornitura di informazioni è quella applicabile al canale utilizzato.

Una panoramica degli **accordi bilaterali o di altro tipo mantenuti** è allegata al presente manuale.

Figura 1

ALLEGATO A

SCAMBIO DI INFORMAZIONI A NORMA DELLA DECISIONE QUADRO DEL CONSIGLIO 2006/960/GAI
FORMULARIO CHE DEVE ESSERE UTILIZZATO DALLO STATO MEMBRO RICHIESTO IN CASO DI TRASMISSIONE, RITARDO O RIFIUTO DI INFORMAZIONE

Questo formulario dev'essere utilizzato per trasmettere l'informazione, e/o l'intelligence richiesta, al fine di informare l'autorità richiedente dell'impossibilità di rispettare il termine normale, della necessità di sottoporre la richiesta all'autorizzazione di un'autorità giudiziaria o del rifiuto di trasmettere l'informazione.

Questo formulario può essere utilizzato più di una volta durante la procedura (per esempio se la richiesta deve prima essere sottoposta a un'autorità giudiziaria e si riscontra in seguito che l'esecuzione della richiesta deve essere rifiutata).

Autorità richiesta (denominazione, indirizzo, telefono, fax, posta elettronica, Stato membro)	
Particolari del funzionario responsabile (facoltativo):	
Numero di riferimento della risposta	
Data e numero di riferimento della risposta precedente	
Risposta alla seguente autorità richiedente	
Data e ora della richiesta	
Numero di riferimento della richiesta	

Il termine normale in virtù dell'articolo 4 della decisione quadro 2006/960/GAI		
Reato di cui all'articolo 2, paragrafo 2 della decisione quadro 2002/584/GAI e l'informazione o intelligence richiesta è conservata in una banca di dati alla quale l'autorità incaricata dell'applicazione della legge dello Stato membro richiesto può accedere direttamente.	Richiesta urgente	→ ❑ 8 ore
	Richiesta non urgente	→ ❑ 1 settimana
Altri casi		→ ❑ 14 giorni

Informazioni trasmesse a norma della decisione quadro 2006/960/GAI: l'informazione e l'intelligence fornita
1. Uso dell'informazione o intelligence trasmessa ❑ può essere utilizzata soltanto per gli scopi per i quali è stata fornita o per la prevenzione di un pericolo grave ed immediato per la sicurezza pubblica; ❑ è autorizzata anche per altri scopi, (facoltativo) alle seguenti condizioni:
2. Affidabilità della fonte ❑ affidabile ❑ per lo più affidabile ❑ non affidabile ❑ non può essere valutata
3. Esattezza dell'informazione o intelligence ❑ certa ❑ stabilita dalla fonte ❑ confermata per sentito dire ❑ non confermata per sentito dire

4 Il risultato delle indagini sul reato o dell'operazione di intelligence nel cui ambito è avvenuto lo scambio di informazioni deve essere riferito all'autorità che effettua la trasmissione

❑ no
❑ sì

5 In caso di scambio spontaneo: motivi che inducono a credere che l'informazione o intelligence possa contribuire all'individuazione o prevenzione di reati di cui all'articolo 2, paragrafo 2 della decisione quadro 2002/584/GAI o alle indagini su tali reati.

RITARDO - Non è possibile rispondere entro il termine previsto dall'articolo 4 della decisione quadro 2006/960/GAI

L' informazione o intelligence non può essere fornita entro il termine stabilito per i seguenti motivi:

Sarà probabilmente fornita entro:

❑ 1 giorno ❑ 2 giorni ❑ 3 giorni
❑ settimane
❑ 1 mese

❑ È stata richiesta l'autorizzazione di un'autorità giudiziaria.
Si prevede che la procedura per la concessione o il rifiuto dell'autorizzazione durerà … settimane

RIFIUTO - L'informazione o intelligence:
❑ non ha potuto essere trasmessa e richiesta a livello nazionale; o
❑ non può essere trasmessa, per uno o più dei seguenti motivi:

A - Motivo connesso con il controllo giudiziario che impedisce la trasmissione o richiede il ricorso all'assistenza giudiziaria reciproca

❑ l'autorità giudiziaria competente non ha autorizzato l'accesso e lo scambio per quanto riguarda l'informazione o intelligence

❑ l'informazione o intelligence richiesta è stata precedentemente ottenuta con mezzi coercitivi e la legislazione nazionale non ne consente la trasmissione

❑ l'informazione o intelligence non è in possesso

- delle autorità incaricate dell'applicazione della legge; o
- delle autorità pubbliche o di enti privati in un modo da essere disponibile alle autorità incaricate dell'applicazione della legge senza il ricorso a mezzi coercitivi

❑ B - la comunicazione dell'informazione o intelligence richiesta pregiudicherebbe interessi fondamentali della sicurezza nazionale o metterebbe a repentaglio il buon esito di un'indagine, di un'operazione di intelligence criminale in corso o la sicurezza di persone o sarebbe palesemente sproporzionata o irrilevante per lo scopo per cui è stata richiesta.

Se sono contrassegnate le caselle A o B, aggiungere, se ritenuto necessario, ulteriori informazioni o indicare la ragione per il rifiuto (facoltativo):

❑ D - L'autorità richiesta decide di rifiutare l'esecuzione, perché la richiesta riguarda, a norma della legislazione dello Stato membro richiesto, il reato seguente (specificare la natura e la qualificazione giuridica del reato).....
passibile di una pena privativa della libertà di un anno o meno

❑ E - L' informazione o intelligence richiesta non è disponibile

❑ F – L'informazione o intelligence richiesta è stata ottenuta da un altro Stato membro o da un paese terzo ed è soggetta al principio di specialità e lo Stato membro o il paese terzo in questione non ha dato il consenso alla trasmissione dell'informazione o intelligence.

ALLEGATO B

SCAMBIO DI INFORMAZIONI A NORMA DELLA DECISIONE QUADRO DEL CONSIGLIO 2006/960/GAI
FORMULARIO CHE DEVE ESSERE UTILIZZATO DALLO STATO CHE FA RICHIESTA DI INFORMAZIONI E INTELLIGENCE

Questo formulario è utilizzato per richiedere informazioni e intelligence a norma della decisione quadro 2006/960/GAI.

I - Informazione amministrativa

Autorità richiedente (denominazione, indirizzo, telefono, fax, posta elettronica, Stato membro) :	
Particolari del funzionario responsabile (facoltativo)	
Allo Stato membro seguente:	
Data e ora della richiesta :	
Numero di riferimento della richiesta:	

Richieste precedenti				
❑ È la prima richiesta relativa a questo caso				
❑ La richiesta è successiva ad altre relative allo stesso caso				
Richiesta precedente/richieste precedenti			Risposta/risposte	
	Data	Numero di riferimento (dello Stato membro richiedente)	Data	Numero di riferimento (dello Stato membro richesto)
1.				
2.				
3.				
4.				

Qualora la richiesta sia inviata a più autorità dello Stato membro richiesto si prega di specificare ciascun canale utilizzato	
❑UNE/Ufficiale di collegamento dell'Europol	❑ per informazione ❑ per esecuzione
❑ Ufficio centrale nazionale Interpol	❑ per informazione ❑ per esecuzione
❑ Sirene	❑ per informazione ❑ per esecuzione
❑ Ufficiale di collegamento	❑ per informazione ❑ per esecuzione
❑ Altro (si prega di specificare)	❑ per informazione ❑ per esecuzione
Qualora la stessa richiesta sia inviata a altri Stati membri si prega di specificare l'altro Stato membro e il canale utilizzato (facoltativo)	

II - Termini

p. m. : termini previsti dall'articolo 4 della decisione quadro 2006/960/GAI

A - Il reato è contemplato dall'articolo 2, paragrafo 2 della decisione quadro 2002/584/GAI

e

l'informazione o intelligence richiesta è conservata in una banca dati alla quale un'autorità incaricata dell'applicazione della legge può accedere direttamente

→ La richiesta è urgente → Termine: 8 ore con possibilità di proroga

→ La richiesta non è urgente → Termine : 1 settimana

B – Altri casi: termine: 14 giorni

❑ **Richiesta URGENTE**
❑ **Richiesta NON urgente**
Motivi dell'urgenza (ad esempio: le persone sospettate sono sottoposte a detenzione, il procedimento deve essere portato dinanzi al giudice prima di una data specifica):
Informazione o intelligence richiesta

TIPO DI REATO(I) O ATTIVITÀ CRIMINALE(I) OGGETTO DI INDAGINE
Descrizione delle circostanze del reato/dei reati, compresa la data, il luogo e il grado di partecipazione della persona che forma oggetto della richiesta di informazione o intelligence:

Natura del reato/dei reati

A – Applicazione dell'articolo 4, paragrafo 1 o paragrafo 3 della decisione quadro 2006/960/GAI

❑ A1. Il reato è punibile nello Stato membro richiedente con una pena detentiva della durata massima di almeno tre anni
E
A 2. Si tratta di uno o più dei seguenti reati:

- ❑ partecipazione a un'organizzazione criminale
- ❑ terrorismo
- ❑ tratta di esseri umani
- ❑ sfruttamento sessuale dei bambini e pornografia infantile
- ❑ traffico illecito di stupefacenti e sostanze psicotrope
- ❑ traffico illecito di armi, munizioni ed esplosivi
- ❑ corruzione
- ❑ frode, compresa la frode che lede gli interessi finanziari delle Comunità europee ai sensi della convenzione del 26 luglio 1995 relativa alla tutela degli interessi finanziari delle Comunità europee
- ❑ furti organizzati o con l'uso di armi
- ❑ traffico illecito di beni culturali, compresi gli oggetti d'antiquariato e le opere d'arte
- ❑ truffa
- ❑ racket e estorsioni
- ❑ contraffazione e pirateria in materia di prodotti
- ❑ falsificazione di atti amministrativi e traffico di documenti falsi
- ❑ falsificazione di mezzi di pagamento
- ❑ traffico illecito di sostanze ormonali ed altri fattori di crescita
- ❑ riciclaggio di proventi di reato
- ❑ falsificazione di monete, ivi compresa la contraffazione dell'euro
- ❑ criminalità informatica
- ❑ criminalità ambientale, compreso il traffico illecito di specie animali protette e il traffico illecito di specie e di essenze vegetali protette
- ❑ favoreggiamento dell'ingresso e del soggiorno illegali
- ❑ omicidio volontario, lesioni personali gravi
- ❑ traffico illecito di organi e tessuti umani
- ❑ rapimento, sequestro e presa di ostaggi
- ❑ razzismo e xenofobia
- ❑ traffico illecito di materie nucleari e radioattive
- ❑ traffico di veicoli rubati
- ❑ stupro
- ❑ incendio doloso
- ❑ reati che rientrano nella competenza giurisdizionale della Corte penale internazionale
- ❑ dirottamento di aereo/nave
- ❑ sabotaggio

→ Il reato è quindi contemplato dall'articolo 2, paragrafo 2 della decisione quadro relativa al mandato d'arresto europeo → Riguardo ai termini da rispettare per la risposta alla presente richiesta sono pertanto applicabili il paragrafo 1 (casi urgenti) e il paragrafo 3 (casi non urgenti) dell'articolo 4 della decisione quadro 2006/584/GAI.

Oppure

❑ B - Il reato/i reati non è (sono) contemplato (i) dalla lettera A.
In questo caso, fornire una descrizione del reato/dei reati:

Finalità della richiesta di informazioni o intelligence

Nesso tra la finalità della richiesta di informazioni o intelligence e la persona oggetto delle informazioni o dell'intelligence

Identità (se nota) della persona/delle persone oggetto principale dell'indagine penale o dell'operazione di intelligence criminale alla base della richiesta di informazioni o intelligence

Motivi che fanno ritenere che le informazioni o l'intelligence siano nello Stato membro richiesto

Restrizioni sull'utilizzo dell'informazione fornita nella richiesta per scopi diversi da quelli per cui è stata trasmessa o per la prevenzione di un pericolo grave e immediato per la pubblica sicurezza

- ❑ utilizzo autorizzato
- ❑ utilizzo autorizzato, ma non dev'essere menzionato chi ha fornito l'informazione
- ❑ utilizzo non permesso senza l'autorizzazione di chi ha fornito l'informazione
- ❑ utilizzo non permesso

Figura 2

RICHIESTA DI INFORMAZIONI E ANALISI (INTELLIGENCE)

Ai sensi della decisione quadro 2006/960/GAI del Consiglio

I – Informazioni amministrative

Stato membro richiedente	
Autorità richiedente (denominazione, indirizzo, telefono, fax, posta elettronica):	
Particolari del funzionario responsabile *(facoltativo)***:**	
Data e ora della richiesta:	
Numero di riferimento della richiesta:	
Numeri di riferimento precedenti:	

Stato/i membro/i richiesto/i:		
Canale		
☐UNE/Ufficiale di collegamento Europol	☐per informazione	☐per esecuzione
☐Ufficio centrale nazionale Interpol	☐per informazione	☐per esecuzione
☐SIRENE	☐per informazione	☐per esecuzione
☐Ufficiali di collegamento	☐per informazione	☐per esecuzione
☐Altro (specificare):	☐per informazione	☐per esecuzione

II – Urgenza

Urgenza richiesta	☐ Sì ☐ No
Motivi dell'urgenza (ad es. le persone sospettate sono sottoposte a detenzione, il procedimento deve essere portato dinanzi al giudice prima di una data specifica): Applicazione dell'articolo	
Reato ai sensi dell'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI relativa al mandato d'arresto europeo	☐ Sì ☐ No

III – Finalità

Tipo di reato(i) o attività criminale(i) oggetto di indagine
Descrizione: - circostanze del reato/dei reati (ad es. data, luogo e grado di partecipazione della persona che forma oggetto della richiesta di informazione o intelligence) - motivi che fanno ritenere che le informazioni o l'intelligence siano nello Stato membro richiesto - nesso tra la finalità della richiesta di informazioni o intelligence e la persona oggetto delle informazioni o dell'intelligence
☐ Richiesta di usare l'informazione come prova, se la normativa nazionale lo permette *(facoltativo)*

IV – Tipo di informazione

Identità (se nota) della persona/delle persone o identificazione dell'oggetto/degli oggetti	
Persona	Oggetto/i
Cognome: Cognome di nascita: Nome: Data di nascita: Luogo di nascita: Sesso: ☐maschile ☐femminile ☐non noto Cittadinanza: Altre informazioni:	Numero di serie dell'arma: Numero del documento: Altro numero o nome identificativo: Numero di immatricolazione del veicolo: Numero di serie del veicolo: Tipo di documenti: Estremi della società (n. telefono, posta elettronica, indirizzo, sito internet…): Altre informazioni:

Informazioni o analisi (intelligence) richieste		
Persona	Veicolo	Altro
☐ accertamento dell'identità ☐ verifiche nelle banche dati ☐ ricerca dell'indirizzo/domicilio	☐ compilazione dei dati d'identificazione ☐ identificazione del proprietario ☐ identificazione del conducente ☐ verifiche nelle banche dati	☐ identificazione di una società ☐ verifiche sulla società nelle banche dati ☐ verifiche di documenti nelle banche dati ☐ identificazione numero telefono/fax ☐ identificazione del titolare di un indirizzo di posta elettronica ☐ verifica di indirizzo ☐ verifica di armi ☐ rotta commerciale delle armi
Altri criteri:		

V - Codici di gestione

Restrizioni dell'uso dell'informazione fornita nella richiesta per scopi diversi da quelli per cui è stata trasmessa o per la prevenzione di un pericolo grave e immediato per la pubblica sicurezza
☐ solo per finalità di polizia, non accessibile a fini giudiziari ☐ contattare preliminarmente la fonte dell'informazione

3.3. Accordo di Schengen

3.3.1. Scambio di dati all'interno e all'esterno del SIS II

L'accordo di Schengen firmato il 14 giugno 1985 è stato integrato nel 1990 dalla convenzione di applicazione dell'accordo di Schengen (CAS)[81], che ha creato lo spazio Schengen attraverso l'abolizione dei controlli alle frontiere tra gli Stati Schengen, norme comuni in materia di visti e la cooperazione di polizia e giudiziaria. La CAS stabilisce un obbligo generale di cooperazione di polizia e autorizza le autorità di polizia a scambiare informazioni entro i limiti fissati dai rispettivi ordinamenti nazionali.

Con l'entrata in vigore del trattato di Amsterdam nel 1999, le misure di cooperazione fino ad allora presenti nel quadro di Schengen sono state integrate nel quadro giuridico dell'Unione europea e le questioni attinenti a Schengen sono oggi trattate dagli organi legislativi dell'UE. Il protocollo di Schengen allegato al trattato di Amsterdam ha stabilito disposizioni dettagliate per tale processo di integrazione.

Il sistema d'informazione Schengen (SIS) è stato istituito a norma delle disposizioni del titolo IV della convenzione del 19 giugno 1990. Rappresenta uno strumento fondamentale per l'applicazione dell'*acquis* di Schengen. Costituisce inoltre una misura intesa a compensare l'assenza di controlli sulle persone alle frontiere interne dello spazio Schengen attraverso uno strumento per lo scambio di informazioni tra le autorità competenti.

Il fatto che il quadro giuridico necessario per disciplinare il SIS consti attualmente di strumenti distinti non pregiudica il principio secondo il quale il SIS costituisce un unico sistema d'informazione. I tre nuovi regolamenti SIS non pregiudicano tale principio. Mirano a creare sinergie nella lotta contro il terrorismo e le forme gravi di criminalità, in particolare attraverso un migliore scambio di informazioni tra le autorità competenti. Sostengono inoltre la gestione delle frontiere e della migrazione e preparano il SIS all'interoperabilità con i sistemi IT dell'UE su larga scala, quali VIS, Eurodac, ETIAS ed EES.

---

81 Convenzione di applicazione dell'accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni, GU L 239 del 22.9.2000, pag. 19.

Legislazione

Regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II), GU L 381 del 28.12.2006, pag. 4.

Decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II), GU L 205 del 7.8.2007, pag. 63.

Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione, GU L 312 del 7.12.2018, pag. 56.

Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27.

Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85.

Disposizioni fondamentali

Il sistema d'informazione Schengen (SIS) è un sistema di cooperazione di polizia e di controllo delle frontiere e sostiene la cooperazione operativa fra autorità di polizia e giudiziarie in materia penale. Può essere consultato dagli agenti di polizia designati, dalle guardie di frontiera, dagli agenti doganali, dalle autorità competenti per i visti e dalle autorità giudiziarie di tutto lo spazio Schengen.[82]

Il sistema d'informazione Schengen di seconda generazione ("SIS II") è attualmente operativo in 26 Stati membri dell'UE nonché nei quattro paesi non membri dell'UE che sono associati alla cooperazione Schengen: Norvegia, Islanda, Svizzera e Liechtenstein.

- Per quanto riguarda la cooperazione di polizia, il Regno Unito e l'Irlanda hanno chiesto l'autorizzazione a parteciparvi, ma soltanto il Regno Unito è stato autorizzato, nel 2015, a caricare dati reali di tale parte del SIS[83] in via provvisoria come primo passo per consentire l'effettuazione della valutazione prima dell'adozione di una decisione finale di "messa in applicazione". Il Regno Unito e l'Irlanda non partecipano all'applicazione del SIS ai fini del controllo alle frontiere.

- Bulgaria, Romania[84] e Croazia[85] applicano le disposizioni dell'*acquis* di Schengen relative alla cooperazione di polizia e al controllo alle frontiere. A tali paesi è stato concesso l'accesso in tempo reale ai fini della valutazione della corretta applicazione delle disposizioni dell'*acquis* di Schengen relative al SIS. Una volta effettuate in modo soddisfacente le valutazioni, una decisione del Consiglio distinta definirà una data per la soppressione dei controlli alle frontiere interne. Fino a tale data, permangono talune restrizioni all'uso del SIS.

---

82 Un elenco consolidato delle autorità competenti indicante per ciascuna autorità i dati che essa può consultare e a quali fini è pubblicato annualmente nella Gazzetta ufficiale dell'UE conformemente all'articolo 31, paragrafo 8, del regolamento SIS e all'articolo 46, paragrafo 8, della decisione SIS II.

83 Decisione di esecuzione (UE) 2015/215 del Consiglio, del 10 febbraio 2015, relativa all'applicazione delle disposizioni dell'*acquis* di Schengen in materia di protezione dei dati e all'applicazione provvisoria di parti delle disposizioni dell'*acquis* di Schengen relativamente al sistema d'informazione Schengen nei confronti del Regno Unito di Gran Bretagna e Irlanda del Nord, GU L 36 del 12.2.2015, pag. 8.

84 Decisione 2010/365/UE del Consiglio, del 29 giugno 2010, sull'applicazione delle disposizioni dell'acquis di Schengen relative al sistema d'informazione Schengen nella Repubblica di Bulgaria e in Romania, GU L 166 dell'1.7.2010, pag. 17.

85 Decisione (UE) 2017/733 del Consiglio, del 25 aprile 2017, sull'applicazione delle disposizioni dell'acquis di Schengen relative al sistema d'informazione Schengen nella Repubblica di Croazia, GU L 108 del 26.4.2017, pag. 31.

- Cipro non ha ancora accesso al SIS.

I dati SIS II possono essere consultati in linea (nel rispetto di rigorose norme in materia di protezione dei dati), 24 ore su 24 e 7 giorni su 7, attraverso gli uffici SIRENE, nei posti di controllo delle frontiere, sul territorio nazionale e presso i consolati all'estero. I dati sono denominati segnalazioni; una segnalazione è un insieme di dati che consente alle autorità di identificare **persone**, vale a dire cittadini europei e non, od **oggetti** al fine di intraprendere azioni appropriate per la lotta alla criminalità e all'immigrazione irregolare.

Il personale di Europol specificatamente autorizzato ha il diritto, nei limiti del proprio mandato, di accedere e consultare direttamente i dati inseriti nel SIS II e può chiedere ulteriori informazioni allo Stato membro interessato.

I membri nazionali di Eurojust e i loro assistenti hanno il diritto, nei limiti del proprio mandato, di accedere e consultare i dati inseriti nel SIS II.

Ai sensi dell'articolo 47 della CAS, i funzionari di collegamento distaccati presso le autorità di polizia di altri Stati Schengen o di paesi terzi sono responsabili dello scambio di informazioni a norma degli articoli:

- 39, paragrafi 1, 2 e 3, in conformità del diritto nazionale ai fini della prevenzione e della ricerca di fatti punibili;

- articolo 46, anche di propria iniziativa, ai fini della prevenzione di reati o di minacce per l'ordine pubblico e la sicurezza.

Occorre notare che le disposizioni dell'articolo 39, paragrafi 1, 2 e 3, e dell'articolo 46, nella misura in cui riguardano lo scambio di informazioni e di intelligence attinenti a forme gravi di criminalità, sono sostituite da quelle della decisione quadro 2006/960/GAI del Consiglio, la "decisione quadro svedese". Tuttavia, le disposizioni dell'articolo 39, paragrafi 1, 2 e 3, e dell'articolo 46 restano applicabili per quanto riguarda reati passibili di una pena privativa della libertà di durata inferiore a 12 mesi.

3.3.2. Rifusione del Sistema d'informazione Schengen

Legislazione

Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare, GU L 312 del 7.12.2018, pag. 1.

Regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006, GU L 312 del 7.12.2018, pag. 14.

Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione, GU L 312 del 7.12.2018, pag. 56.

Disposizioni fondamentali

Tre anni dopo l'entrata in funzione del SIS II, la Commissione ha svolto una valutazione del sistema. La rifusione del SIS II tiene conto di tale valutazione e della partecipazione dei diversi Stati membri dell'UE alle politiche UE nello spazio di libertà, sicurezza e giustizia. I tre regolamenti introducono una serie di miglioramenti al SIS che accresceranno la sua efficacia, rafforzeranno la protezione dei dati ed estenderanno i diritti di accesso. Sostengono inoltre la gestione delle frontiere e della migrazione e spianano la strada all'interoperabilità del SIS con i sistemi IT dell'UE su larga scala[86].

I regolamenti contengono disposizioni specifiche per gli Stati membri che godono di uno status speciale per quanto riguarda Schengen e le misure nello spazio di libertà, sicurezza e giustizia del TFUE, ossia Danimarca, Irlanda, Croazia, Bulgaria, Romania e Cipro.

---

86 Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85

Le disposizioni del regolamento (UE) 2018/1862 sull'esercizio e l'uso del SIS nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale riguardano, in particolare:

- nuove categorie di segnalazioni sia su persone, come "ignoti ricercati" e "controllo di indagine", l'estensione della categoria "persone scomparse" alle "persone vulnerabili a cui deve essere impedito di viaggiare", sia su oggetti, come "oggetti di elevato valore";
- obbligo per gli Stati membri di segnalare nel SIS i casi connessi a reati di terrorismo;
- norme relative all'informazione di Europol in caso di riscontro positivo (hit) per segnalazioni su reati di terrorismo;
- norme relative all'uso, a fini di identificazione, di dati biometrici, quali immagini del volto e fotografie, ove tecnicamente possibile[87], impronte digitali, impronte palmari e, in particolare, profili DNA ai fini soltanto dell'identificazione delle persone scomparse;
- conferimento di diritti di accesso a fini di contrasto alle autorità competenti per l'immigrazione, ai servizi competenti per l'immatricolazione di natanti e aeromobili e ai servizi preposti alla registrazione di armi da fuoco; a Europol affinché possa avere pieno accesso al SIS, compreso alle segnalazioni relative a persone scomparse e ai rimpatri e alle segnalazioni relative a cittadini di paesi terzi, e possa scambiare e richiedere ulteriori informazioni supplementari in conformità delle disposizioni del manuale SIRENE; all'Agenzia europea della guardia di frontiera e costiera (Frontex) e alle sue squadre, nella misura in cui sia necessario all'assolvimento dei loro compiti e come richiesto dal piano operativo per una specifica operazione delle guardie di frontiera;
- una maggiore protezione e sicurezza dei dati grazie a salvaguardie aggiuntive per limitare la raccolta e il trattamento dei dati, e l'accesso ai medesimi, a quanto strettamente necessario e indispensabile dal punto di vista operativo, attraverso l'applicazione del quadro dell'UE in materia di protezione dei dati, in particolare la direttiva 2016/680 e il regolamento generale sulla protezione dei dati, attraverso il coordinamento e la sorveglianza da punto a punto delle autorità nazionali preposte alla protezione dei dati e del garante europeo della protezione dei dati.

---

87 In un primo momento si dovrebbe poter ricorrere a immagini del volto e a fotografie a fini di identificazione solo presso valichi di frontiera regolari. Tale ricorso dovrebbe essere oggetto di una relazione della Commissione che confermi la disponibilità, lo stato di preparazione e l'affidabilità della tecnologia necessaria. In una fase successiva, la Commissione potrebbe adottare atti riguardo alla determinazione dei casi in cui è possibile ricorrere a fotografie e immagini del volto per identificare le persone in un contesto diverso da quello dei valichi di frontiera regolari.

3.4. Europol

Legislazione

Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI, GU L 135 del 24.5.2016, pag. 53 (applicabile a decorrere dal 1º maggio 2017).

Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27.

Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85.

Disposizioni fondamentali

L'obiettivo di Europol è sostenere e rafforzare l'azione delle autorità competenti degli Stati membri preposte alla prevenzione e alla lotta contro la criminalità, e la loro cooperazione reciproca intesa a prevenire e combattere la criminalità organizzata, il terrorismo e altre forme gravi di criminalità che interessano due o più Stati membri. A tal fine, Europol raccoglie, conserva, tratta, analizza e scambia informazioni e intelligence criminale.

Ogni Stato membro designa un'unità nazionale (UNE) che funge da organo di collegamento tra Europol e le autorità competenti negli Stati membri. Le UNE svolgono compiti connessi alla condivisione di informazioni e intelligence pertinenti. Ogni unità nazionale distacca almeno un ufficiale di collegamento che costituisce l'ufficio di collegamento nazionale presso Europol e rappresenta gli interessi dell'unità nazionale. Gli ufficiali di collegamento sono incaricati della condivisione di informazioni, da un lato, tra gli Stati membri e l'Europol, e, dall'altro, a livello bilaterale tra altri paesi. Tali scambi bilaterali possono riguardare reati che esulano dal mandato di Europol.

Il regolamento Europol introduce un nuovo concetto per il trattamento dei dati, comunemente indicato come concetto di gestione integrata dei dati (Integrated Data Management Concept - IDMC). L'IDMC può essere definito come la possibilità di utilizzare le informazioni relative alla criminalità per molteplici fini commerciali quali indicati dal proprietario dei dati, consentendone una gestione e un trattamento integrati e tecnologicamente neutrali. In base alla decisione del Consiglio che istituiva Europol, il trattamento dei dati era strutturato attorno a sistemi. Il regolamento Europol non contiene più riferimenti a sistemi, ma richiede invece l'indicazione delle finalità del trattamento. Per agevolare una transizione fluida, gli utenti possono continuare a operare con i sistemi esistenti in un modo che sia conforme al nuovo quadro giuridico.

L'unità nazionale è responsabile della comunicazione con il sistema di informazione Europol (SIE) utilizzato per il trattamento dei dati necessari per lo svolgimento dei compiti di Europol. Le unità nazionali, gli ufficiali di collegamento e il personale di Europol debitamente autorizzato hanno il diritto di introdurre e reperire dati nei sistemi. Le informazioni inserite nel SIE sono considerate in generale come fornite a fini di controlli incrociati (articolo 18, paragrafo 2, lettera a), del regolamento) e di analisi strategiche/tematiche (articolo 18, paragrafo 2, lettera b), del regolamento).

3.5. Agenzia europea della guardia di frontiera e costiera (Frontex)

Legislazione

Regolamento (UE) 2019/1896 del Parlamento europeo e del Consiglio, del 13 novembre 2019, relativo alla guardia di frontiera e costiera europea e che abroga i regolamenti (UE) n. 1052/2013 e (UE) 2016/1624, GU L 295 del 14.11.2019, pag. 1 (applicabile dal 4 dicembre 2019).

Il regolamento (UE) n. 1052/2013 che istituisce il sistema europeo di sorveglianza delle frontiere (EUROSUR) prevede un quadro comune per lo scambio di informazioni e per la cooperazione tra gli Stati membri e Frontex al fine di migliorare la conoscenza situazionale e di aumentare la capacità di reazione alle frontiere esterne degli Stati membri dell'Unione ("frontiere esterne"), al fine di individuare, prevenire e combattere l'immigrazione clandestina e la criminalità transfrontaliera e contribuire a garantire la protezione e la salvezza della vita dei migranti ("EUROSUR"). Il regolamento EUROSUR è stato abrogato e sostituito dal regolamento (UE) 2019/1896, che reca disposizioni rivedute su EUROSUR.

Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27.

Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85.

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, GU L 236 del 19.09.2018, pag. 1.

Disposizioni fondamentali

L'obiettivo della guardia di frontiera e costiera europea è quello di garantire una gestione europea integrata alle frontiere esterne, allo scopo di gestire tali frontiere efficacemente e nel pieno rispetto dei diritti fondamentali e aumentare l'efficienza della politica dei rimpatri dell'Unione.

L'Agenzia europea della guardia di frontiera e costiera - Frontex (l'Agenzia) affronta le sfide migratorie e le potenziali sfide e minacce future alle frontiere esterne. Al fine di prevenire, individuare e combattere la criminalità transfrontaliera alle frontiere esterne, garantisce un livello elevato di sicurezza interna nell'Unione, nel pieno rispetto dei diritti fondamentali, salvaguardando al contempo la libera circolazione delle persone al suo interno.

Ogni Stato membro designa un punto di contatto nazionale per la comunicazione con l'Agenzia su tutte le questioni attinenti alle attività della stessa, fatto salvo il ruolo dei centri nazionali di coordinamento. Gli Stati membri possono designare fino a due membri da assegnare quali funzionari di collegamento presso l'Agenzia in rappresentanza del loro punto di contatto nazionale.

Ogni Stato membro istituisce, attiva e gestisce un centro nazionale di coordinamento che provvede al coordinamento e allo scambio di informazioni tra tutte le autorità responsabili del controllo delle frontiere esterne a livello nazionale, nonché con gli altri centri nazionali di coordinamento e con l'Agenzia.

Il regolamento relativo alla guardia di frontiera e costiera europea istituisce EUROSUR quale quadro integrato per lo scambio di informazioni e la cooperazione operativa all'interno della stessa guardia di frontiera e costiera europea, inteso a migliorare la conoscenza situazionale e ad aumentare la capacità di reazione ai fini della gestione delle frontiere al fine di prevenire, individuare e combattere l'immigrazione illegale e la criminalità transfrontaliera e garantire la protezione e la salvezza della vita dei migranti. L'Agenzia coordina i servizi EUROSUR per la fusione dei dati, al fine di fornire ai centri nazionali di coordinamento, alla Commissione e a sé medesima informazioni sulle frontiere esterne e sulla zona pre-frontaliera su base regolare e in modo affidabile ed economicamente efficiente.

Nell'attuazione del regolamento ETIAS, l'Agenzia provvederà a istituire l'unità centrale ETIAS. L'unità, operativa 24 ore al giorno, sette giorni su sette, è incaricata di verificare, laddove dal trattamento automatizzato della domanda emerga un riscontro positivo, se i dati personali del richiedente corrispondono ai dati personali della persona per cui è emerso tale riscontro positivo. Nel caso in cui una corrispondenza sia confermata o permangano dubbi, l'unità centrale ETIAS avvia il trattamento manuale della domanda. Nell'attuazione del regolamento sull'interoperabilità, per un periodo di un anno dopo che eu-LISA comunica il completamento del collaudo del MID e prima dell'entrata in funzione di quest'ultimo, l'unità centrale ETIAS è competente per effettuare le rilevazioni di identità multiple usando i dati conservati nell'EES, nel VIS, nell'Eurodac e nel SIS.

Nell'attuazione del mandato dell'Agenzia europea della guardia di frontiera e costiera (Frontex), l'Agenzia ha esaminato in che modo le informazioni ottenute prima dell'arrivo di un viaggiatore alle frontiere esterne (informazioni anticipate) possano essere utilizzate per perfezionare l'analisi del rischio viaggiatori. L'attenzione si è incentrata sul vaglio delle capacità esistenti e sull'individuazione di nuovi metodi per ottimizzare tale analisi, che migliora il processo decisionale relativo all'attraversamento delle frontiere e offre nel contempo maggiori agevolazioni ai viaggiatori in buona fede.

Gli orientamenti sulle informazioni anticipate contribuiscono all'elaborazione di profili per meglio individuare in anticipo i viaggiatori che destano interesse; contribuiscono anche alla creazione di capacità di definizione degli obiettivi. Frontex ha avviato un corso di formazione specifico sulle informazioni anticipate per assistere gli Stati membri nella creazione di capacità di analisi armonizzate ("capacità di definizione degli obiettivi") ai fini della gestione delle frontiere.

Inoltre, uno studio avviato nel gennaio 2020 esamina l'uso delle informazioni anticipate sui viaggiatori che entrano nello spazio Schengen attraverso le frontiere esterne terrestri e marittime. Uno dei principali obiettivi dello studio è individuare, descrivere e definire le migliori prassi relative alla raccolta e al trattamento di tali informazioni anticipate.

3.6. Interpol

Legislazione

Costituzione di Interpol[88].

Norme che disciplinano il trattamento delle informazioni[89].

Regolamento relativo al controllo delle informazioni e all'accesso agli archivi di INTERPOL.

Disposizioni fondamentali

La missione di Interpol consiste nel facilitare la cooperazione internazionale tra forze di polizia per la prevenzione e la lotta alla criminalità attraverso un rafforzamento della cooperazione e dell'innovazione su questioni di polizia e di sicurezza. Sono intraprese azioni entro i limiti fissati dalle leggi vigenti negli Stati membri e nello spirito della Dichiarazione universale dei diritti dell'uomo. Ciascuno dei 190 Stati membri dispone di un ufficio centrale nazionale (UCN) il cui personale è composto da propri funzionari di contrasto altamente formati.

La costituzione di Interpol è un accordo internazionale che conferma, in qualità di membri, i governi di tutti i paesi che hanno partecipato alla sua adozione nel 1956 e stabilisce la procedura di presentazione della domanda di adesione a Interpol da parte dei paesi che non erano membri nel 1956.

---

88 http://www.interpol.int/en/About-INTERPOL/Legal-materials/The-Constitution
89 http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts

In quanto principale documento giuridico, la costituzione enuncia le finalità e gli obiettivi di Interpol. Essa stabilisce il mandato dell'organizzazione per garantire la più ampia cooperazione possibile tra tutte le autorità di polizia criminale e per reprimere i reati di diritto comune.

Il quadro giuridico di Interpol è composto, oltre che dalla costituzione, da una serie di testi fondamentali. Per garantire il rispetto delle norme, sono stati istituiti diversi livelli di controllo connessi ai controlli effettuati dagli uffici centrali nazionali (UCN), dal segretariato generale e dall'organo di monitoraggio indipendente noto come la commissione per il controllo dei fascicoli di Interpol.

3.7. Ufficiali di collegamento

Legislazione

Convenzione di applicazione dell'accordo di Schengen (CAS) del 19 giugno 1990,[90] articolo 47.

Decisione 2003/170/GAI del Consiglio, del 27 febbraio 2003, relativa all'utilizzo comune degli ufficiali di collegamento distaccati all'estero dalle autorità degli Stati membri incaricate dell'applicazione della legge[91].

Decisione 2006/560/GAI del Consiglio, del 24 luglio 2006, recante modifica della decisione 2003/170/GAI relativa all'utilizzo comune degli ufficiali di collegamento distaccati all'estero dalle autorità degli Stati membri incaricate dell'applicazione della legge[92].

Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI, GU L 135 del 24.5.2016, pag. 53 (applicabile a decorrere dal 1º maggio 2017).

Decisione 2008/615/GAI del Consiglio sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, GU L 210 del 6.8.2008, pag. 1.

Accordi bilaterali

---

90 Convenzione di applicazione dell'accordo di Schengen (CAS) del 19 giugno 1990, GU L 239 del 22.9.2000, pag. 19.

91 Decisione 2003/170/GAI del Consiglio, del 27 febbraio 2003, GU L 67 del 12.3.2003, pag. 27.

92 Decisione 2006/560/GAI del Consiglio, del 24 luglio 2006, GU L 219 del 10.8.2006, pag. 31.

Disposizioni fondamentali

L'articolo 47 della CAS dispone che gli Stati membri "possono concludere accordi bilaterali che consentono il distacco, a tempo determinato o indeterminato, di funzionari di collegamento di un[o] [Stato membro] presso i servizi di polizia dell'altr[o] [Stato membro]". Gli ufficiali di collegamento non hanno il potere di eseguire autonomamente misure di polizia e l'articolo 47 precisa che tali distacchi sono intesi a "promuovere ed accelerare la cooperazione [...], soprattutto fornendo assistenza:

a) in forma di scambio di informazioni per la lotta preventiva e repressiva contro la criminalità;

b) nell'esecuzione di richieste di mutua assistenza giudiziaria e fra polizie in materia penale;

c) per le esigenze inerenti allo svolgimento dei compiti delle autorità incaricate della sorveglianza delle frontiere esterne."

Maggiori informazioni su tali distacchi sono reperibili nel "manuale per il settore calcistico"[93] e nella raccomandazione del Consiglio, del 6 dicembre 2007, relativa a un manuale per le autorità di polizia e di sicurezza concernente la cooperazione in occasione di eventi importanti di dimensione internazionale[94].

La disposizione della CAS in base alla quale gli ufficiali di collegamento nazionali possono anche rappresentare gli interessi di uno o più altri Stati membri è stata ulteriormente sviluppata dalla decisione del Consiglio relativa all'utilizzo comune degli ufficiali di collegamento distaccati all'estero dalle autorità degli Stati membri incaricate dell'applicazione della legge (modificata nel 2006). È previsto, inoltre, un miglioramento della cooperazione tra gli ufficiali di collegamento di diversi Stati membri nel loro luogo di distacco. La necessità di incoraggiare tale cooperazione è stata sottolineata in varie sedi.

---

93 Risoluzione del Consiglio, del 3 giugno 2010, concernente un manuale aggiornato di raccomandazioni per la cooperazione internazionale tra forze di polizia e misure per prevenire e combattere la violenza e i disordini in occasione delle partite di calcio di dimensione internazionale alle quali è interessato almeno uno Stato membro, GU C 165 del 24.6.2010, pag. 1.

94 GU C 314 del 22.12.2007, pag. 4.

Conformemente al regolamento Europol, ogni Stato membro designa un'unità nazionale (UNE) che funge da organo di collegamento tra Europol e le autorità competenti degli Stati membri preposte alla prevenzione e alla lotta contro i reati. Le UNE svolgono compiti connessi alla condivisione di informazioni e intelligence pertinenti. Ogni unità nazionale distacca almeno un ufficiale di collegamento che costituisce l'ufficio di collegamento nazionale presso Europol e rappresenta gli interessi dell'unità nazionale. Gli ufficiali di collegamento sono incaricati della condivisione di informazioni, da un lato, tra l'unità nazionale e l'Europol, e, dall'altro, a livello bilaterale con altre unità nazionali. Tali scambi bilaterali possono riguardare reati che esulano dal mandato di Europol.

La decisione 2008/615/GAI del Consiglio ("decisione Prüm") prevede, agli articoli 17 e 18, il distacco di ufficiali nazionali al fine di mantenere l'ordine e la sicurezza pubblici e prevenire i reati.

3.8. Scambio di dati "Prüm"

Legislazione

- Decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera.

- Decisione 2008/616/GAI del Consiglio, del 23 giugno 2008, relativa all'attuazione della decisione 2008/615/GAI sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, GU L 210 del 6.8.2008, pag. 12.

Disposizioni fondamentali

Gli Stati membri si concedono reciprocamente l'accesso in linea transfrontaliero ai dati indicizzati di schedari nazionali designati di analisi del DNA e dei sistemi automatizzati di identificazione dattiloscopica (AFIS), nonché ai dati di immatricolazione dei veicoli (cfr. capo 2 della decisione 2008/615/GAI del Consiglio).

In ogni Stato membro è necessario designare specifici punti di contatto nazionali. La legislazione nazionale deve tener conto in modo adeguato delle disposizioni in materia di protezione e sicurezza dei dati. Il raffronto automatizzato dei profili biometrici anonimi si basa su un sistema di riscontro positivo o negativo ("hit/no hit"), tranne nel caso di dati di immatricolazione dei veicoli, dove si ottengono automaticamente i dati del proprietario/intestatario cercati.

Nel caso di una concordanza biometrica, il PCN dello Stato membro richiedente riceve, mediante un procedimento automatizzato, i dati indicizzati con cui è stata trovata una concordanza.

Dati personali specifici aggiuntivi e ulteriori informazioni relative ai dati indicizzati possono essere poi richiesti mediante procedure di assistenza reciproca, comprese quelle adottate ai sensi della "decisione quadro svedese".

La fornitura di tali dati supplementari è disciplinata dalla legislazione nazionale dello Stato membro richiesto, ivi incluse le norme relative all'assistenza giudiziaria. Resta inteso che la fornitura di dati personali richiede un livello adeguato di protezione dei dati da parte degli Stati membri riceventi.[95]

Per la prevenzione di reati e nell'interesse del mantenimento dell'ordine e della sicurezza pubblici durante eventi di rilievo a dimensione transfrontaliera, gli Stati membri possono, sia su richiesta che di propria iniziativa, trasmettersi dati personali e non personali. A tal fine, sono designati specifici punti di contatto nazionali (PCN) (cfr. capo 3 della decisione 2008/615/GAI del Consiglio).

Allo scopo di prevenire i reati terroristici, in determinate circostanze gli Stati membri possono trasmettersi dati personali. A tal fine, sono designati specifici punti di contatto nazionali (cfr. capo 4 della decisione 2008/615/GAI del Consiglio).

3.9. Sistema d'informazione visti (VIS)

Legislazione

Decisione del Consiglio, dell'8 giugno 2004, che istituisce il sistema di informazione visti (VIS) (2004/512/CE), GU L 213 del 15.6.2004, pag. 5.

[95] La decisione 2008/615/GAI del Consiglio soddisfa il livello di protezione prescritto per il trattamento dei dati personali dalla convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, dal protocollo aggiuntivo dell'8 novembre 2001 della convenzione, nonché dai principi della raccomandazione R (87) 15 del Consiglio d'Europa che disciplina l'uso di dati personali nel settore della polizia.

Decisione 2013/392/UE del Consiglio che fissa la data di decorrenza degli effetti della decisione 2008/633/GAI relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi, GU L 198 del 23.7.2013, pag. 45.[96]

Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27.

Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85.

Disposizioni fondamentali

Il VIS è un sistema che consente alle autorità nazionali competenti di inserire e aggiornare dati relativi ai visti per soggiorni di breve durata (cosiddetti Schengen), nonché di consultare tali dati per via elettronica. Si basa su un'architettura centralizzata ed è costituito da un sistema d'informazione centrale, il sistema centrale d'informazione sui visti (CS-VIS), da un'interfaccia nazionale in ciascuno Stato membro (NI-VIS) e dall'infrastruttura di comunicazione tra il CS-VIS e l'NI-VIS. La decisione 2008/633/GAI consente di utilizzare il VIS per prevenire, individuare e investigare su reati di terrorismo e altri reati gravi. Permette alle autorità di contrasto designate (quali le autorità responsabili della lotta al terrorismo o ad altri reati gravi, per esempio il traffico di droga o la tratta di esseri umani) nei paesi dello spazio Schengen, e a Europol di accedere al VIS. Le autorità nazionali designate devono seguire una procedura per accedere al VIS una volta soddisfatte tutte le condizioni di accesso.

---

96 Il 16 aprile 2015 la Corte di giustizia ha annullato la decisione 2013/392/UE del Consiglio, del 22 luglio 2013, che fissa la data di decorrenza degli effetti della decisione 2008/633/GAI relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi. Ciononostante, la Corte ha dichiarato che gli effetti della decisione 2013/392 dovevano essere mantenuti fino all'entrata in vigore di un nuovo atto diretto a sostituirla.

Nel maggio 2018 la Commissione ha presentato una proposta legislativa di modifica del regolamento VIS mirante, tra l'altro, a garantire l'interoperabilità tra le altre banche dati del settore GAI registrando nel VIS i visti per soggiorni di lunga durata e i permessi di soggiorno. Inoltre, la proposta include e sviluppa ulteriormente le norme di accesso al VIS delle autorità di contrasto, abrogando la decisione 2008/633/GAI.

Il VIS potenziato non dovrebbe essere operativo prima della fine del 2021.

3.10. Eurodac

Legislazione

Il sistema automatico europeo per il riconoscimento delle impronte digitali (Eurodac) è un sistema informatico originariamente concepito per facilitare l'efficace l'applicazione della convenzione di Dublino. La convenzione di Dublino, firmata il 15 giugno 1990, è stata sostituita dal regolamento (CE) n. 343/2003 del Consiglio, del 18 febbraio 2003, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda d'asilo presentata in uno degli Stati membri da un cittadino di un paese terzo.

Dopo essere stati modificati, i regolamenti relativi all'Eurodac sono stati rifusi dai seguenti atti.

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), GU L 180 del 29.6.2013, pag. 1.

Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27.

Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85.

Disposizioni fondamentali

Il regolamento n. 603/2013 stabilisce le finalità dell'Eurodac e definisce le condizioni di accesso, da parte delle autorità di contrasto nazionali designate e di Europol, ai dati Eurodac a fini di prevenzione, accertamento o indagine di reati di terrorismo[97] o di altri reati gravi[98].

3.11. Napoli II

Legislazione

Atto del Consiglio del 18 dicembre 1997 che stabilisce la convenzione, in base all'articolo K.3 del trattato sull'Unione europea, relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali, pubblicato nella GU C 24 del 23.1.1998, pag. 1.

---

97 Decisione quadro 2002/475/GAI del Consiglio, del 13 giugno 2002, sulla lotta contro il terrorismo, GU L 164 del 22.6.2002, pag. 3.

98 Decisione quadro 2002/584/GAI del Consiglio, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri, GU L 190 del 18.7.2002, pag. 1.

Disposizioni fondamentali

Gli Stati membri si assistono reciprocamente al fine di prevenire e accertare le violazioni delle disposizioni doganali nazionali nonché perseguire e punire violazioni delle disposizioni doganali comunitarie e nazionali. Nell'ambito delle indagini penali, la convenzione "Napoli II" introduce procedure che consentono alle amministrazioni doganali di agire in comune e di scambiarsi, spontaneamente o su richiesta, dati relativi ai traffici illeciti.

Le domande sono presentate per iscritto in una delle lingue ufficiali dello Stato membro dell'autorità richiesta o in una lingua accettata da quest'ultima. In un formulario è definita la norma per la comunicazione delle informazioni. Le autorità interessate comunicano tutte le informazioni che possono fornire assistenza alla prevenzione, all'accertamento e al perseguimento delle violazioni. Si scambiano dati personali, vale a dire qualsiasi informazione concernente una persona fisica identificata o identificabile.

Nell'assistenza da fornire, l'autorità richiesta o l'autorità competente cui quest'ultima si rivolge procede come se agisse per conto proprio o su richiesta di un'altra autorità del proprio Stato membro.

3.11.1. Sistema d'informazione doganale - SID[99]

Il sistema d'informazione doganale integra la convenzione "Napoli II"[100]. Il sistema d'informazione centralizzato è gestito dalla Commissione e mira a rafforzare l'amministrazione doganale degli Stati membri attraverso un rapido scambio di informazioni al fine di prevenire, accertare e perseguire gravi infrazioni al diritto nazionale e comunitario. Il SID istituisce inoltre un archivio d'identificazione dei fascicoli a fini doganali (FIDE) per prestare assistenza alle indagini doganali.

---

99 Decisione 2009/917/GAI del Consiglio, del 30 novembre 2009, sull'uso dell'informatica nel settore doganale, GU L 323 del 10.12.2009, pag. 20.

100 Convenzione stabilita in base all'articolo K.3, del trattato sull'Unione europea relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali, GU C 24 del 23.1.1998, pag. 2.

Le autorità designate dagli Stati membri[101] hanno accesso diretto ai dati contenuti nel SID. Al fine di rafforzare la complementarità con Europol ed Eurojust, entrambi gli organismi hanno accesso in sola lettura al SID e al FIDE.

Il SID comprende dati personali raggruppati secondo le seguenti categorie: merci, mezzi di trasporto, imprese, persone e merci e denaro contante bloccati, sequestrati o confiscati. I dati personali immessi nel SID possono essere copiati in altri sistemi di trattamento dei dati soltanto a fini di gestione dei rischi o di analisi operativa e possono essere consultati soltanto dagli analisti designati dagli Stati membri.

Il FIDE consente alle autorità nazionali preposte alle indagini doganali, quando istruiscono un fascicolo, di individuare le altre autorità che possono aver indagato sulle persone o sulle imprese in questione.

3.12. Uffici nazionali per il recupero dei beni (URB) e CARIN

Legislazione

Decisione 2007/845/GAI del Consiglio, del 6 dicembre 2007, concernente la cooperazione tra gli uffici degli Stati membri per il recupero dei beni nel settore del reperimento e dell'identificazione dei proventi di reato o altri beni connessi, GU L 332 del 18.12.2007, pag. 103.

La rete interagenzie Camden per il recupero dei beni (CARIN) è stata istituita all'Aia il 22-23 settembre 2004 da Austria, Belgio, Germania, Irlanda, Paesi Bassi e Regno Unito.

[101] Attuazione dell'articolo 7, paragrafo 2, e dell'articolo 8, paragrafo 3, della decisione 2009/917/GAI del Consiglio, del 30 novembre 2009, sull'uso dell'informatica nel settore doganale - elenchi aggiornati delle autorità competenti, doc. 13394/11 ENFOCUSTOM 85.

Disposizioni fondamentali

In seguito all'adozione della decisione 2007/845/GAI del Consiglio[102], tutti gli Stati membri hanno istituito e designato uffici per il recupero dei beni (URB), i quali possono scambiarsi direttamente informazioni su questioni relative al recupero dei beni tramite il sistema SIENA. Sotto l'egida della Commissione europea e di Europol, la rete degli URB facilita la cooperazione tra gli URB degli Stati membri, la discussione strategica e lo scambio di migliori pratiche. L'Ufficio Europol per i proventi criminali (Europol Criminal Assets Bureau - ECAB) funge da punto focale per il recupero dei beni nell'UE.

Le disposizioni di cui alla direttiva 2014/42/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa al congelamento e alla confisca dei beni strumentali e dei proventi da reato nell'Unione europea[103] miglioreranno ulteriormente l'efficacia della cooperazione tra gli uffici per il recupero dei beni nell'Unione europea. Gli Stati membri sono tenuti a recepire la direttiva entro il 4 ottobre 2016.

La rete interagenzie Camden per il recupero dei beni (CARIN), istituita nel 2004 per sostenere l'identificazione, il congelamento, il sequestro e la confisca a livello transfrontaliero di beni connessi a reati, promuove lo scambio reciproco di informazioni relative ai diversi approcci nazionali anche al di là dell'UE.

Dal 2015 la rete CARIN include operatori di 53 giurisdizioni e 9 organizzazioni internazionali che fungono da punti di contatto ai fini del rapido scambio di informazioni a livello transfrontaliero, su richiesta o spontaneamente. Gli URB nazionali cooperano tra loro o con le altre autorità che facilitano il reperimento e l'identificazione dei proventi di reato. Sebbene tutti gli Stati membri abbiano istituito un URB, tra essi esistono notevoli differenze in termini di assetto organizzativo, risorse e attività.

---

102 Decisione 2007/845/GAI del Consiglio, del 6 dicembre 2007, concernente la cooperazione tra gli uffici degli Stati membri per il recupero dei beni nel settore del reperimento e dell'identificazione dei proventi di reato o altri beni connessi, GU L 332 del 18.12.2007, pag. 103.

103 Direttiva 2014/42/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa al congelamento e alla confisca dei beni strumentali e dei proventi da reato nell'Unione europea, GU L 127 del 29.4.2014, pag. 39.

Le informazioni scambiate possono essere utilizzate in conformità delle disposizioni in materia di protezione dei dati dello Stato membro ricevente e sono soggette a norme di protezione dei dati identiche a quelle applicabili se fossero raccolte nello Stato membro ricevente. Occorre promuovere lo scambio spontaneo di informazioni in linea con la presente decisione, applicando le procedure e le tempistiche previste dalla decisione quadro svedese.

3.13. Unità di informazione finanziaria (FIU)

Legislazione

Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 658/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione
GU L 141 del 5.6.2015, pag. 73

Direttiva (UE) 2019/1153 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati, e che abroga la decisione 2000/642/GAI del Consiglio
GU L 186 dell'11.7.2019, pag. 122

Disposizioni fondamentali

A norma della direttiva 2015/849 (la quarta direttiva antiriciclaggio - o direttiva AML, modificata dalla direttiva 2018/843), ciascuno Stato membro istituisce una FIU per prevenire, individuare e combattere efficacemente il riciclaggio e il finanziamento del terrorismo. La FIU in quanto unità nazionale centrale ha la responsabilità di ricevere e analizzare le segnalazioni di operazioni sospette ed altre informazioni che riguardano attività di riciclaggio, reati presupposto associati o attività di finanziamento del terrorismo. La FIU ha la responsabilità di comunicare alle autorità competenti i risultati delle sue analisi e qualsiasi altra informazione pertinente qualora vi siano motivi di sospettare attività di riciclaggio, reati presupposto associati o attività di finanziamento del terrorismo. Essa può acquisire informazioni ulteriori dai soggetti obbligati. Le FIU devono essere in grado di rispondere alle richieste di informazioni ad esse rivolte da autorità competenti dei rispettivi Stati membri qualora tali richieste di informazioni siano motivate da esigenze relative ad attività di riciclaggio, reati presupposto associati o attività di finanziamento del terrorismo.

Oltre al suddetto scambio relativo al riciclaggio e al finanziamento del terrorismo, la direttiva (UE) 2019/1153 dispone che ciascuno Stato membro provvede affinché la FIU nazionale sia tenuta a cooperare con le rispettive autorità di contrasto designate di detto Stato e sia in grado di rispondere alle richieste motivate di informazioni finanziarie o di analisi finanziarie che siano motivate da esigenze relative alla prevenzione, all'accertamento, all'indagine o al perseguimento di reati gravi, quali definiti nell'allegato I del regolamento Europol (2016/794).

In entrambi i casi, la FIU può rifiutare di fornire le informazioni qualora vi siano ragioni oggettive per supporre che questo abbia un impatto negativo su indagini in corso o qualora la comunicazione delle informazioni sia palesemente sproporzionata rispetto agli interessi legittimi di una persona fisica o giuridica oppure non sia pertinente agli scopi per cui è stata richiesta.

A norma della direttiva 2015/849 (direttiva AML), gli Stati membri provvedono affinché le FIU si scambino, spontaneamente o su richiesta, ogni informazione che possa risultare loro utile per il trattamento o l'analisi di informazioni da parte delle FIU collegate al riciclaggio o al finanziamento del terrorismo e alle persone fisiche o giuridiche implicate, indipendentemente dal tipo di reati presupposto eventualmente associato e anche laddove il tipo di reati presupposto eventualmente associato non sia stato individuato al momento dello scambio. Una FIU può rifiutare di scambiare informazioni solo in circostanze eccezionali, se lo scambio potrebbe essere contrario ai principi fondamentali del suo diritto nazionale. Gli Stati membri provvedono affinché le informazioni scambiate ai sensi degli articoli 52 e 53 siano utilizzate solo ai fini per cui sono state richieste o fornite.

In aggiunta allo scambio tra le FIU di differenti Stati membri a norma della direttiva 2015/849, la direttiva 2019/1153 ora dispone che in casi urgenti ed eccezionali le rispettive FIU siano inoltre autorizzate a scambiare informazioni finanziarie o analisi finanziarie che potrebbero essere pertinenti per il trattamento o l'analisi di informazioni connesse al terrorismo o alla criminalità organizzata associata al terrorismo. La direttiva 2019/1153 autorizza inoltre lo scambio di informazioni tra le FIU ed Europol.

FIU.NET è una rete informatica decentralizzata per lo scambio di informazioni tra FIU.

FIU.NET, originariamente intesa a rafforzare la posizione delle FIU, negli ultimi anni, da strumento di base sicuro per lo scambio bilaterale strutturato di informazioni, si è trasformata in uno strumento sicuro multifunzionale per lo scambio multilaterale di informazioni, con funzionalità di gestione dei fascicoli nonché una standardizzazione semiautomatica dei processi. Su FIU.NET ogni nuova caratteristica e ogni nuovo processo automatizzato sono opzionali e non soggetti a condizioni. Le singole FIU possono decidere quali possibilità e caratteristiche offerte da FIU.NET utilizzare; ricorrono soltanto alle funzioni che ritengono convenienti ed escludono quelle di cui non hanno bisogno o che non desiderano utilizzare.

3.14. Accordo UE/USA sul programma di controllo delle transazioni finanziarie dei terroristi (TFTP)

Legislazione

Accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi,
GU L 195 del 27.7.2010, pag. 5

Disposizioni fondamentali

All'indomani dell'11 settembre, l'UE e gli USA hanno deciso di collaborare strettamente e hanno concluso l'accordo sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (accordo TFTP UE-USA). Ai sensi dell'accordo, il dipartimento del Tesoro degli Stati Uniti mette le informazioni relative al TFTP a disposizione anche delle autorità di contrasto, di pubblica sicurezza o antiterrorismo degli Stati membri interessati e, se del caso, di Europol ed Eurojust.

Il TFTP è dotato di solide misure di controllo per garantire il rispetto di salvaguardie, ivi comprese quelle in materia di protezione dei dati personali. I dati sono trattati esclusivamente a fini di prevenzione, indagine, accertamento o perseguimento nei confronti del terrorismo o del suo finanziamento. Ai fini dell'accordo, il dipartimento del Tesoro degli Stati Uniti può richiedere ai fornitori designati di servizi internazionali di messaggistica finanziaria dati di messaggistica relativi ai pagamenti finanziari e dati connessi conservati nel territorio dell'UE.

I vantaggi derivanti dai dati TFTP per gli Stati membri, Europol ed Eurojust sono limitati dal fatto che l'analisi dei pagamenti transfrontalieri effettuata nel quadro del TFTP si fonda esclusivamente sui messaggi FIN (Financial Institution Transfer - messaggi di trasferimento degli istituti finanziari), un tipo di messaggio SWIFT mediante il quale le informazioni finanziarie sono trasferite da un istituto finanziario all'altro. Non sono presi in considerazione altri metodi di pagamento. Tuttavia, il TFTP è l'unico meccanismo che, ai fini di una maggiore sicurezza interna, consente di procedere, in un periodo di tempo molto breve, alla mappatura e alla profilazione delle operazioni sospettate di essere connesse al terrorismo o al finanziamento del terrorismo. Grazie a una maggiore consapevolezza delle clausole di reciprocità di cui all'accordo, le autorità dell'UE applicano sempre di più tale meccanismo in modo da beneficiare dello scambio di dati con gli Stati Uniti. Va osservato, al riguardo, che tutte le richieste di consultazione del TFTP da parte delle autorità dell'UE devono soddisfare i requisiti di cui all'articolo 10 dell'accordo.

Sebbene l'accordo non preveda che gli Stati membri richiedano tramite Europol una ricerca al fine di ottenere informazioni tramite il TFTP, per migliorare la risposta dell'UE al terrorismo e al suo finanziamento sarebbe utile che gli Stati membri almeno informino Europol in modo sistematico e tempestivo delle proprie richieste dirette ai sensi dell'articolo 10. Per aiutare gli Stati membri a convogliare le richieste di consultazione del TFTP, Europol ha istituito uno sportello unico (punto di contatto unico - SPOC). Grazie al suo ambiente basato sull'archivio di lavoro per fini di analisi e alla cooperazione consolidata con il dipartimento del Tesoro degli Stati Uniti, esso è adatto a gestire efficacemente le richieste degli Stati membri.

3.15. Scambio di informazioni sui casellari giudiziali (ECRIS)

Legislazione

Decisione quadro 2009/315/GAI del Consiglio, del 26 febbraio 2009, relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario, GU L 93 del 7.4.2009, pag. 23. Tale decisione quadro abroga la decisione 2005/876/GAI del Consiglio, del 21 novembre 2005, relativa allo scambio di informazioni estratte dal casellario giudiziario, GU L 322 del 9.12.2005, pag. 33.

Direttiva (UE) 2019/884 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio, GU L 151 del 7.6.2019, pag. 143.

Disposizioni fondamentali

La decisione quadro 2009/315/GAI del Consiglio impone a uno Stato membro di condanna di trasmettere quanto prima possibile, allo o agli Stati membri di cittadinanza, tutte le informazioni iscritte nel casellario giudiziale relative a condanne, nonché modifiche o soppressioni delle stesse. Lo Stato membro di cittadinanza è tenuto a conservare le informazioni a fini di ritrasmissione. Qualsiasi modifica o soppressione effettuata nello Stato membro di condanna comporta un'identica modifica o soppressione nel casellario giudiziale dello Stato membro di cittadinanza. Le informazioni su condanne possono essere richieste dallo Stato membro di cittadinanza ai fini di un procedimento penale o a fini diversi dal procedimento penale, come prevenire un pericolo grave e immediato per la pubblica sicurezza. Tuttavia, l'uso delle informazioni trasmesse a titolo di questa decisione a fini diversi da un procedimento penale può essere limitato conformemente al diritto interno dello Stato membro richiesto e dello Stato membro richiedente al fine di non compromettere le possibilità di riabilitazione sociale della persona condannata.

La decisione 2009/316/GAI del Consiglio definisce le modalità secondo le quali uno Stato membro deve trasmettere tali informazioni. Detta decisione del Consiglio stabilisce il quadro per un sistema informatizzato di scambio di informazioni estratte dal casellario giudiziale. Le autorità centrali di ciascuno Stato membro utilizzano gli appositi moduli di richiesta e di risposta allegati alla decisione quadro mediante la procedura elettronica descritta nella legislazione.

3.15.1. Scambio di informazioni sui casellari giudiziali in ordine a cittadini di paesi terzi e apolidi (ECRIS-TCN)

Legislazione

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 cittadini 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, GU L 135 del 22.5.2019, pag. 1.

Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27.

Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85.

Direttiva (UE) 2019/884 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che modifica la decisione quadro 2009/315/GAI del Consiglio per quanto riguarda lo scambio di informazioni sui cittadini di paesi terzi e il sistema europeo di informazione sui casellari giudiziali (ECRIS), e che sostituisce la decisione 2009/316/GAI del Consiglio, GU L 151 del 7.6.2019, pag. 143.

Disposizioni fondamentali

Il regolamento si applica al trattamento delle informazioni sull'identità di cittadini di paesi terzi che siano stati oggetto di condanne negli Stati membri. Per "cittadino di paese terzo" si intende chiunque non sia cittadino dell'Unione ai sensi dell'articolo 20, paragrafo 1, TFUE, l'apolide o qualsiasi persona la cui cittadinanza è ignota. I casellari giudiziali riguardanti queste persone sono conservati nello Stato membro di condanna. Lo scopo dell'ECRIS-TCN[104] è verificare quali altri Stati membri siano in possesso di informazioni sul casellario giudiziale. Il quadro ECRIS può pertanto essere utilizzato per richiedere tali informazioni a quegli Stati membri conformemente alla decisione quadro 2009/315/GAI.

Il regolamento stabilisce le norme che istituiscono un sistema contenente dati personali, il cui sviluppo e la cui manutenzione fanno capo a eu-LISA e che è centralizzato a livello di Unione, e le norme sulla ripartizione delle responsabilità tra gli Stati membri e sull'organizzazione responsabile dello sviluppo e della manutenzione del sistema centralizzato. Esso prevede globalmente un livello adeguato di protezione e sicurezza dei dati e di salvaguardia dei diritti fondamentali degli interessati.

Eurojust, Europol ed EPPO dovrebbero avere accesso all'ECRIS-TCN al fine di individuare gli Stati membri in possesso di informazioni sul casellario giudiziale di un cittadino di paese terzo, ai fini dello svolgimento dei loro compiti statutari.

3.16. Conservazione di dati sulle telecomunicazioni

Legislazione

Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.[105]

---

[104] La Commissione determinerà la data a partire dalla quale l'ECRIS-TCN entrerà in funzione una volta soddisfatte le condizioni di cui all'articolo 35 del regolamento (UE) 2019/816.

[105] La sentenza della Corte di giustizia dell'Unione europea dell'8 aprile 2014 ha dichiarato la direttiva invalida.

Disposizioni fondamentali

La direttiva si applica ai fornitori di servizi di comunicazione elettronica e afferma che questi ultimi dovrebbero conservare i dati relativi al traffico e i dati relativi all'ubicazione, nonché i dati connessi necessari per identificare l'abbonato o l'utente, al fine di comunicarli alle autorità nazionali competenti che ne facciano richiesta. A fini di indagine, accertamento e perseguimento di forme gravi di criminalità, gli Stati membri obbligano i fornitori di servizi di comunicazione elettronica o di reti pubbliche di comunicazione a conservare le categorie di dati necessari per determinare:

- la fonte di una comunicazione;
- la destinazione di una comunicazione;
- la data, l'ora e la durata di una comunicazione;
- il tipo di comunicazione;
- le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature;
- l'ubicazione delle apparecchiature di comunicazione mobile.

Non può essere conservato alcun dato relativo al contenuto della comunicazione.

3.17. Direttiva sul codice di prenotazione (PNR)

Legislazione

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

Disposizioni fondamentali

La direttiva stabilisce, a livello dell'Unione, un quadro giuridico comune per il trasferimento e il trattamento dei dati PNR e prevede:

a) il trasferimento a cura dei vettori aerei[106] dei dati del codice di prenotazione (PNR) dei passeggeri sui voli extra-UE. Se uno Stato membro decide di applicare la direttiva ai voli intra-UE, tutte le disposizioni si applicano ai voli intra-UE come se fossero voli extra-UE;

b) il trattamento dei dati PNR, comprese le operazioni di raccolta, uso e conservazione a cura degli Stati membri e il loro scambio tra gli Stati membri.

Ai fini del trattamento dei dati PNR, ciascuno Stato membro istituisce o designa un'autorità competente che agisca in qualità di "unità d'informazione sui passeggeri" (UIP). Due o più Stati membri possono istituire o designare una stessa autorità che agisca in qualità di UIP comune.

I dati PNR, che figurano nell'allegato I della direttiva, devono essere trasferiti alle UIP a condizione che siano già raccolti dai vettori aerei nel normale svolgimento della loro attività. Alcuni vettori conservano informazioni anticipate sui passeggeri (API) come parte dei dati PNR, mentre altri non lo fanno. Indipendentemente dalla maniera in cui i vettori arerei raccolgono i dati API, questi devono essere trasferiti alle UIP che li trattano nello stesso modo dei dati PNR. L'allegato II della direttiva contiene l'elenco dei "reati gravi" nell'ambito di applicazione della direttiva.

Il trattamento dei dati PNR serve per la valutazione dei passeggeri prima del loro arrivo in uno Stato membro o della partenza da esso allo scopo di identificare le persone da sottoporre a ulteriore verifica da parte delle autorità competenti a fini di prevenzione, accertamento, indagine e perseguimento nei confronti di reati di terrorismo e altri reati gravi e, se del caso, da parte di Europol entro i limiti delle sue competenze e per l'adempimento dei suoi compiti.

---

106 La direttiva non pregiudica la possibilità che gli Stati membri istituiscano, ai sensi del diritto nazionale, un sistema di raccolta e trattamento dei dati PNR provenienti da operatori economici diversi dai vettori aerei, come le agenzie di viaggio e gli operatori turistici, che forniscono servizi connessi ai viaggi, fra cui la prenotazione di voli per i quali raccolgono e trattano dati PNR, o da imprese di trasporto diverse da quelle previste nella direttiva, purché tale diritto nazionale sia conforme al diritto dell'Unione.

Per effettuare la valutazione le UIP possono:

a) confrontare i dati PNR rispetto a banche dati pertinenti a fini di prevenzione, accertamento, indagine e perseguimento nei confronti di reati di terrorismo e altri reati gravi, comprese le banche dati riguardanti persone od oggetti ricercati o segnalati, conformemente alle norme dell'Unione, internazionali e nazionali applicabili a tali banche dati, o

b) trattare i dati PNR sulla base di criteri prestabiliti.

A livello nazionale, le UIP trasmettono i dati PNR o i risultati del loro trattamento alle autorità nazionali di contrasto competenti autorizzate a effettuare un'ulteriore verifica del fascicolo o interventi appropriati per prevenire, accertare, indagare e perseguire reati di terrorismo e altri reati gravi. Mentre le UIP costituiscono il principale canale di scambio di informazioni a livello transfrontaliero, le autorità competenti possono rivolgersi direttamente alle UIP di un altro Stato membro in caso di emergenza e a condizioni ben definite.

A livello dell'Unione, le UIP scambiano sia i dati PNR raccolti presso i vettori aerei che i risultati del trattamento di tali dati tra di loro e con Europol che, entro i limiti delle sue competenze e per l'adempimento dei suoi compiti, ha diritto di chiedere tali dati alle UIP.

I dati PNR devono essere conservati in una banca dati presso le UIP per un periodo di cinque anni dal loro trasferimento dallo Stato membro di arrivo o di partenza del volo. Tuttavia tutti i dati PNR sono resi anonimi dopo un periodo di sei mesi. Ciò deve esser fatto mediante la mascheratura degli elementi di dati che potrebbero servire a identificare direttamente il passeggero cui i dati si riferiscono. L'elenco dei dati PNR da mascherare figura nella direttiva. Dopo cinque anni i dati PNR devono essere cancellati a meno che non siano stati trasferiti a un'autorità competente a fini di prevenzione, accertamento, indagine e perseguimento di reati di terrorismo e altri reati gravi, nel qual caso la loro conservazione è disciplinata dal diritto nazionale.

Conformemente alla normativa dell'UE in materia di protezione dei dati, la direttiva PNR vieta il trattamento di dati sensibili quali l'origine razziale o etnica, le opinioni politiche, la religione o le convinzioni filosofiche, l'appartenenza sindacale, lo stato di salute, la vita sessuale o l'orientamento sessuale.

3.18. Informazioni anticipate sui passeggeri (API)

Legislazione

Direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate

Disposizioni fondamentali

La direttiva è intesa a migliorare i controlli alle frontiere e combattere l'immigrazione irregolare. A tal fine, la direttiva impone agli Stati membri di stabilire l'obbligo per i vettori aerei di comunicare determinate informazioni relative ai loro viaggiatori prima del loro ingresso nell'Unione europea. Tali informazioni sono denominate "informazioni anticipate sui passeggeri" (API). In determinate condizioni e circostanze gli Stati membri possono altresì utilizzare i dati API a fini di contrasto.

Le informazioni sono trasmesse su richiesta delle autorità preposte all'esecuzione dei controlli delle persone alle frontiere esterne dell'UE.

I vettori aerei dovrebbero trasmettere i dati API in forma elettronica o, in caso di guasto, con altro mezzo appropriato, alle autorità che eseguono i controlli di frontiera nel luogo in cui il passeggero entra nell'UE. I dati API sono verificati rispetto alle banche dati nazionali ed europee quali il sistema d'informazione Schengen (SIS) e il sistema d'informazione visti (VIS).

Quando i dati API corrispondono a una voce in una banca dati (elenco di controllo), una segnalazione è inviata alla polizia di frontiera e il passeggero corrispondente è selezionato per la verifica all'arrivo. In caso di corrispondenza con un profilo di rischio, si crea un obiettivo. I dati API raccolti e trasmessi devono essere cancellati dai vettori e dalle autorità entro 24 ore dalla trasmissione o dall'arrivo. Tuttavia le autorità di frontiera possono conservare i file provvisori oltre le 24 ore se i dati sono necessari successivamente per l'esercizio delle loro funzioni regolamentari o per l'applicazione della normativa in materia di ingresso e immigrazione, incluse le relative disposizioni sulla tutela dell'ordine pubblico ("*ordre public*") e della sicurezza nazionale.

3.19. Infrazioni in materia di sicurezza stradale

Legislazione

Direttiva (UE) 2015/413 del Parlamento europeo e del Consiglio, dell'11 marzo 2015, intesa ad agevolare lo scambio transfrontaliero di informazioni sulle infrazioni in materia di sicurezza stradale, GU L 68 del 13.3.2015, pag. 9.

Disposizioni fondamentali

Gli Stati membri si concedono reciprocamente l'accesso in linea ai propri dati nazionali di immatricolazione dei veicoli per l'applicazione di sanzioni relative a determinate infrazioni in materia di sicurezza stradale commesse con un veicolo immatricolato in uno Stato membro diverso da quello in cui l'infrazione è stata commessa. Lo Stato membro dell'infrazione utilizza i dati ottenuti per stabilire la responsabilità personale dell'infrazione stradale. Lo scambio di informazioni riguarda:

- eccesso di velocità;
- mancato uso della cintura di sicurezza;
- mancato arresto davanti a un semaforo rosso;
- guida in stato di ebbrezza;
- guida sotto l'influsso di sostanze stupefacenti;
- mancato uso del casco protettivo;
- circolazione su una corsia vietata;
- uso illecito di telefono cellulare o di altri dispositivi di comunicazione durante la guida.

Mediante la specifica applicazione informatica EUCARIS, gli Stati membri consentono reciprocamente ai rispettivi punti di contatto nazionali (PCN) designati di accedere ai dati di immatricolazione dei veicoli, con la facoltà di effettuare consultazioni automatizzate sui:

a) dati relativi ai veicoli e

b) dati relativi ai proprietari o agli intestatari del veicolo.

3.20. Sistema di ingressi/uscite (EES)

Legislazione

Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011, GU L 327 del 9.12.2017, pag. 20.

Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27.

Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85.

Il regolamento costituisce uno sviluppo delle disposizioni dell'*acquis* di Schengen.

La Danimarca ha notificato che ha deciso di attuare i suddetti regolamenti nel diritto danese, a norma dell'articolo 4 del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea. Tale decisione creerà un obbligo a norma del diritto internazionale tra la Danimarca e gli altri Stati membri vincolati dalle misure.

Il Regno Unito e l'Irlanda non partecipano all'*acquis* e pertanto non sono vincolati dal regolamento né sono soggetti alla sua applicazione.

L'Islanda, la Norvegia, il Liechtenstein e la Svizzera sono vincolati dall'*acquis* ai sensi del rispettivo accordo o protocollo concernente l'*acquis* di Schengen.

Per quanto riguarda Cipro, la Bulgaria, la Romania e la Croazia, le disposizioni del regolamento riguardanti il SIS e il VIS costituiscono disposizioni basate sull'*acquis* di Schengen o a esso altrimenti connesse, ai sensi dei rispettivi atti di adesione.

Disposizioni fondamentali

Il regolamento[107] specifica gli obiettivi dell'EES, le categorie di dati da inserirvi, le finalità per le quali i dati devono essere utilizzati, i criteri di inserimento dei dati, le autorità autorizzate ad accedere ai dati, ulteriori norme sul trattamento dei dati e sulla protezione dei dati personali, nonché l'architettura tecnica dell'EES, le norme relative al suo funzionamento e utilizzo e l'interoperabilità con altri sistemi d'informazione. Gli obiettivi dell'EES consistono nel migliorare la gestione delle frontiere esterne, nel prevenire l'immigrazione irregolare e nel facilitare la gestione dei flussi migratori. A tal fine l'EES è concepito per registrare e conservare la data, l'ora e il luogo d'ingresso e di uscita di determinati cittadini di paesi terzi che attraversano le frontiere degli Stati membri presso cui l'EES è operativo. In aggiunta, l'EES può essere consultato a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi da parte delle autorità di contrasto nazionali[108].

---

107 La Commissione determinerà la data a partire dalla quale l'EES entrerà in funzione una volta soddisfatte le condizioni di cui all'articolo 66 del regolamento (UE) 2017/2226.

108 "Reati di terrorismo": il reato che corrisponde o è equivalente a uno dei reati di cui alla direttiva (UE) 2017/541; "reato grave": il reato che corrisponde o è equivalente a uno dei reati di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI, se è punibile conformemente al diritto nazionale con una pena detentiva o una misura di sicurezza privativa della libertà personale per un periodo massimo di almeno tre anni.

L'EES è composto da un sistema centrale (sistema centrale dell'EES), che gestisce una banca dati centrale informatizzata di dati biometrici e alfanumerici, un'interfaccia uniforme nazionale in ciascuno Stato membro. Un canale di comunicazione sicuro connette il sistema centrale dell'EES e il sistema centrale d'informazione visti (sistema centrale del VIS), e un'infrastruttura di comunicazione sicura e criptata connette il sistema centrale dell'EES all'interfaccia uniforme nazionale. È stabilita l'interoperabilità tra l'EES e il VIS mediante un canale diretto di comunicazione tra i loro sistemi centrali affinché le autorità di frontiera possano consultare il VIS a partire dall'EES e le autorità competenti per i visti possano consultare l'EES a partire dal VIS.

Il regolamento stabilisce rigorose norme relative all'accesso all'EES. Stabilisce inoltre i diritti individuali di accesso, rettifica, completamento, cancellazione e ricorso, in particolare il diritto a un ricorso giurisdizionale, e il controllo del trattamento dei dati da parte di autorità pubbliche indipendenti.

Il regolamento rispetta i diritti fondamentali ed è conforme ai principi riconosciuti dalla Carta dei diritti fondamentali dell'UE. Fatte salve le norme più specifiche di cui al regolamento concernenti il trattamento dei dati personali, al trattamento dei dati personali in applicazione di questo regolamento si applica il regolamento (UE) 2016/679[109] (regolamento generale sulla protezione dei dati), tranne il caso in cui tale trattamento sia effettuato dalle autorità di contrasto designate o dai punti di accesso centrale degli Stati membri, nel qual caso si applica la direttiva (UE) 2016/680[110] (direttiva polizia).

---

109 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), GU L 119 del 4.5.2016, pag. 1.

110 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2019, 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, GU L 119 del 4.5.2016, pag. 89.

3.21. Sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)

Legislazione

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, GU L 236 del 19.9.2018, pag. 1.

Regolamento (UE) 2018/1241 del Parlamento europeo e del Consiglio, del 12 settembre 2018, recante modifica del regolamento (UE) 2016/794 ai fini dell'istituzione di un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), GU L 236 del 19.9.2018, pag. 72.

Il regolamento 2018/1240[111] precisa gli obiettivi dell'ETIAS, ne definisce l'architettura tecnica e organizzativa, stabilisce le norme relative al suo funzionamento e all'uso dei dati che il richiedente deve inserire nel sistema e le norme sul rilascio o rifiuto dell'autorizzazione ai viaggi, stabilisce le finalità del trattamento dei dati, identifica le autorità con diritto di accesso ai dati e garantisce la protezione dei dati personali.

Il regolamento costituisce uno sviluppo delle disposizioni dell'*acquis* di Schengen. Il Regno Unito e l'Irlanda non partecipano all'*acquis* e pertanto non sono vincolati dal regolamento né sono soggetti alla sua applicazione. L'Islanda, la Norvegia, il Liechtenstein e la Svizzera sono vincolati dall'*acquis* ai sensi del rispettivo accordo o protocollo concernente l'*acquis* di Schengen.

Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27.

---

[111] La Commissione determinerà la data a partire dalla quale l'ETIAS entrerà in funzione una volta soddisfatte le condizioni di cui all'articolo 88 del regolamento (UE) 2018/1240.

Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85.

Disposizioni fondamentali

L'ETIAS rilascia un'autorizzazione ai viaggi, che per sua natura è diversa da un visto ma costituisce una condizione per l'ingresso e il soggiorno nello spazio Schengen, e indica che il richiedente l'autorizzazione ai viaggi non presenta un rischio per la sicurezza, di immigrazione illegale o un alto rischio epidemico nell'Unione.

L'ETIAS consta degli elementi seguenti:

- un sistema IT su larga scala, ossia il sistema d'informazione dell'ETIAS, che è progettato, sviluppato e gestito tecnicamente da eu-LISA;
- l'unità centrale ETIAS, che è parte dell'Agenzia europea della guardia di frontiera e costiera;
- le unità nazionali ETIAS, competenti per l'esame delle domande e la decisione se rilasciare o rifiutare, annullare o revocare le autorizzazioni ai viaggi. A tal fine, le unità nazionali dovrebbero cooperare tra loro e con Europol per valutare le domande.

L'accesso ai dati personali nell'ETIAS dovrebbe essere limitato al personale strettamente autorizzato e in nessun caso l'accesso dovrebbe essere utilizzato per giungere a decisioni basate su una qualche forma di discriminazione. Per quanto riguarda le autorità di contrasto designate dagli Stati membri, il trattamento dei dati conservati nel sistema centrale ETIAS dovrebbe avvenire solo in casi specifici e solo quando necessario a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi. Le autorità designate ed Europol dovrebbero chiedere l'accesso all'ETIAS soltanto quando abbiano fondati motivi per ritenere che tale accesso fornisca informazioni che contribuiranno alla prevenzione, all'accertamento o all'indagine di reati di terrorismo o altri reati gravi.

Il regolamento rispetta i diritti fondamentali ed è conforme ai principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea. Per quanto riguarda il trattamento dei dati personali, garanzie adeguate tendono pertanto a limitare l'ingerenza nel diritto al rispetto della vita privata e nel diritto alla protezione dei dati di carattere personale a quanto necessario e proporzionato in una società democratica.

Al trattamento dei dati personali in applicazione di questo regolamento si applica il regolamento (UE) 2016/679[112] (regolamento generale sulla protezione dei dati), tranne il caso in cui tale trattamento sia effettuato dalle autorità di contrasto designate o dai punti di accesso centrale degli Stati membri, nel qual caso si applica la direttiva (UE) 2016/680[113] (direttiva polizia).

3.22. Normativa in materia di interoperabilità

Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27.

Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85.

---

112 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, GU L 119 del 4.5.2016, pag. 1.

113 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2019, 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, GU L 119 del 4.5.2016, pag. 89.

Disposizioni fondamentali

Il regolamento (UE) 2019/817 e il regolamento (UE) 2019/818 costituiscono il "pacchetto interoperabilità" e riguardano i dati personali conservati in sistemi di informazione che sono centralizzati a livello dell'UE. I regolamenti sono volti a migliorare l'architettura di gestione dei dati dell'Unione per la gestione delle frontiere e la sicurezza. Pertanto il quadro del "pacchetto interoperabilità" si applica al trattamento dei dati personali nel settore delle frontiere e dei visti o nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione. L'interoperabilità tra questi sistemi di informazione sottostanti dovrebbe consentire agli stessi di integrarsi reciprocamente al fine di conseguire meglio i rispettivi obiettivi.

I regolamenti adattano inoltre le procedure e le condizioni per l'accesso delle autorità designate e di Europol all'EES, al VIS, all'ETIAS e all'Eurodac a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi.

Le componenti tecniche dell'interoperabilità riguardano l'EES (cfr. punto 3.20), il VIS (cfr. punto 3.9), l'ETIAS (cfr. punto 3.21), Eurodac (cfr. punto 3.10), il SIS (cfr. punto 3.3) e l'ECRIS-TCN (cfr. punto 3.15.1). Le componenti dell'interoperabilità[114] sono:

- un portale di ricerca europeo (ESP), inteso quale interfaccia unica o mediatore di messaggi ("message broker"), che permette l'interrogazione parallela dei suddetti strumenti dell'UE, dei dati Europol e delle banche dati Interpol. Le interrogazioni sono limitate ai dati riguardanti persone o documenti di viaggio;

- un servizio comune di confronto biometrico (BMS comune), il cui scopo principale è agevolare l'identificazione di una persona che è registrata in diverse banche dati utilizzando un'unica componente tecnologica per far corrispondere i dati biometrici di quella persona contenuti in diversi sistemi. I template AFIS in uso dovrebbero essere riuniti e conservati nel BMS in un unico luogo;

[114] La Commissione determinerà la data a partire dalla quale si applicheranno le disposizioni dei regolamenti relativi all'ESP, al BMS comune, al CIR e al MID.

- un archivio comune di dati di identità (CIR), inteso quale contenitore comune per i dati di identità, i dati dei documenti di viaggio e biometrici delle persone registrate nell'EES, nel VIS, nell'ETIAS, nell'Eurodac e nell'ECRIS-TCN. Questi dati possono riferirsi alla stessa persona ma con identità differenti o incomplete. Una migliore accuratezza dell'identificazione dovrebbe essere raggiunta attraverso il confronto e l'abbinamento automatizzati dei dati. Il CIR prevede verifiche di identità da parte delle autorità di contrasto designate al fine di sostenere i loro sforzi per identificare una persona;

- un rilevatore di identità multiple (MID), che sostiene il funzionamento del CIR.

Le nuove operazioni di trattamento dei dati previste dal regolamento costituiscono un'ingerenza nei diritti fondamentali tutelati dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'UE. Poiché l'attuazione efficace dei sistemi di informazione dell'UE dipende dalla corretta identificazione delle persone interessate, tale ingerenza è in linea con gli stessi obiettivi per i quali ciascuno di questi sistemi è stato istituito, vale a dire: la gestione efficace delle frontiere dell'Unione, la sicurezza interna dell'Unione e l'attuazione efficace delle politiche dell'Unione in materia di asilo e di visti.

Il regolamento (UE) 2016/679 si applica al trattamento dei dati personali finalizzato all'interoperabilità, a meno che tale trattamento non sia effettuato dalle autorità di contrasto designate o dai punti di accesso centrale degli Stati membri a fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi. In questo caso si applica la direttiva (UE) 2016/680 (cfr. punto 3.0).

Le autorità di controllo di cui al regolamento (UE) 2016/679 o alla direttiva (UE) 2016/680 dovrebbero verificare la liceità del trattamento dei dati personali da parte degli Stati membri. Il garante europeo della protezione dei dati dovrebbe sorvegliare le attività delle istituzioni e degli organi dell'Unione connesse al trattamento dei dati personali.