Consiglio dell'Unione europea

Bruxelles, 23 dicembre 2016
(OR. en)

15814/16

Fascicolo interistituzionale: 2016/0409 (COD)

SIRIS 178
ENFOPOL 501
COPEN 404
SCHENGEN 22
COMIX 863
CODEC 1945

PROPOSTA

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	22 dicembre 2016
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2016) 883 final
Oggetto:	Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO 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 il regolamento (UE) n. 515/2014 e abroga il regolamento (CE) n. 1986/2006, la decisione 2007/533/GAI del Consiglio e la decisione 2010/261/UE della Commissione

Si trasmette in allegato, per le delegazioni, il documento COM(2016) 883 final.

All.: COM(2016) 883 final

COMMISSIONE
EUROPEA

Bruxelles, 21.12.2016
COM(2016) 883 final

2016/0409 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

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 il regolamento (UE) n. 515/2014 e abroga il regolamento (CE) n. 1986/2006, la decisione 2007/533/GAI del Consiglio e la decisione 2010/261/UE della Commissione

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

Nel corso degli ultimi due anni l'Unione europea ha affrontato contemporaneamente tre sfide distinte: la gestione della migrazione, la gestione integrata delle frontiere esterne dell'UE e la lotta contro il terrorismo e la criminalità transfrontaliera. Per fornire una valida risposta a tali sfide e per costruire un'efficace e autentica Unione della sicurezza, è essenziale un efficace scambio di informazioni tra gli Stati membri, e tra gli Stati membri e le agenzie competenti dell'UE.

Il sistema d'informazione Schengen (SIS) è lo strumento più utile per una cooperazione efficace tra le autorità competenti per l'immigrazione, la polizia, le autorità doganali e le autorità giudiziarie nell'UE e nei paesi associati a Schengen. Le autorità competenti degli Stati membri, quali la polizia, le guardie di frontiera e i servizi doganali, devono avere accesso a informazioni di alta qualità sulle persone e sugli oggetti che controllano, con chiare istruzioni su come comportarsi in ogni singolo caso. Questo sistema d'informazione su larga scala è al centro della cooperazione Schengen e svolge un ruolo cruciale nel facilitare la libera circolazione delle persone all'interno dello spazio Schengen. Permette alle autorità competenti di inserire e consultare dati su persone ricercate, persone che potrebbero non avere il diritto di entrare o di soggiornare nell'UE, persone scomparse (soprattutto minori) e oggetti che potrebbero essere stati rubati, sottratti o smarriti. Oltre a conservare informazioni su persone o oggetti specifici, il SIS contiene chiare istruzioni per le autorità competenti sulle iniziative da prendere una volta reperito un oggetto o una persona.

Nel 2016, tre anni dopo l'entrata in funzione della seconda generazione del SIS, la Commissione ha svolto una valutazione globale del sistema[1], dalla quale risulta che il SIS è stato un autentico successo operativo. Nel 2015 le autorità nazionali competenti hanno verificato persone e oggetti consultando i dati contenuti nel SIS in quasi 2,9 miliardi di casi e si sono scambiate più di 1,8 milioni di informazioni supplementari. Tuttavia, come annunciato nel programma di lavoro della Commissione per il 2017, sulla base di questa esperienza positiva occorre rafforzare ulteriormente l'efficacia e l'efficienza del sistema. A tal fine la Commissione presenta una prima serie di tre proposte intese a migliorare e ampliare l'uso del SIS sulla base della valutazione, continuando al contempo a impegnarsi per aumentare l'interoperabilità degli attuali e futuri sistemi di contrasto alla criminalità e di gestione delle frontiere sulla scia delle attività del gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità.

Queste proposte riguardano rispettivamente l'uso del sistema a) per la gestione delle frontiere, b) per la cooperazione e di polizia e la cooperazione giudiziaria in materia penale, e c) per il rimpatrio dei cittadini di paesi terzi in soggiorno irregolare. L'insieme delle prime due proposte costituisce la base giuridica per l'istituzione, l'esercizio e l'uso del SIS. La proposta

[1] 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, e documento di lavoro dei servizi della Commissione che accompagna la relazione. (GU...).

relativa all'uso del SIS per il rimpatrio dei cittadini di paesi terzi in soggiorno irregolare completa la proposta sulla gestione delle frontiere e integra le disposizioni ivi contenute; stabilisce una nuova categoria di segnalazioni e contribuisce all'attuazione e al monitoraggio della direttiva 2008/115/CE[2].

A causa della geometria variabile della partecipazione degli Stati membri alle politiche dell'UE relative allo spazio di libertà, sicurezza e giustizia, è necessario adottare tre strumenti giuridici distinti che tuttavia operino in piena sintonia per consentire il funzionamento e l'uso generale del sistema.

Parallelamente, al fine di rafforzare e migliorare la gestione delle informazioni a livello di UE, nell'aprile 2016 la Commissione ha avviato un processo di riflessione su "Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza"[3]. L'obiettivo generale è garantire che le autorità competenti ottengano sistematicamente le informazioni necessarie dai diversi sistemi di informazione a loro disposizione. Per conseguire tale obiettivo, la Commissione ha riesaminato l'attuale architettura dell'informazione per individuare le lacune e i punti deboli che derivano da carenze nelle funzionalità dei sistemi esistenti, ma anche dalla frammentazione dell'architettura generale della gestione dei dati nell'UE. A sostegno di questa attività la Commissione ha istituito un gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità, le cui constatazioni provvisorie sono state utilizzate per questa prima serie di proposte riguardo alle questioni di qualità dei dati[4]. Nel discorso sullo stato dell'Unione del settembre 2016 il presidente Juncker ha fatto riferimento anche all'importanza di colmare le attuali carenze nella gestione delle informazioni e di migliorare l'interoperabilità e il collegamento tra gli attuali sistemi di informazione.

Sulla base delle conclusioni del gruppo di esperti ad alto livello sui sistemi d'informazione e l'interoperabilità, che saranno presentate nel primo semestre del 2017, la Commissione esaminerà, verso la metà del 2017, una seconda serie di proposte volte a migliorare ulteriormente l'interoperabilità del SIS con altri sistemi informatici. Altrettanto importante in questo contesto è la revisione del regolamento (UE) n. 1077/2011[5] sull'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), che sarà probabilmente oggetto, sempre nel 2017, di proposte distinte della Commissione. Per affrontare le attuali sfide in materia di sicurezza è importante investire in uno scambio e in una gestione delle informazioni che siano rapidi, efficaci e di qualità e garantire l'interoperabilità delle banche dati e dei sistemi di informazione dell'UE.

La presente proposta fa parte di un primo insieme di proposte[6] volte a migliorare il funzionamento del SIS e il suo esercizio e uso nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale. Essa attua:

---

2 Direttiva 2008/115/CE del Parlamento europeo e del Consiglio, del 16 dicembre 2008, recante norme e procedure comuni applicabili negli Stati membri al rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare (GU L 348 del 24.12.2008, pag. 98).

3 COM(2016) 205 final del 6.4.2016.

4 Decisione 2016/C 257/03 della Commissione del 17.6.2016.

5 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).

6 Regolamento (UE) 2018/xxx [verifiche di frontiera] e regolamento (UE) 2018/xxx [rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare].

(1) l'intenzione espressa dalla Commissione di aumentare il valore aggiunto del SIS a fini di contrasto[7] in risposta alle nuove minacce;

(2) il consolidamento dei risultati dei lavori per l'attuazione del SIS svolti negli ultimi tre anni, che comportano modifiche tecniche al SIS centrale al fine di ampliare alcune delle attuali categorie di segnalazioni e di introdurre nuove funzionalità;

(3) le raccomandazioni relative a modifiche tecniche e procedurali formulate in seguito alla valutazione globale del SIS[8];

(4) le richieste di miglioramenti tecnici del SIS da parte degli utenti finali;

(5) le conclusioni provvisorie del gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità[9] per quanto riguarda la qualità dei dati.

Poiché la presente proposta è strettamente legata alla proposta della Commissione relativa a un regolamento sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen nel settore delle verifiche di frontiera, alcune disposizioni sono comuni a entrambi i testi. Tra queste figurano misure che riguardano l'uso del SIS da un'estremità all'altra, compresi non soltanto il funzionamento del sistema centrale e dei sistemi nazionali, ma anche le esigenze degli utenti finali; misure rafforzate per la continuità operativa; misure riguardanti la qualità dei dati, la protezione dei dati e la sicurezza dei dati e disposizioni in materia di monitoraggio, valutazione e relazioni. Entrambe le proposte ampliano inoltre l'uso delle informazioni biometriche[10].

L'attuale quadro giuridico della seconda generazione del SIS - per quanto riguarda il suo uso a fini di cooperazione di polizia e cooperazione giudiziaria in materia penale - si basa su un precedente strumento del terzo pilastro, la decisione 2007/533/GAI del Consiglio[11], e su un precedente strumento del primo pilastro, il regolamento (CE) n. 1986/2006[12].La presente proposta consolida il contenuto degli strumenti già esistenti e aggiunge nuove disposizioni allo scopo di:

- armonizzare meglio le procedure nazionali di uso del SIS, in particolare per i reati legati al terrorismo e i rischi di sottrazione di minori da parte di uno dei genitori;

---

7 Si veda la comunicazione "Attuare l'Agenda europea sulla sicurezza per combattere il terrorismo e preparare il terreno per l'Unione della sicurezza", pag. 4 segg., COM(2016) 230 final del 20.4.2016.

8 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, e documento di lavoro dei servizi della Commissione che accompagna la relazione. (GU...).

9 Gruppo di esperti ad alto livello – relazione del Presidente del 21 dicembre 2016.

10 Per una spiegazione dettagliata delle modifiche contenute nella presente proposta si veda la sezione 5 "Altri elementi".

11 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).

12 Regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'accesso al sistema d'informazione Schengen di seconda generazione (SIS II) dei servizi competenti negli Stati membri per il rilascio delle carte di circolazione (GU L 381 del 28.12.2006, pag. 1).

- estendere il campo di applicazione del SIS aggiungendo alle attuali segnalazioni nuovi elementi di identificazione biometrica;

- introdurre cambiamenti tecnici che migliorano la sicurezza e contribuire a ridurre gli oneri amministrativi prevedendo copie nazionali obbligatorie e norme tecniche comuni di attuazione;

- trattare l'uso completo del SIS da un'estremità all'altra, non limitandosi a occuparsi dei sistemi centrale e nazionali, ma garantendo anche che gli utenti finali ricevano tutti i dati necessari per adempiere le loro funzioni e rispettino tutte le norme di sicurezza nel trattamento dei dati SIS.

•Coerenza con le altre normative dell'Unione e con gli strumenti giuridici vigenti e futuri

La presente proposta è strettamente collegata ad altre politiche dell'Unione e le completa. Si tratta in particolare delle seguenti politiche:

(1) la politica di **sicurezza interna** quale illustrata dall'Agenda europea sulla sicurezza[13] e dall'operato della Commissione per un'efficace e autentica Unione della sicurezza[14], in quanto permette alle autorità di contrasto di trattare i dati personali di persone sospettate di coinvolgimento in atti di terrorismo o in altri reati gravi a fini di prevenzione, accertamento e indagine di reati di terrorismo e altri reati gravi e relativa azione penale;

(2) la politica di **protezione dei dati**, nella misura in cui la presente proposta garantisce la tutela dei diritti fondamentali delle persone i cui dati personali sono trattati nel SIS.

La presente proposta è inoltre strettamente collegata alla legislazione vigente nell'Unione e la completa. Si tratta in particolare dei seguenti settori:

(3) **la guardia di frontiera e costiera europea**, per quanto riguarda il suo accesso al SIS ai fini del proposto sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)[15], e in quanto la presente proposta fornisce alle squadre della guardia di frontiera e costiera europea, alle squadre di personale che assolve compiti attinenti al rimpatrio e ai membri delle squadre di sostegno per la gestione della migrazione un'interfaccia tecnica per l'accesso al SIS accordando loro il diritto, nell'ambito del rispettivo mandato, di accedere ai dati inseriti nel SIS e consultarli;

(4) **Europol** , nella misura in cui la presente proposta conferisce a Europol diritti aggiuntivi di accedere ai dati inseriti nel SIS e consultarli, nell'ambito del suo mandato;

(5) **Prüm**, nella misura in cui gli sviluppi previsti dalla presente proposta che consentono di identificare le persone mediante le impronte digitali (nonché le

13 COM(2015) 185 final.
14 COM(2016) 230 final.
15 COM(2016) 731 final.

immagini facciali e i profili DNA) completano le vigenti disposizioni Prüm[16] sull'accesso reciproco in linea transfrontaliero a banche dati nazionali del DNA designate e a sistemi automatizzati di identificazione delle impronte digitali.

La presente proposta è inoltre strettamente collegata alla legislazione futura dell'Unione e la completa. Si tratta in particolare dei seguenti settori:

(6) **gestione delle frontiere esterne**: la proposta completa il nuovo principio che si prevede di inserire nel codice frontiere Schengen in reazione al fenomeno dei terroristi combattenti stranieri, che prevede la verifica sistematica nelle banche dati pertinenti di tutti i viaggiatori, compresi i cittadini dell'UE, all'ingresso nello spazio Schengen e all'uscita dal medesimo;

(7) **sistema di ingressi/uscite:** la proposta riflette l'uso proposto di una combinazione di impronte digitali e immagine facciale come identificatori biometrici per il funzionamento del sistema di ingressi/uscite (EES);

(8) **ETIAS:** la proposta tiene conto del proposto sistema ETIAS che prevede una valutazione accurata sotto il profilo della sicurezza, compresa una verifica nel SIS, dei cittadini di paesi terzi che intendono recarsi nell'UE.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

• Base giuridica

La presente proposta si basa sull'articolo 82, paragrafo 1, lettera d), sull'articolo 85, paragrafo 1, sull'articolo 87, paragrafo 2, lettera a), e sull'articolo 88, paragrafo 2, lettera a), del trattato sul funzionamento dell'Unione europea come basi giuridiche per le disposizioni sulla cooperazione di polizia e sulla cooperazione giudiziaria in materia penale.

• Geometria variabile

La proposta si basa sulle disposizioni dell'acquis di Schengen sulla cooperazione di polizia e sulla cooperazione giudiziaria in materia penale. Devono pertanto essere prese in considerazione le conseguenze dei vari protocolli e accordi con i paesi associati esposte in appresso.

Danimarca: a norma dell'articolo 4 del protocollo n. 22 sulla posizione della Danimarca allegato ai trattati, la Danimarca deciderà, entro un periodo di sei mesi dalla decisione del Consiglio sul presente regolamento, se intende recepire la presente proposta, che si basa sull'acquis di Schengen, nel proprio diritto interno.

Regno Unito: il Regno Unito è vincolato dal presente regolamento ai sensi dell'articolo 5 del protocollo sull'acquis di Schengen integrato nell'ambito dell'Unione europea, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, e

[16] 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); e 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).

dell'articolo 8, paragrafo 2, della decisione 2000/365/CE del Consiglio, del 29 maggio 2000, riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune disposizioni dell'acquis di Schengen[17].

Irlanda: l'Irlanda è vincolata dal presente regolamento ai sensi dell'articolo 5 del protocollo sull'acquis di Schengen integrato nell'ambito dell'Unione europea, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, e dell'articolo 6, paragrafo 2, della decisione 2002/192/CE del Consiglio, del 28 febbraio 2002, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'acquis di Schengen[18].

Bulgaria e Romania: il presente regolamento costituisce un atto basato sull'acquis di Schengen o ad esso altrimenti connesso ai sensi dell'articolo 4, paragrafo 2, dell'atto di adesione del 2005. Il presente regolamento deve essere letto in combinato disposto con la decisione 2010/365/UE del Consiglio, del 29 giugno 2010[19], che ha reso applicabili, fatte salve alcune restrizioni, le disposizioni dell'acquis di Schengen relative al sistema d'informazione Schengen in Bulgaria e Romania.

Cipro e Croazia: il presente regolamento costituisce un atto basato sull'acquis di Schengen o ad esso altrimenti connesso ai sensi, rispettivamente, dell'articolo 3, paragrafo 2, dell'atto di adesione del 2003 e dell'articolo 4, paragrafo 2, dell'atto di adesione del 2011.

Paesi associati: sulla base dei rispettivi accordi che associano tali paesi all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen, l'Islanda, la Norvegia, la Svizzera e il Liechtenstein devono essere vincolati dal regolamento proposto.

- **Sussidiarietà**

La presente proposta intende sviluppare e consolidare l'attuale SIS, che è operativo dal 1995. Il quadro intergovernativo originario è stato sostituito da strumenti dell'Unione il 9 aprile 2013 (regolamento (CE) n. 1987/2006 e decisione 2007/533/GAI del Consiglio). In precedenti occasioni è stata svolta un'analisi completa della sussidiarietà; la presente iniziativa mira a perfezionare le disposizioni vigenti, ovviare alle carenze individuate e migliorare le procedure operative.

Il livello notevole dello scambio di informazioni tra Stati membri raggiunto grazie al SIS non può essere conseguito con metodi decentrati. A motivo della portata, degli effetti e delle ripercussioni dell'azione, gli obiettivi della presente proposta possono essere conseguiti meglio a livello di Unione.

Tra gli obiettivi della presente proposta figurano miglioramenti tecnici volti a migliorare l'efficienza del SIS, nonché l'armonizzazione dell'uso del sistema in tutti gli Stati membri partecipanti. Dato il carattere transnazionale di tali obiettivi e delle sfide da affrontare per garantire un efficace scambio di informazioni al fine di combattere minacce sempre più

[17] GU L 131 dell'1.6.2000, pag. 43.

[18] GU L 64 del 7.3.2002, pag. 20.

[19] Decisione 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).

diversificate, l'UE si trova nella posizione migliore per proporre soluzioni a problemi che non possono essere gestiti in maniera sufficiente dai soli Stati membri.

Se non si superano le attuali limitazioni del SIS, si rischia di non cogliere numerose opportunità per massimizzare l'efficienza e il valore aggiunto dell'UE e di lasciare che le lacune esistenti ostacolino il lavoro delle autorità competenti. A titolo di esempio, la mancanza di norme armonizzate in materia di cancellazione delle segnalazioni ridondanti all'interno del sistema può ostacolare la libera circolazione delle persone, principio fondamentale dell'Unione.

- **Proporzionalità**

Ai sensi dell'articolo 5 del trattato sull'Unione europea, l'azione dell'Unione si limita a quanto necessario per il conseguimento degli obiettivi fissati nel trattato. La forma prescelta per questa azione dell'Unione deve permettere alla proposta di raggiungere il suo obiettivo ed essere attuata il più efficacemente possibile. L'iniziativa proposta costituisce una revisione del SIS per quanto riguarda la cooperazione di polizia e la cooperazione giudiziaria in materia penale.

La proposta è formulata in base ai principi della tutela della vita privata fin dalla progettazione. In termini di diritto alla protezione dei dati personali, la presente proposta è proporzionata in quanto introduce regole specifiche sulla cancellazione delle segnalazioni e non richiede che i dati siano raccolti e conservati per una durata superiore a quella strettamente necessaria per permettere al sistema di funzionare e conseguire i suoi obiettivi. Tenendo conto delle esigenze operative, la presente proposta riduce il periodo di conservazione per le segnalazioni sugli oggetti e lo allinea a quello per le segnalazioni sulle persone (poiché sono spesso connesse a dati personali, quali documenti di identificazione personale o targhe di veicoli). L'esperienza delle forze di polizia dimostra che i beni rubati possono essere recuperati entro un periodo di tempo relativamente breve, il che rende inutilmente lunga la scadenza di 10 anni per le segnalazioni relative agli oggetti.

Le segnalazioni del SIS contengono solo i dati necessari per identificare e localizzare una persona o un oggetto e consentire l'intervento operativo adeguato. Gli uffici SIRENE forniscono ogni altra informazione necessaria per lo scambio di informazioni supplementari.

La proposta prevede inoltre l'applicazione di tutte le salvaguardie e i meccanismi necessari per un'efficace protezione dei diritti fondamentali degli interessati, in particolare la protezione della vita privata e dei dati personali. Comprende anche disposizioni specificamente destinate a rafforzare la sicurezza dei dati personali archiviati nel SIS.

Non saranno necessari ulteriori processi o armonizzazioni a livello dell'UE affinché il sistema funzioni. La misura proposta è proporzionata, dato che limita l'azione dell'UE a quanto è necessario per conseguire gli obiettivi stabiliti.

- **Scelta dell'atto giuridico**

La revisione proposta assumerà la forma di regolamento e sostituirà la decisione 2007/533/GAI del Consiglio conservandone gran parte del contenuto. La decisione 2007/533/GAI è stata adottata quale strumento giuridico del cosiddetto terzo pilastro in virtù del precedente trattato sull'Unione europea. Tali strumenti del "terzo pilastro" erano adottati dal Consiglio senza l'intervento del Parlamento europeo in veste di colegislatore. La base giuridica della presente proposta è nel trattato sul funzionamento dell'Unione europea

(TFUE), dato che la struttura a pilastri ha cessato di esistere con l'entrata in vigore del trattato di Lisbona, il 1º dicembre 2009. Questa base giuridica impone il ricorso alla procedura legislativa ordinaria. Deve essere scelta la forma del regolamento (del Parlamento europeo e del Consiglio) in quanto le disposizioni devono essere vincolanti e direttamente applicabili in tutti gli Stati membri.

La presente proposta si basa su un sistema centralizzato già esistente che permette agli Stati membri di cooperare tra loro e intende rafforzare tale sistema: ciò richiede un'architettura comune e norme di funzionamento vincolanti. Stabilisce inoltre norme obbligatorie sull'accesso al sistema, in particolare a fini di contrasto, che sono uniformi per tutti gli Stati membri, nonché per l'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA)[20]. Dal 9 maggio 2013 eu-LISA è responsabile della gestione operativa del SIS centrale, che consiste nell'insieme dei compiti necessari a garantire il pieno funzionamento del SIS centrale 24 ore su 24 e 7 giorni su 7. La presente proposta si fonda sulle responsabilità di eu-LISA in relazione al SIS.

La proposta prevede inoltre norme direttamente applicabili che permettono agli interessati di accedere ai dati che li riguardano e a mezzi di impugnazione senza necessità di ulteriori misure di applicazione.

Il regolamento è quindi l'unico strumento giuridico che si presti a tale scopo.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

• Valutazioni ex post / Vaglio di adeguatezza della legislazione vigente

In conformità del regolamento (CE) n. 1987/2006 e della decisione 2007/533/GAI del Consiglio, tre anni dopo l'entrata in funzione del SIS II la Commissione ha svolto una valutazione globale del SIS II centrale e dello scambio bilaterale e multilaterale di informazioni supplementari tra Stati membri.

I risultati della valutazione hanno evidenziato la necessità di modificare la base giuridica del SIS per rispondere meglio alle nuove sfide in materia di sicurezza e migrazione. Occorre ad esempio una proposta sulla prospettiva del SIS da un'estremità all'altra ("end-to-end"), disciplinandone l'uso da parte degli utenti finali e fissando norme sulla sicurezza dei dati applicabili anche alle applicazioni degli utenti finali; occorre potenziare il sistema a fini di lotta contro il terrorismo prevendendo un nuovo intervento, chiarire la situazione dei minori a rischio di sottrazione da parte di genitori e ampliare gli identificatori biometrici disponibili nel sistema.

I risultati della valutazione hanno inoltre mostrato la necessità di introdurre modifiche giuridiche per migliorare il funzionamento tecnico del sistema e razionalizzare i processi nazionali. Tali misure aumenteranno l'efficienza e l'efficacia del SIS agevolandone l'uso e riducendo gli oneri superflui. Altre misure mirano a migliorare la qualità dei dati e la

[20] Istituita dal 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).

trasparenza del sistema descrivendo più chiaramente gli specifici compiti di comunicazione da parte degli Stati membri e di eu-LISA.

I risultati della valutazione generale (la relazione di valutazione e il relativo documento di lavoro dei servizi della Commissione sono stati adottati il 21 dicembre 2016[21]) hanno costituito la base delle misure previste dalla presente proposta.

- **Consultazioni dei portatori di interessi**

Durante la valutazione del SIS svolta dalla Commissione i portatori d'interessi, compresi i delegati del comitato SISVIS secondo la procedura di cui all'articolo 67 della decisione 2007/533/GAI del Consiglio, sono stati invitati a formulare commenti e suggerimenti. Il comitato SISVIS comprende i rappresentanti degli Stati membri competenti sia per questioni operative di SIRENE (cooperazione transfrontaliera in relazione al SIS), sia per questioni tecniche inerenti allo sviluppo e alla manutenzione del SIS e alla relativa applicazione SIRENE.

I delegati hanno risposto a questionari dettagliati nell'ambito del processo di valutazione. Quando è stato necessario introdurre ulteriori chiarimenti o approfondire un argomento, si è fatto ricorso a scambi di e-mail o colloqui mirati. Questo processo iterativo ha permesso di affrontare i problemi in modo globale e trasparente. Per tutto il 2015 e il 2016, i delegati al comitato SISVIS hanno trattato tali questioni nel corso di riunioni e seminari ad hoc.

La Commissione ha inoltre consultato specificamente le autorità nazionali di protezione dei dati degli Stati membri e i membri del gruppo di coordinamento del controllo del SIS II in materia di protezione dei dati. Gli Stati membri si sono scambiati le loro esperienze sulle richieste di accesso degli interessati e sull'operato delle autorità nazionali di protezione dei dati, rispondendo a un apposito questionario. Le risposte a tale questionario comunicate dal giugno 2015 sono state prese in considerazione per lo sviluppo della presente proposta.

A livello interno la Commissione ha istituito un gruppo direttivo interservizi composto dal segretariato generale e dalle direzioni generali Migrazione e affari interni, Giustizia e consumatori, Risorse umane e sicurezza, e Informatica. Il gruppo direttivo ha monitorato il processo di valutazione e fornito orientamenti ove necessario.

I risultati della valutazione hanno tenuto conto anche di elementi di prova raccolti durante le visite di valutazione in loco negli Stati membri, grazie alle quali è stato esaminato in modo approfondito l'uso del SIS nella pratica. Sono stati svolti colloqui e discussioni con professionisti, personale dell'ufficio SIRENE e autorità nazionali competenti.

Sulla base dei riscontri ottenuti, la presente proposta introduce misure volte a migliorare l'efficienza e l'efficacia tecnica e operativa del sistema.

[21] 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, e documento di lavoro dei servizi della Commissione che accompagna la relazione.

- **Assunzione e uso di perizie**

Oltre a consultare i portatori di interessi, la Commissione ha fatto ricorso a perizie esterne tramite tre studi, i cui risultati sono stati inseriti negli sviluppi della presente proposta:

- Valutazione tecnica del SIS (Kurt Salmon)[22]

  La valutazione ha individuato le questioni centrali inerenti al funzionamento del SIS e i problemi da affrontare in futuro, esaminando in primo luogo l'esigenza di aumentare al massimo la continuità operativa e di fare in modo che l'architettura generale possa adeguarsi al crescente fabbisogno di capacità.

- TIC – Valutazione d'impatto di possibili miglioramenti all'architettura del SIS II (Kurt Salmon)[23]

  Lo studio ha valutato l'attuale costo del funzionamento del SIS a livello nazionale e due possibili soluzioni tecniche per il miglioramento del sistema. Entrambe le soluzioni comprendono una serie di proposte tecniche finalizzate a migliorare il sistema centrale e l'architettura generale.

- TIC – Valutazione d'impatto di possibili miglioramenti all'architettura del SIS II – Relazione finale, 10 novembre 2016 (Wavestone)[24]

  Lo studio ha valutato l'impatto della realizzazione di una copia nazionale in termini di costi per gli Stati membri analizzando tre opzioni (un sistema pienamente centralizzato, un'attuazione standardizzata dell'N.SIS sviluppata e fornita da eu-LISA agli Stati membri e un'attuazione distinta dell'N.SIS con norme tecniche comuni).

- **Valutazione d'impatto**

La Commissione non ha effettuato una valutazione d'impatto.

Sulla base delle tre valutazioni indipendenti sopra citate (al punto "Assunzione e uso di perizie") sono stati valutati gli effetti dei cambiamenti del sistema sotto il profilo tecnico. Dal 2013, ossia da quando è entrato in funzione il SIS II il 9 aprile 2013 ed è diventata applicabile la decisione 2007/533/GAI, la Commissione ha inoltre compiuto due revisioni del manuale SIRENE, compresa una valutazione intermedia da cui è scaturito, il 29 gennaio 2015, un nuovo manuale SIRENE[25]. La Commissione ha inoltre adottato un catalogo di raccomandazioni e migliori pratiche[26]. Per di più, eu-LISA e gli Stati membri apportano

22 RELAZIONE FINALE della Commissione europea – Valutazione tecnica del SIS II

23 Commissione europea – Relazione finale – TIC – Valutazione d'impatto di possibili miglioramenti all'architettura del SIS II - 2016.

24 Commissione europea – "TIC – Valutazione d'impatto di possibili miglioramenti all'architettura del SIS II – Relazione finale",10 novembre 2016 (Wavestone)

25 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) (GU L 44 del 18.2.2015, pag. 75).

26 Raccomandazione della Commissione che istituisce un catalogo di raccomandazioni e migliori pratiche per la corretta applicazione del sistema d'informazione Schengen di seconda generazione (SIS II) e lo scambio di informazioni supplementari da parte delle autorità competenti degli Stati membri che applicano e usano il SIS II [C(2015)9169/1].

regolarmente al sistema miglioramenti tecnici iterativi. Si ritiene che queste opzioni siano ormai esaurite e che sia necessario modificare su più larga scala la base giuridica. Migliorare l'attuazione e l'esecuzione non basta per apportare chiarezza in settori come l'applicazione di sistemi destinati agli utenti finali e le regole specifiche sulla cancellazione delle segnalazioni.

La Commissione ha inoltre svolto una valutazione generale del SIS come previsto all'articolo 24, paragrafo 5, all'articolo 43, paragrafo 3, e all'articolo 50, paragrafo 5, del regolamento (CE) n. 1987/2006 e all'articolo 59, paragrafo 3, e all'articolo 66, paragrafo 5, della decisione 2007/533/GAI, e ha pubblicato un documento di lavoro dei servizi della Commissione. I risultati della valutazione generale (la relazione di valutazione e il relativo documento di lavoro dei servizi della Commissione sono stati adottati il 21 dicembre 2016) hanno costituito la base delle misure previste dalla presente proposta.

Il meccanismo di valutazione Schengen, istituito dal regolamento (UE) n. 1053/2013[27], permette la valutazione periodica in termini giuridici e operativi del funzionamento del SIS negli Stati membri. Le valutazioni sono svolte congiuntamente dalla Commissione e dagli Stati membri. Tramite questo meccanismo il Consiglio formula raccomandazioni destinate ai singoli Stati membri sulla base delle valutazioni svolte nel quadro di programmi pluriennali e annuali. Data la loro natura specifica, tali raccomandazioni non possono sostituire norme giuridicamente vincolanti applicabili contemporaneamente a tutti gli Stati membri che usano il SIS.

Il comitato SISVIS tratta regolarmente questioni pratiche di ordine operativo e tecnico. Malgrado l'utilità di tali riunioni per la cooperazione tra la Commissione e gli Stati membri, i risultati delle discussioni (in mancanza di modifiche legislative) non possono rimediare a problemi dovuti, ad esempio, a divergenze tra le prassi nazionali.

I cambiamenti proposti nel presente regolamento non presentano un'incidenza economica o ambientale significativa. Si prevede d'altra parte che esercitino un impatto sociale decisamente positivo, in quanto permettono di aumentare la sicurezza consentendo una migliore identificazione delle persone che usano false identità, autori di reati gravi la cui identità rimane ignota e minori scomparsi. L'impatto di tali cambiamenti sui diritti fondamentali e la protezione dei dati è valutato e illustrato in modo più approfondito nella sezione successiva ("Diritti fondamentali").

La proposta è stata redatta ricorrendo alle prove sostanziali raccolte ai fini della valutazione generale della seconda generazione del SIS, che ha esaminato il funzionamento del sistema e i possibili miglioramenti. È stata inoltre svolta una valutazione d'impatto relativa ai costi per verificare che l'architettura nazionale prescelta fosse la più appropriata e proporzionata.

- **Diritti fondamentali e protezione dei dati**

La presente proposta sviluppa e migliora un sistema già esistente piuttosto che svilupparne uno nuovo, e di conseguenza si basa su importanti e valide garanzie che sono già in atto. Nonostante ciò, poiché il sistema continua a trattare dati personali e tratterà ulteriori categorie

[27] Regolamento (UE) n. 1053/2013 del Consiglio, del 7 ottobre 2013, che istituisce un meccanismo di valutazione e di controllo per verificare l'applicazione dell'acquis di Schengen e che abroga la decisione del comitato esecutivo del 16 settembre 1998 che istituisce una Commissione permanente di valutazione e di applicazione di Schengen (GU L 295 del 6.11.2013, pag. 27).

di dati biometrici sensibili, la proposta ha una potenziale incidenza sui diritti fondamentali delle persone fisiche. Tale incidenza è stata accuratamente valutata e sono state predisposte salvaguardie aggiuntive per limitare la raccolta e il successivo trattamento dei dati a quanto strettamente necessario e indispensabile dal punto di vista operativo, e per limitare l'accesso ai dati ai soli soggetti che ne hanno esigenza a fini operativi. La proposta fissa termini precisi per la conservazione dei dati, compresi periodi di conservazione ridotti per le segnalazioni relative a oggetti. Sono chiaramente riconosciuti e sanciti i diritti dell'interessato di accedere ai dati che lo riguardano e rettificarli, e di chiederne la cancellazione nel rispetto dei diritti fondamentali (si veda la sezione sulla protezione e sicurezza dei dati).

Inoltre la proposta rafforza le misure volte a proteggere i diritti fondamentali, in quanto introduce nella normativa l'obbligo di cancellare una segnalazione e introduce una valutazione di proporzionalità in caso di proroga della validità di una segnalazione. Sarà possibile identificare le persone in modo più affidabile grazie ai dati biometrici per le persone scomparse che necessitano di protezione, garantendo che i dati personali siano esatti e adeguatamente protetti. La proposta definisce ampie e solide salvaguardie per l'uso degli identificatori biometrici al fine di evitare che persone innocenti subiscano disagi.

La proposta prevede inoltre la sicurezza del sistema da un'estremità all'altra, garantendo una maggiore protezione per i dati ivi conservati. Introducendo una chiara procedura di gestione degli incidenti e aumentando la continuità operativa del SIS, la proposta è pienamente conforme alla Carta dei diritti fondamentali dell'Unione europea[28] per quanto riguarda il diritto alla protezione dei dati personali. Lo sviluppo e l'efficacia ininterrotta del SIS contribuiranno alla sicurezza delle persone nell'ambito della società.

La proposta prevede modifiche importanti per quanto riguarda gli identificatori biometrici. Oltre alle impronte digitali dovrebbero essere raccolte e conservate anche le impronte palmari, nel rispetto degli obblighi giuridici. A norma degli articoli 26, 32, 34 e 36, i registri delle impronte digitali saranno allegati alle segnalazioni alfanumeriche del SIS. In futuro dovrebbe essere possibile confrontare questi dati dattiloscopici (impronte digitali e palmari) con le impronte digitali rilevate sul luogo del reato, purché si tratti di un reato grave o di un atto di terrorismo e purché possa essere stabilito con un elevato grado di probabilità che tali impronte appartengano all'autore del reato. La proposta prevede inoltre la conservazione di impronte digitali per i cosiddetti "ignoti ricercati" (alle condizioni illustrate nella sezione 5, sottosezione "Fotografie, immagini facciali, dati dattiloscopici e profili DNA"). Qualora i documenti di una persona non permettano di definirne con certezza l'identità, le autorità competenti dovrebbero confrontare le sue impronte digitali con quelle conservate nella banca dati del SIS.

La proposta impone la raccolta e la conservazione di dati complementari (quali i dati contenuti nei documenti di identificazione personale) per facilitare il lavoro sul terreno del personale addetto a verificare l'identità.

La proposta garantisce il diritto dell'interessato a un ricorso effettivo avverso qualsiasi decisione, il che comprende in ogni caso un ricorso effettivo dinanzi a un giudice ai sensi dell'articolo 47 della Carta dei diritti fondamentali.

[28] Carta dei diritti fondamentali dell'Unione europea (2012/C 326/02).

4. INCIDENZA SUL BILANCIO

Il SIS costituisce un sistema d'informazione unico. Di conseguenza, le spese previste in due delle proposte (la presente e la proposta di regolamento sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera) non vanno considerate due importi separati ma un unico importo. L'incidenza sul bilancio delle modifiche necessarie per attuare entrambe le proposte è compresa in un'unica scheda finanziaria legislativa.

Data la natura complementare della terza proposta (riguardante il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare), la sua incidenza sul bilancio è esaminata separatamente e in una scheda finanziaria distinta, che concerne soltanto l'istituzione di questa specifica categoria di segnalazione.

Secondo la valutazione dei vari aspetti del lavoro richiesto per la rete, la gestione del SIS centrale da parte di eu-LISA e gli sviluppi nazionali negli Stati membri, le due proposte di regolamento richiederanno un importo totale di 64,3 milioni di EUR per il periodo 2018-2020.

Questo importo copre un aumento della larghezza di banda di TESTA-NG: secondo le due proposte, infatti, la rete trasmetterà i file delle impronte digitali e delle immagini facciali e quindi necessiterà di una maggiore velocità di elaborazione e capacità di flusso (9,9 milioni di EUR). Copre inoltre i costi sostenuti da eu-LISA per le spese di personale e operative (17,6 milioni di EUR). eu-LISA ha comunicato alla Commissione che nel gennaio 2018 è prevista l'assunzione di 3 nuovi agenti contrattuali per iniziare la fase di sviluppo a tempo debito e garantire così l'avvio delle funzionalità aggiornate del SIS nel 2020. La presente proposta comporta modifiche tecniche al SIS centrale per estendere alcune delle attuali categorie di segnalazione e fornire nuove funzionalità. La scheda finanziaria allegata alla presente proposta riflette questi cambiamenti.

La Commissione ha inoltre svolto una valutazione d'impatto sui costi per valutare i costi degli sviluppi nazionali resi necessari dalla presente proposta[29]. Il costo stimato è di 36,8 milioni di EUR, che sarebbero elargiti agli Stati membri sotto forma di somma forfettaria. Di conseguenza, ogni Stato membro riceverà un importo di 1,2 milioni di EUR per aggiornare il sistema nazionale secondo i requisiti previsti dalla presente proposta, fra l'altro istituendo una copia parziale nazionale laddove non è ancora creata o introducendo un sistema di copie di riserva.

È prevista una riprogrammazione della dotazione rimanente per le "Frontiere intelligenti" del Fondo sicurezza interna, per apportare gli aggiornamenti e applicare le funzionalità introdotte dalle due proposte. Il regolamento ISF-Frontiere[30] è lo strumento finanziario in cui è stato inserito il bilancio per l'attuazione del pacchetto "Frontiere intelligenti". All'articolo 5 il regolamento prevede che 791 milioni di EUR siano destinati a un programma per lo sviluppo di sistemi informatici a sostegno della gestione dei flussi migratori attraverso le frontiere esterne, alle condizioni previste all'articolo 15. Di questi 791 milioni di EUR, 480 sono riservati allo sviluppo del sistema di ingressi/uscite e 210 allo sviluppo del sistema europeo di

[29] "TIC - Valutazione d'impatto di possibili miglioramenti all'architettura del SIS II, relazione finale", 10 novembre 2016 (Wavestone), opzione 3: Applicazione distinta dell'N.SIS II.

[30] Regolamento (UE) n. 515/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, che istituisce, nell'ambito del Fondo sicurezza interna, lo strumento di sostegno finanziario per le frontiere esterne e i visti (GU L 150 del 20.5.2014, pag. 143).

informazione e autorizzazione ai viaggi (ETIAS). L'importo rimanente sarà in parte usato per coprire i costi dei cambiamenti previsti dalle due proposte riguardo al SIS.

5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

La Commissione, gli Stati membri ed eu-LISA dovranno riesaminare periodicamente e monitorare l'uso del SIS, per verificare che continui a funzionare in modo efficace ed efficiente. La Commissione sarà assistita dal comitato SISVIS per l'attuazione delle misure tecniche e operative previste dalla presente proposta.

Il proposto regolamento prevede inoltre all'articolo 71, paragrafi 7 e 8, un processo formale e periodico di revisione e valutazione.

Ogni due anni eu-LISA riferirà al Parlamento europeo e al Consiglio in merito al funzionamento tecnico del SIS (compresa la sicurezza), all'infrastruttura di comunicazione su cui si basa e allo scambio bilaterale e multilaterale di informazioni supplementari fra gli Stati membri.

Inoltre, ogni quattro anni la Commissione è tenuta a effettuare e trasmettere al Parlamento e al Consiglio una valutazione globale del SIS e dello scambio di informazioni tra gli Stati membri. In questo quadro la Commissione:

- analizzerà i risultati conseguiti in relazione agli obiettivi;
- valuterà se restino validi i principi di base del sistema;
- esaminerà il modo in cui il regolamento è applicato al sistema centrale;
- valuterà la sicurezza del sistema centrale;
- valuterà le implicazioni per il futuro funzionamento del sistema.

eu-LISA è inoltre tenuta a pubblicare statistiche giornaliere, mensili e annuali sull'uso del SIS e a provvedere al monitoraggio permanente del sistema e del suo funzionamento in relazione agli obiettivi.

- **Illustrazione dettagliata delle singole disposizioni della proposta**

Disposizioni comuni alla presente proposta e alla proposta di regolamento sull'istituzione, l'esercizio e l'uso del SIS nel settore delle verifiche di frontiera

- Disposizioni generali (articoli 1-3)
- Architettura tecnica e modalità operative del SIS (articoli 4-14)
- Responsabilità di eu-LISA (articoli 15-18)
- Diritto di accesso e conservazione delle segnalazioni (articoli 43, 46, 48, 50 e 51)

- Regole generali sul trattamento e sulla protezione dei dati (articoli 53-70)
- Monitoraggio e statistiche (articolo 71)

Uso del SIS da un'estremità all'altra

Con oltre 2 milioni di utenti finali nell'ambito delle autorità competenti di tutta Europa, il SIS è uno strumento di larghissimo uso e di grande efficacia per lo scambio di informazioni. La presente proposta prevede regole sul funzionamento completo del sistema da un'estremità all'altra, compresi il SIS centrale gestito da eu-LISA, i sistemi nazionali e le applicazioni destinate agli utenti finali. Riguarda non solo i sistemi centrale e nazionali, ma anche le esigenze tecniche e operative degli utenti finali.

L'articolo 9, paragrafo 2, specifica che gli utenti finali devono ricevere i dati necessari allo svolgimento dei loro compiti (in particolare i dati richiesti per identificare l'interessato e intraprendere le azioni necessarie). Prevede inoltre uno schema comune per l'attuazione del SIS da parte degli Stati membri, che garantisce l'armonizzazione di tutti i sistemi nazionali. A norma dell'articolo 6 gli Stati membri devono garantire la disponibilità ininterrotta dei dati SIS agli utenti finali, per aumentare al massimo i vantaggi operativi riducendo la possibilità di tempi di inattività.

L'articolo 10, paragrafo 3, garantisce che la sicurezza del trattamento dei dati comprenda anche le attività di trattamento dei dati da parte dell'utente finale. A norma dell'articolo 14 gli Stati membri sono tenuti a garantire che il personale con accesso al SIS riceva una formazione regolare e continua sulle norme relative alla sicurezza e alla protezione dei dati.

Grazie all'introduzione di queste misure, la presente proposta tratta in modo più generale il funzionamento completo del SIS da un'estremità all'altra, con norme e obblighi che riguardano milioni di utenti finali in Europa. Per sfruttare in pieno l'efficacia del SIS gli Stati membri dovrebbero garantire che i loro utenti finali, ogni volta che sono autorizzati a consultare una banca dati nazionale della polizia o dell'immigrazione, consultino parallelamente anche il SIS. In tal modo il SIS può conseguire il suo obiettivo di costituire la principale misura compensativa nello spazio senza controlli alle frontiere interne, e gli Stati membri possono affrontare meglio la dimensione transfrontaliera della criminalità e la mobilità dei criminali. Questa ricerca parallela deve rimanere conforme all'articolo 4 della direttiva (UE) 2016/680[31].

Continuità operativa

La proposta rafforza le disposizioni relative alla continuità operativa, sia a livello nazionale sia per eu-LISA (articoli 4, 6, 7 e 15). Tali disposizioni fanno sì che il SIS rimanga operativo e accessibile al personale sul terreno, anche se si verificano problemi che incidono sul sistema.

Qualità dei dati

[31] 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 (GU L 119 del 4.5.2016, pag. 89).

La proposta mantiene il principio secondo cui spetta allo Stato membro, che è il proprietario dei dati, garantire l'esattezza dei dati inseriti nel SIS (articolo 56). Occorre comunque istituire un meccanismo centrale gestito da eu-LISA che permetta agli Stati membri di riesaminare periodicamente le segnalazioni in cui i campi di dati obbligatori possono sollevare preoccupazioni in ordine alla qualità. Di conseguenza, l'articolo 15 della proposta incarica eu-LISA di fornire agli Stati membri relazioni sulla qualità dei dati a scadenze regolari. Tale attività può essere agevolata da un archivio di dati per la produzione di statistiche e relazioni sulla qualità dei dati (articolo 71). Tali miglioramenti riflettono le conclusioni provvisorie del gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità.

Fotografie, immagini facciali, dati dattiloscopici e profili DNA

La possibilità di effettuare un'interrogazione con le impronte digitali per identificare una persona è già prevista all'articolo 22 del regolamento (CE) n. 1987/2006 e della decisione 2007/533/GAI del Consiglio. Le proposte rendono obbligatoria tale consultazione qualora l'identità della persona non possa essere accertata in altro modo. Inoltre, i cambiamenti dell'articolo 22 e i nuovi articoli 40, 41 e 42 permetteranno di ricorrere, oltre che alle impronte digitali, a immagini facciali, impronte palmari e profili DNA per identificare una persona. Attualmente le immagini facciali possono essere usate solo per confermare l'identità di una persona in seguito a una ricerca alfanumerica, invece che servire da base per un'interrogazione. La dattiloscopia consiste nello studio scientifico delle impronte digitali come metodo di identificazione. Gli esperti in dattiloscopia riconoscono che le impronte palmari hanno caratteristiche di unicità e contengono punti caratteristici che permettono confronti precisi e irrefutabili, proprio come le impronte digitali. Le impronte palmari possono essere usate per appurare l'identità di una persona allo stesso modo delle impronte digitali. Da decenni la polizia acquisisce le impronte palmari insieme alle impronte ruotate e piane delle dieci dita. Le impronte palmari sono usate soprattutto in due modi:

i) a scopo di identificazione, quando la persona in questione ha danneggiato i polpastrelli, o volontariamente, nel tentativo di eludere l'identificazione o l'assunzione delle impronte digitali, o involontariamente, in seguito a un incidente o per effetto di un intenso lavoro manuale; nel corso della discussione sulle norme tecniche del sistema AFIS del SIS, l'Italia ha dichiarato di aver conseguito notevoli successi nell'identificazione di migranti irregolari che avevano intenzionalmente danneggiato i polpastrelli per evitare di essere identificati: rilevando le impronte palmari le autorità italiane hanno ottenuto l'identificazione;

ii) in caso di impronte latenti sul luogo di un reato: spesso l'autore presunto lascia tracce sul luogo del reato che risultano essere impronte palmari. Solo grazie a un'acquisizione sistematica delle impronte palmari, al momento in cui una persona è legalmente sottoposta a assunzione delle impronte digitali, è possibile identificare l'autore del reato. Inoltre, l'impronta palmare contiene di solito dettagli relativi alla base delle dita che spesso mancano dalle impronte digitali ruotate e piane, che tendono a concentrarsi sul polpastrello e le articolazioni superiori.

L'uso delle immagini facciali per l'identificazione aumenterà la coerenza tra il SIS e il proposto sistema di ingressi/uscite dell'UE, con varchi automatici e dispositivi self-service. Tale funzionalità sarà limitata ai valichi di frontiera regolari.

In mancanza di impronte digitali o palmari, l'articolo 22, paragrafo 1, lettera b), autorizza l'uso di profili DNA per le persone scomparse che devono essere poste sotto protezione,

specialmente i minori. Tale funzionalità sarà usata solo laddove non siano disponibili impronte digitali e sarà accessibile solo agli utenti autorizzati. La disposizione permette quindi di usare profili DNA dei genitori o dei fratelli della persona o del minore scomparso, per consentire alle autorità nazionali di identificarlo e localizzarlo. Gli Stati membri si scambiano già queste informazioni a livello operativo, tramite scambio di informazioni supplementari. La presente proposta iscrive questa prassi in un quadro normativo, inserendola nella fonte normativa sostanziale per l'esercizio e l'uso del SIS e disponendo chiare procedure per le circostanze in cui tali profili possono essere usati.

I cambiamenti proposti permetteranno anche di effettuare segnalazioni nel SIS per ignoti ricercati in relazione a un reato, sulla base di impronte digitali o palmari (articoli 40-42). Tali segnalazioni possono essere effettuate se, ad esempio, si rilevano impronte digitali o palmari latenti sul luogo di un reato grave e sussistono validi motivi per sospettare che appartengano all'autore di tale reato, ad esempio, se le impronte sono rinvenute su un'arma usata per commettere un delitto o un altro oggetto usato dall'autore del reato nel momento in cui l'ha commesso. Questa nuova categoria di segnalazione completa le disposizioni di Prüm che consentono l'interconnessione dei sistemi nazionali di identificazione dei criminali tramite impronte digitali. Tramite il meccanismo di Prüm, uno Stato membro può introdurre una richiesta per verificare se l'autore di un reato di cui sono state rinvenute le impronte digitali sia noto in altri Stati membri (di solito a fini di indagine). Una persona può essere identificata tramite il meccanismo di Prüm solo se le sue impronte digitali sono state acquisite in un altro Stato membro nell'ambito di un procedimento penale. Non è quindi possibile identificare un incensurato. Gli sviluppi previsti dalla presente proposta, ossia la conservazione di impronte digitali di ignoti ricercati, permetteranno di caricare nel SIS le impronte digitali dell'autore ignoto di un reato in modo da poterlo identificare in quanto ricercato se viene reperito in un altro Stato membro. L'uso di questa funzionalità presuppone che gli Stati membri abbiano svolto in via preliminare una consultazione di tutte le fonti disponibili a livello nazionale e internazionale, senza però essere riusciti ad accertare l'identità della persona in questione. La proposta contiene garanzie sufficienti per assicurare che in questa categoria il SIS conservi soltanto le impronte digitali di persone per le quali sussistono forti sospetti che abbiano commesso un reato grave o un reato di terrorismo. Di conseguenza, questa nuova categoria di segnalazione può essere usata solo in casi in cui l'autore ignoto di un reato rappresenta un grave rischio per la pubblica sicurezza tale da giustificare il confronto delle impronte con quelle di viaggiatori, ad esempio per evitare che la persona lasci lo spazio senza controlli alle frontiere interne.

La disposizione non autorizza gli utenti finali a inserire impronte digitali in questa categoria qualora non sia possibile stabilirne il collegamento con l'autore di un reato. Un'ulteriore condizione consiste nell'impossibilità di stabilire l'identità della persona ricorrendo ad altre banche dati di impronte digitali nazionali, europee o internazionali. Una volta inserite nel SIS, tali impronte digitali saranno usate per identificare persone la cui identità non può essere accertata altrimenti. Se da tale verifica dovesse risultare una potenziale corrispondenza, lo Stato membro dovrebbe svolgere ulteriori verifiche di impronte digitali, eventualmente con la partecipazione di esperti in dattiloscopia, per appurare se le impronte conservate nel SIS appartengono alla persona in questione, e dovrebbe stabilirne l'identità. Le procedure saranno soggette alla legislazione nazionale. L'identificazione dell'"ignoto ricercato" nel SIS può dar luogo al suo arresto.

Accesso al SIS

Questa sottosezione descrive i nuovi elementi in termini di diritto di accesso al SIS per le autorità nazionali competenti e le agenzie dell'UE (utenti istituzionali).

Autorità nazionali - autorità competenti per l'immigrazione

Per garantire l'uso più efficace del SIS, la proposta permette di accedervi alle autorità nazionali competenti per l'esame delle condizioni e per le decisioni in materia di ingresso, soggiorno e rimpatrio di cittadini di paesi terzi sul territorio degli Stati membri. Questa nuova disposizione permette di consultare il SIS riguardo ai migranti irregolari che non sono stati sottoposti a verifiche in occasione dei consueti controlli di frontiera. La proposta prevede lo stesso trattamento per i cittadini di paesi terzi che attraversano le frontiere esterne ai valichi di frontiera regolari (e quindi sono sottoposti alle verifiche previste per i cittadini di paesi terzi) e per i cittadini di paesi terzi che entrano irregolarmente nello spazio Schengen.

Inoltre, la proposta prevede che gli enti preposti all'immatricolazione di veicoli (articolo 44), natanti e aeromobili abbiano accesso limitato al sistema per svolgere i loro compiti, purché siano servizi pubblici. Ciò permetterà di evitare che tali mezzi di trasporto siano immatricolati se rubati e ricercati in un altro Stato membro. L'iniziativa non è nuova per quanto riguarda i servizi competenti per il rilascio delle carte di circolazione dei veicoli, il cui accesso al SIS era già previsto all'articolo 102 bis della convenzione di Schengen e dal regolamento (CE) n. 1986/2006[32]. Secondo la stessa logica, la proposta prevede l'accesso dei servizi competenti per l'immatricolazione di natanti e aeromobili alle segnalazioni del SIS relative a natanti e aeromobili.

Utenti istituzionali

Europol (articolo 46), Eurojust (articolo 47) e l'Agenzia europea della guardia di frontiera e costiera – nonché le relative squadre, le squadre di personale che assolve compiti attinenti al rimpatrio e i membri delle squadre di sostegno per la gestione della migrazione (articoli 48 e 49) – hanno accesso al SIS e ai dati del SIS di cui hanno bisogno. Sono predisposte garanzie adeguate per assicurare che i dati contenuti nel sistema siano opportunamente protetti (comprese le disposizioni dell'articolo 50, secondo cui tali organi possono accedere esclusivamente ai dati di cui hanno bisogno per svolgere i loro compiti).

Grazie a tali modifiche Europol potrà accedere al SIS anche per consultare segnalazioni su persone scomparse, per sfruttare al meglio il sistema nello svolgimento dei suoi compiti; sono inoltre aggiunte disposizioni che permettono all'Agenzia europea della guardia di frontiera e costiera e alle sue squadre di accedere al sistema quando svolgono le varie operazioni afferenti al loro mandato nell'assistenza agli Stati membri. Nel contesto delle attività del gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità, e al fine di potenziare la condivisione di informazioni sul terrorismo, la Commissione valuterà se Europol debba ricevere automaticamente una notifica dal SIS quando viene creata una segnalazione su un'attività connessa al terrorismo.

Inoltre, secondo la proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)[33], l'unità centrale ETIAS dell'Agenzia europea della guardia di frontiera e costiera interrogherà il SIS

[32] Regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'accesso al sistema d'informazione Schengen di seconda generazione (SIS II) dei servizi competenti negli Stati membri per il rilascio delle carte di circolazione (GU L 381 del 28.12.2006, pag. 1).

[33] COM (2016)731 final.

tramite l'ETIAS per controllare se un cittadino di paese terzo che chiede un'autorizzazione ai viaggi sia oggetto di segnalazione nel SIS. A questo scopo anche l'unità centrale ETIAS avrà pieno accesso al SIS.

Cambiamenti specifici delle segnalazioni

L'articolo 26 prevede che gli Stati membri sospendano temporaneamente le segnalazioni per l'arresto (nel caso di un'operazione di polizia o un'indagine in corso) rendendole visibili soltanto agli uffici SIRENE ma non agli operatori sul terreno per un determinato periodo. Tale disposizione contribuisce a evitare che un'operazione di polizia riservata volta ad arrestare un ricercato pericoloso sia compromessa da un poliziotto non coinvolto nell'operazione stessa.

Gli articoli 32 e 33 riguardano le segnalazioni di persone scomparse. Tali segnalazioni sono modificate in modo da consentire di effettuare segnalazioni preventive qualora si configuri un alto rischio di sottrazione di minori da parte di uno dei genitori e da perfezionare la categorizzazione delle segnalazioni di persone scomparse. La sottrazione di minori da parte di uno dei genitori avviene spesso in circostanze accuratamente pianificate, con l'intenzione di lasciare rapidamente lo Stato membro in cui è stato stabilito il regime di affidamento. Le modifiche colmano una potenziale lacuna dell'attuale legislazione, in cui le segnalazioni relative ai minori possono essere effettuate soltanto quando i minori sono scomparsi, e permetteranno alle autorità degli Stati membri di segnalare i minori soggetti a rischi particolarmente gravi. Grazie a queste modifiche, quando si configura un alto rischio di sottrazione imminente di un minore da parte di uno dei genitori, le guardie di frontiera e le autorità di contrasto ne saranno informate e potranno esaminare più attentamente le circostanze in cui il minore in questione sta viaggiando, sottoponendolo se necessario a custodia protettiva. Tramite gli uffici SIRENE saranno fornite informazioni supplementari, fra l'altro sulla decisione dell'autorità giudiziaria competente che ha richiesto la segnalazione. Il manuale SIRENE sarà modificato di conseguenza. Questa segnalazione richiederà un'apposita decisione dell'autorità giudiziaria che ha affidato la custodia a uno solo dei genitori. Un'ulteriore condizione consiste nell'esistenza di un rischio immediato di sottrazione. Lo status delle segnalazioni di minori scomparsi sarà aggiornato automaticamente al raggiungimento dell'età adulta.

L'articolo 34 permette di aggiungere a una segnalazione i dati sui veicoli se esistono indizi concreti che il veicolo sia collegato alla persona ricercata.

L'articolo 37 introduce una nuova forma di verifica, il "controllo di indagine", intesa soprattutto a sostenere misure contro il terrorismo e i reati gravi, che permette alle autorità di fermare e interrogare una persona. Si tratta di un controllo più approfondito dell'attuale controllo discreto, ma che non comprende la perquisizione personale e non equivale all'arresto; può comunque fornire informazioni sufficienti per decidere di prendere ulteriori provvedimenti. Anche l'articolo 36 è modificato per tener conto di questo tipo di verifica aggiuntivo.

La proposta prevede la possibilità di inserire nel SIS segnalazioni relative a documenti vergini e documenti di identità rilasciati (articolo 36) nonché veicoli, compresi natanti e aeromobili (articoli 32 e 34), se collegati a segnalazioni su persone effettuate in conformità di tali articoli. L'articolo 37 modificato prevede le iniziative da prendere sulla base di dette segnalazioni. L'obiettivo è puramente investigativo, ossia consentire alle autorità di affrontare situazioni in cui più persone usano documenti autentici simili tra loro di cui non sono i legittimi proprietari.

L'articolo 38 amplia l'elenco degli oggetti per i quali possono essere effettuate segnalazioni, aggiungendo documenti falsificati, veicoli a prescindere dal sistema di propulsione (non solo a benzina o diesel ma anche elettrici ecc.), banconote falsificate, apparecchiature informatiche e componenti identificabili di veicoli e macchinari industriali. L'elenco non comprende più i mezzi di pagamento poiché le relative segnalazioni erano poco efficaci e non davano luogo quasi mai a riscontri positivi.

Per chiarire il procedimento da seguire quando viene rinvenuto un oggetto per il quale è stata effettuata una segnalazione, l'articolo 39 modificato prevede il sequestro dell'oggetto conformemente alla legislazione nazionale, oltre all'obbligo di contattare l'autorità che ha effettuato la segnalazione.

Protezione dei dati e sicurezza

La proposta chiarisce le competenze in materia di prevenzione, segnalazione e reazione a incidenti che potrebbero minacciare la sicurezza o l'integrità dell'infrastruttura del SIS, dei dati SIS o delle informazioni supplementari (articoli 10, 16 e 57).

L'articolo 12 contiene disposizioni sulla conservazione e consultazione di registri della cronistoria delle segnalazioni.

Lo stesso articolo 12 contiene disposizioni sull'interrogazione automatizzata mediante scansione delle targhe di veicoli a motore, mediante sistemi di riconoscimento automatico delle targhe, e prevede che gli Stati membri tengano un registro aggiornato di tali interrogazioni conformemente alle rispettive legislazioni nazionali.

L'articolo 15, paragrafo 3, riprende l'articolo 15, paragrafo 3, della decisione 2007/533/GAI del Consiglio e prevede che la Commissione sia responsabile della gestione del contratto dell'infrastruttura di comunicazione, ivi compresi l'esecuzione del bilancio, l'acquisizione e il rinnovo. Tali compiti saranno trasferiti a eu-LISA nella seconda mandata di proposte sul SIS del giugno 2017.

L'articolo 21 estende l'obbligo di valutare l'adeguatezza, la pertinenza e l'importanza di un caso ai fini della sua applicazione alle decisioni di proroga della validità di una segnalazione. Tale articolo impone inoltre per la prima volta agli Stati membri di effettuare in ogni circostanza una segnalazione a norma degli articoli 34, 36 e 38 (secondo i casi) su persone la cui attività rientra nell'ambito di applicazione degli articoli 1, 2, 3 e 4 della decisione quadro 2002/475/GAI del Consiglio sulla lotta contro il terrorismo, e su oggetti collegati a dette persone.

Categorie di dati e trattamento dei dati

La proposta introduce nuovi tipi di informazioni (articolo 20) che possono essere conservate su persone per cui è stata effettuata una segnalazione:

- il fatto che la persona sia coinvolta in attività di cui agli articoli 1, 2, 3 e 4 della decisione quadro 2002/475/GAI del Consiglio;
- altre osservazioni relative alla persona; la ragione della segnalazione;
- il numero di registrazione nazionale della persona e il luogo di registrazione;

- la categorizzazione del tipo di caso se si riferisce a una persona scomparsa (solo per le segnalazioni di cui all'articolo 32);
- gli estremi del documento d'identità o di viaggio;
- copia a colori del documento d'identità o di viaggio;
- i profili DNA (solo in mancanza di impronte digitali che permettano l'identificazione).

L'articolo 59 amplia l'elenco dei dati personali che possono essere inseriti e trattati nel SIS in casi di usurpazione di identità. Tali dati possono essere inseriti solo con il consenso della vittima dell'usurpazione di identità. L'elenco comprende adesso anche:

- immagini facciali;
- impronte palmari;
- estremi dei documenti di identità;
- indirizzo della vittima;
- nomi del padre e della madre della vittima.

L'articolo 20 prevede che le segnalazioni contengano informazioni più dettagliate, in particolare gli estremi del documento di identificazione personale dell'interessato, e la possibilità di introdurre categorie distinte di minori scomparsi secondo le circostanze della scomparsa (minori non accompagnati, sottratti da uno dei genitori, in fuga ecc.): queste informazioni sono essenziali affinché gli utenti finali prendano senza indugio le misure necessarie per proteggere i minori. L'aumento delle informazioni consente di identificare meglio la persona interessata e al contempo permette agli utenti finali di prendere decisioni con maggior cognizione di causa. Al fine di proteggere gli utenti finali che svolgono le verifiche, il SIS mostrerà anche se la persona in relazione alla quale è stata effettuata una segnalazione rientra in una delle categorie di cui agli articoli 1, 2, 3 e 4 della decisione quadro 2002/475/GAI del Consiglio sulla lotta contro il terrorismo[34].

La proposta chiarisce che gli Stati membri non devono copiare dati inseriti da altri Stati membri in altri archivi di dati nazionali (articolo 53).

Conservazione

Il periodo massimo di conservazione delle segnalazioni di persone sarà protratto a cinque anni, fatta eccezione per le segnalazioni nell'ambito di controlli discreti, di indagine o specifici, per le quali il periodo resta pari a un anno. Gli Stati membri possono tuttora stabilire periodi più brevi. L'aumento della scadenza massima segue le pratiche nazionali di estendere tale scadenza se una segnalazione non ha ancora conseguito il suo scopo e la persona interessata continua a essere ricercata. È stato inoltre necessario allineare il SIS al periodo di conservazione previsto da altri strumenti, come la direttiva rimpatri ed Eurodac. A fini di

[34] 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).

trasparenza e chiarezza occorre fissare lo stesso periodo di conservazione per le segnalazioni di persone, tranne le segnalazioni effettuate nell'ambito di controlli discreti, di indagine o specifici. L'aumento del periodo di conservazione non danneggia gli interessati poiché una segnalazione non può essere conservata più a lungo di quanto necessario alla sua finalità. L'articolo 52 fissa esplicitamente norme sulla cancellazione delle segnalazioni. L'articolo 51 stabilisce il periodo di tempo per esaminare le segnalazioni e prevede, in particolare, un periodo di conservazione ridotto per le segnalazioni di oggetti: tranne in caso di necessità operativa di mantenere un periodo più lungo, il periodo di conservazione per gli oggetti è stato ridotto a cinque anni per allinearlo a quello delle segnalazioni su persone. La data di scadenza per documenti rilasciati e documenti vergini rimane invece di 10 anni poiché il periodo di validità dei documenti è appunto di 10 anni.

Cancellazione

L'articolo 52 stabilisce le circostanze in cui le segnalazioni devono essere cancellate, introducendo una maggiore armonizzazione tra le prassi nazionali in questo settore. L'articolo 51 stabilisce disposizioni particolari che permettono all'ufficio SIRENE di cancellare di propria iniziativa segnalazioni non più necessarie se non riceve risposta dalle autorità competenti.

Diritto dell'interessato di accedere ai dati, rettificare i dati inesatti e cancellare i dati archiviati illecitamente

Le norme dettagliate sui diritti degli interessati sono rimaste invariate poiché le regole vigenti garantiscono già un livello elevato di protezione e sono conformi al regolamento (UE) 2016/679[35] e alla direttiva (UE) 2016/680[36]. In più l'articolo 63 stabilisce le circostanze in cui gli Stati membri possono decidere di non comunicare informazioni agli interessati. Ciò può avvenire per uno dei motivi elencati in detto articolo e dev'essere una misura proporzionata e necessaria, in linea con la legislazione nazionale.

Condivisione con Interpol dei dati su documenti smarriti, rubati, altrimenti sottratti o invalidati

L'articolo 63 riprende fedelmente l'articolo 55 della decisione 2007/533/GAI del Consiglio poiché la questione della migliore interoperabilità tra la sezione del SIS relativa ai documenti e la banca dati di Interpol sui documenti rubati o smarriti sarà affrontata dalla comunicazione del gruppo di esperti ad alto livello e nella seconda mandata delle proposte sul SIS del giugno 2017.

Statistiche

[35] 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).

[36] 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 (GU L 119 del 4.5.2016, pag. 89).

Per conservare una visione d'insieme del funzionamento dei ricorsi nella pratica, l'articolo 66 stabilisce disposizioni su un sistema statistico standard che fornisca relazioni annuali sui numeri di:

- richieste di accesso da parte degli interessati;
- richieste di rettifica di dati inesatti e cancellazione di dati archiviati illecitamente;
- cause pendenti dinanzi ai giudici;
- cause in cui il giudice ha statuito a favore del ricorrente; e
- osservazioni sui casi di riconoscimento reciproco delle decisioni definitive adottate da giudici o autorità di altri Stati membri su segnalazioni create dallo Stato segnalante.

Monitoraggio e statistiche

L'articolo 71 stabilisce le disposizioni da adottare per garantire il corretto monitoraggio del SIS e il relativo funzionamento in relazione ai suoi obiettivi. A tale scopo eu-LISA è incaricata di fornire statistiche giornaliere, mensili e annuali sul modo in cui viene utilizzato il sistema.

In virtù dell'articolo 71, paragrafo 5, eu-LISA fornisce agli Stati membri, alla Commissione, a Europol, a Eurojust e all'Agenzia europea della guardia di frontiera e costiera le relazioni statistiche che produce e permette alla Commissione di richiedere relazioni statistiche aggiuntive e relazioni sulla qualità dei dati inerenti alla comunicazione tramite SIS e SIRENE.

L'articolo 71, paragrafo 6, stabilisce che venga creato e ospitato un registro centrale di dati nell'ambito dell'attività di monitoraggio del funzionamento del SIS svolta da eu-LISA. Consente così al personale autorizzato degli Stati membri, della Commissione, di Europol, di Eurojust e dell'Agenzia europea della guardia di frontiera e costiera di accedere ai dati elencati all'articolo 71, paragrafo 3, per redigere le statistiche richieste.

2016/0409 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

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 il regolamento (UE) n. 515/2014 e abroga il regolamento (CE) n. 1986/2006, la decisione 2007/533/GAI del Consiglio e la decisione 2010/261/UE della Commissione

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 82, paragrafo 1, secondo comma, lettera d), l'articolo 85, paragrafo 1, l'articolo 87, paragrafo 2, lettera a), e l'articolo 88, paragrafo 2, lettera a),

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Il sistema d'informazione Schengen (SIS) rappresenta uno strumento fondamentale per l'applicazione delle disposizioni dell'acquis di Schengen integrate nell'ambito dell'Unione europea. Il SIS è una delle principali misure compensative che contribuiscono a mantenere un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione europea, sostenendo la cooperazione operativa fra guardie di frontiera, autorità di polizia, doganali e altre autorità di contrasto e autorità giudiziarie in materia penale.

(2) Il SIS è stato istituito a norma delle disposizioni del titolo IV della 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, firmata il 19 giugno 1990[37] (convenzione di Schengen). L'incarico di sviluppare il SIS di seconda generazione (SIS II) è stato affidato alla Commissione con regolamento (CE) n. 2424/2001 del Consiglio[38] e decisione 2001/886/GAI del Consiglio[39] e il SIS II è stato istituito con regolamento (CE) n. 1987/2006[40] e

[37] GU L 239 del 22.9.2000, pag. 19. Convenzione modificata dal regolamento (CE) n. 1160/2005 del Parlamento europeo e del Consiglio (GU L 191 del 22.7.2005, pag. 18).

[38] GU L 328 del 13.12.2001, pag. 4.

[39] Decisione 2001/886/GAI del Consiglio, del 6 dicembre 2001, sullo sviluppo del Sistema d'informazione Schengen di seconda generazione (SIS II) (GU L 328 del 13.12.2001, pag. 1).

decisione 2007/533/GAI del Consiglio[41]. Il SIS II ha sostituito il SIS istituito sulla base della convenzione di Schengen.

(3) Tre anni dopo l'entrata in funzione del SIS II, la Commissione ha svolto una valutazione del sistema ai sensi dell'articolo 24, paragrafo 5, dell'articolo 43, paragrafo 5, e dell'articolo 50, paragrafo 5, del regolamento (CE) n. 1987/2006 e ai sensi dell'articolo 59 e dell'articolo 65, paragrafo 5, della decisione 2007/533/GAI. La relazione di valutazione e il relativo documento di lavoro dei servizi della Commissione sono stati adottati il 21 dicembre 2016[42]. Le raccomandazioni espresse in tali documenti dovrebbero essere recepite, laddove appropriato, nel presente regolamento.

(4) Il presente regolamento costituisce la fonte normativa necessaria per disciplinare il SIS nelle materie rientranti nell'ambito di applicazione del titolo V, capi 4 e 5, del trattato sul funzionamento dell'Unione europea. Il regolamento (UE) 2018/... del Parlamento europeo e del Consiglio sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera[43] costituisce la fonte normativa necessaria per disciplinare il SIS nelle materie rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sul funzionamento dell'Unione europea.

(5) Il fatto che la fonte normativa necessaria per disciplinare il SIS consti di strumenti separati non pregiudica il principio secondo il quale il SIS costituisce un unico sistema d'informazione che dovrebbe operare in quanto tale. È pertanto opportuno che alcune disposizioni di tali strumenti siano identiche.

(6) È necessario specificare gli obiettivi del SIS, la sua architettura tecnica e il suo finanziamento, fissare regole sul suo esercizio e uso da un'estremità all'altra e definire le competenze, le categorie di dati da inserire nel sistema, le finalità dell'inserimento dei dati e i relativi criteri, le autorità abilitate ad accedere ai dati, l'uso di identificatori biometrici e ulteriori norme sul trattamento dei dati.

(7) Il SIS consta di un sistema centrale (SIS centrale) e di sistemi nazionali con una copia completa o parziale della banca dati del SIS. Considerando che il SIS è il più importante strumento di scambio di informazioni in Europa, è necessario garantirne il funzionamento ininterrotto a livello tanto centrale quanto nazionale. Pertanto ogni Stato membro dovrebbe istituire una copia completa o parziale della banca dati del SIS e un proprio sistema di riserva.

(8) È necessario tenere un manuale aggiornato recante le modalità dettagliate di scambio di talune informazioni supplementari relative all'azione da intraprendere in seguito

---

40 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 181 del 28.12.2006, pag. 4).

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 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, e documento di lavoro dei servizi della Commissione che accompagna la relazione (GU...).

43 Regolamento (UE) 2018/…

alle segnalazioni. Le autorità nazionali di ciascuno Stato membro (gli uffici SIRENE) dovrebbero garantire lo scambio di tali informazioni.

(9) Per provvedere a uno scambio efficace di informazioni supplementari sulle specifiche azioni da intraprendere in seguito alle segnalazioni, è opportuno potenziare il funzionamento degli uffici SIRENE introducendo requisiti sulle risorse disponibili, sulla formazione degli utenti e sui termini di risposta alle richieste ricevute da altri uffici SIRENE.

(10) La gestione operativa delle componenti centrali del SIS è esercitata dall'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (l'agenzia)[44]. Per consentire all'agenzia di dedicare le risorse finanziarie e umane necessarie per tutti gli aspetti della gestione operativa del SIS centrale, il presente regolamento dovrebbe stabilirne dettagliatamente i compiti, in particolare riguardo agli aspetti tecnici dello scambio di informazioni supplementari.

(11) Fatta salva la responsabilità degli Stati membri riguardo all'esattezza dei dati inseriti nel SIS, l'agenzia dovrebbe assumere la competenza di migliorare la qualità dei dati introducendo uno strumento di monitoraggio centrale della qualità dei dati, e di presentare a intervalli regolari relazioni agli Stati membri.

(12) Per consentire di monitorare meglio l'uso del SIS nell'analisi delle tendenze relative ai reati, l'agenzia dovrebbe essere in grado di sviluppare una capacità avanzata di fornire statistiche agli Stati membri, alla Commissione, a Europol e all'Agenzia europea della guardia di frontiera e costiera, senza compromettere l'integrità dei dati. È opportuno pertanto istituire un archivio statistico centrale. Nessuna delle statistiche prodotte dovrebbe contenere dati personali.

(13) Il SIS dovrebbe contenere ulteriori categorie di dati che consentano agli utenti finali di adottare decisioni in piena cognizione di causa sulla base di una segnalazione senza perdere tempo. Di conseguenza, per facilitare l'identificazione delle persone e individuare le identità multiple, le categorie di dati relative alle persone dovrebbero includere un riferimento al documento di identificazione personale o al numero di identificazione personale e una copia di tale documento se disponibile.

(14) Il SIS non dovrebbe conservare i dati usati per l'interrogazione, ad eccezione dei registri conservati per verificare la legittimità dell'interrogazione, per controllare la liceità del trattamento dei dati, per l'autocontrollo e per garantire il corretto funzionamento dell'N.SIS, l'integrità e la sicurezza dei dati.

(15) Il SIS, per contribuire alla corretta identificazione degli interessati, dovrebbe consentire il trattamento di dati biometrici. Per la stessa ragione, il SIS dovrebbe inoltre consentire il trattamento di dati relativi a persone la cui identità è stata usurpata (per evitare i disagi causati da errori di identificazione), fatte salve adeguate garanzie, fra cui il consenso dell'interessato e una rigorosa limitazione delle finalità per cui tali dati possono essere lecitamente trattati.

---

[44] Istituita dal 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).

(16) Gli Stati membri dovrebbero adottare le disposizioni tecniche necessarie affinché gli utenti finali, ogni volta che sono autorizzati a consultare una banca dati nazionale della polizia o dell'immigrazione, consultino parallelamente anche il SIS in conformità dell'articolo 4 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio[45]. Ciò dovrebbe permettere al SIS di funzionare come principale misura compensativa nello spazio senza controlli alle frontiere interne e di contrastare meglio la dimensione transfrontaliera della criminalità e la mobilità dei criminali.

(17) È opportuno che il presente regolamento stabilisca le condizioni per l'uso dei dati dattiloscopici e delle immagini facciali a fini di identificazione. L'uso di immagini facciali a fini di identificazione nel SIS dovrebbe inoltre contribuire a garantire la coerenza nelle procedure di controllo di frontiera in cui l'identificazione e la verifica dell'identità devono essere effettuate mediante impronte digitali e immagini facciali. L'interrogazione con i dati dattiloscopici dovrebbe essere obbligatoria in caso di dubbio sull'identità di una persona. È opportuno che le immagini facciali possano essere usate a fini di identificazione solo nel contesto dei controlli di frontiera di routine ai dispositivi self-service e ai varchi automatici.

(18) L'introduzione di un servizio automatizzato di identificazione delle impronte digitali nel SIS completa l'attuale meccanismo di Prüm sull'accesso reciproco in linea transfrontaliero a banche dati nazionali del DNA designate e ai sistemi automatizzati di identificazione delle impronte digitali[46]. Il meccanismo di Prüm consente l'interconnessione dei sistemi nazionali di identificazione delle impronte digitali, in modo che uno Stato membro possa introdurre una richiesta per verificare se l'autore di un reato di cui sono state rinvenute le impronte digitali sia noto in altri Stati membri. Poiché però il meccanismo verifica soltanto se la persona cui appartengono le impronte digitali sia nota in un determinato momento, se l'autore di un reato viene identificato solo in seguito in uno Stato membro non sarà necessariamente arrestato. L'interrogazione delle impronte digitali del SIS permette di ricercare attivamente l'autore di un reato. Dovrebbe quindi essere possibile caricare le impronte digitali dell'autore ignoto di un reato nel SIS, purché la persona cui appartengono possa essere identificata con un elevato grado di probabilità come autore di un reato grave o di un atto di terrorismo. La misura riguarda soprattutto i casi in cui sono rilevate impronte digitali su un'arma o altro corpo del reato. La mera presenza di impronte digitali sul luogo del reato non andrebbe considerata indicazione di un elevato grado di probabilità che le impronte siano quelle dell'autore del reato. Un'ulteriore condizione per effettuare tale segnalazione dovrebbe consistere nel non poter appurare l'identità dell'autore del reato ricorrendo ad altre banche dati nazionali, europee o internazionali. Se dall'interrogazione di tali impronte digitali dovesse risultare una potenziale corrispondenza, lo Stato membro dovrebbe svolgere ulteriori verifiche

---

45 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).

46 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) e 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).

consultando impronte digitali, possibilmente con la partecipazione di esperti in dattiloscopia, per appurare se le impronte conservate nel SIS appartengano alla persona in questione, di cui dovrebbe altresì stabilire l'identità. Le procedure dovrebbero essere soggette alla legislazione nazionale. L'identificazione di un "ignoto ricercato" nel SIS può contribuire sostanzialmente all'indagine, determinando eventualmente l'arresto se sussistono tutte le condizioni.

(19) Le impronte digitali rilevate sul luogo del reato dovrebbero poter essere confrontate con le impronte digitali conservate nel SIS, se si può stabilire con un elevato grado di probabilità che appartengono all'autore di un reato grave o di un reato di terrorismo. Per reati gravi dovrebbero intendersi i reati elencati nella decisione quadro 2002/584/GAI del Consiglio[47] e per reati terroristici i reati in base al diritto nazionale di cui alla decisione quadro 2002/475/GAI del Consiglio[48].

(20) Qualora non siano disponibili dati dattiloscopici dovrebbe essere possibile aggiungere un profilo DNA, accessibile soltanto agli utenti autorizzati. I profili DNA dovrebbero facilitare l'identificazione di persone scomparse bisognose di protezione e specialmente minori scomparsi, in particolare se è autorizzato l'uso di profili DNA di genitori o fratelli per consentire l'identificazione. I dati DNA non dovrebbero contenere riferimenti all'origine razziale.

(21) Il SIS dovrebbe contenere segnalazioni di persone ricercate per l'arresto a fini di consegna o a fini di estradizione. Oltre alle segnalazioni, è opportuno prevedere lo scambio di informazioni supplementari necessarie ai fini delle procedure di consegna ed estradizione. In particolare, è opportuno che nell'ambito del SIS siano trattati i dati di cui all'articolo 8 della 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[49]. Per ragioni operative è opportuno che lo Stato membro segnalante, su autorizzazione dell'autorità giudiziaria, renda temporaneamente non consultabile una segnalazione per l'arresto qualora una persona destinataria di mandato d'arresto europeo sia intensamente e attivamente ricercata e il successo dell'operazione di ricerca rischi di essere compromesso da utenti finali che non vi partecipano. La temporanea sospensione della disponibilità di tali segnalazioni non dovrebbe superare le 48 ore.

(22) È opportuno contemplare la possibilità di aggiungere nel SIS una traduzione dei dati complementari introdotti ai fini della consegna in forza del mandato d'arresto europeo o ai fini dell'estradizione.

(23) Il SIS dovrebbe contenere segnalazioni su persone scomparse per consentire di proteggerle o prevenire minacce alla pubblica sicurezza. La segnalazione nel SIS di minori a rischio di sottrazione (per impedire un futuro danno non ancora inferto, ad esempio in caso di rischio di sottrazione del minore da parte di uno dei genitori) dovrebbe costituire una prassi limitata sottoposta a garanzie rigorose e adeguate. In

---

47 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).

48 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).

49 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).

caso di minori, tali segnalazioni e le corrispondenti procedure dovrebbero servire l'interesse superiore del minore, in conformità dell'articolo 24 della Carta dei diritti fondamentali dell'Unione europea e della Convenzione delle Nazioni Unite sui diritti del fanciullo del 20 novembre 1989.

(24) È opportuno introdurre una nuova azione per i casi sospetti di terrorismo e reati gravi, che permetta di fermare e interrogare una persona se si sospetta che abbia commesso un reato grave o se vi è motivo di credere che intenda commetterlo, al fine di fornire allo Stato membro segnalante le informazioni più precise possibili. Questa nuova azione non dovrebbe comportare la perquisizione o l'arresto della persona. Dovrebbe comunque fornire informazioni sufficienti per decidere se intraprendere ulteriori iniziative. Per reato grave è opportuno che si intendano i reati elencati nella decisione 2002/584/GAI del Consiglio.

(25) Il SIS dovrebbe contenere nuove categorie di oggetti di valore elevato, quali apparecchiature elettroniche e tecniche, che possono essere identificati e consultati con un numero unico.

(26) Gli Stati membri dovrebbero avere la possibilità di apporre a una segnalazione un'indicazione detta "indicatore di validità", affinché non sia eseguita sul proprio territorio l'azione richiesta dalla segnalazione. Per le segnalazioni a scopo di arresto a fini di consegna è opportuno che il presente regolamento non venga in alcun modo interpretato in modo da derogare alle disposizioni contenute nella decisione quadro 2002/584/GAI o impedirne l'applicazione. La decisione di apporre un indicatore di validità a una segnalazione dovrebbe essere basata unicamente sui motivi di rifiuto previsti dalla suddetta decisione quadro.

(27) Qualora sia stato apposto un indicatore di validità e il luogo di soggiorno della persona ricercata per l'arresto a fini di consegna sia stato individuato, tale luogo dovrebbe essere sempre comunicato all'autorità giudiziaria emittente, che deciderà eventualmente di trasmettere un mandato d'arresto europeo all'autorità giudiziaria competente in conformità delle disposizioni della decisione quadro 2002/584/GAI.

(28) Gli Stati membri dovrebbero avere la possibilità di stabilire connessioni fra le segnalazioni nel SIS. La creazione di connessioni fra due o più segnalazioni da parte di uno Stato membro non dovrebbe incidere sull'azione da eseguire, né sui termini di conservazione o sui diritti di accesso alle segnalazioni.

(29) Le segnalazioni non dovrebbero essere conservate nel SIS oltre il periodo necessario per la realizzazione degli obiettivi per i quali sono state effettuate. Per ridurre gli oneri amministrativi a carico delle diverse autorità competenti per il trattamento dei dati sulle persone a diversi scopi, è opportuno allineare il periodo di conservazione delle segnalazioni di persone ai periodi di conservazione previsti per il rimpatrio e il soggiorno irregolare. Inoltre gli Stati membri prorogano regolarmente la data di scadenza delle segnalazioni di persone se non è stato possibile intraprendere l'azione necessaria entro il termine originariamente stabilito. Pertanto, il periodo di conservazione delle segnalazioni di persone non dovrebbe essere superiore a cinque anni. In linea generale, le segnalazioni di persone dovrebbero essere cancellate automaticamente dal SIS dopo cinque anni, tranne le segnalazioni effettuate nell'ambito di controlli discreti, specifici e di indagine. Queste ultime dovrebbero essere cancellate dopo un anno. Le segnalazioni di oggetti inserite ai fini di un

controllo discreto, di indagine o specifico dovrebbero essere cancellate automaticamente dal SIS dopo un anno, poiché sono sempre collegate a persone. Le segnalazioni di oggetti a fini di sequestro o di prova in un procedimento penale dovrebbero essere cancellate automaticamente dal SIS dopo cinque anni, poiché dopo tale periodo la probabilità di reperire gli oggetti in questione è molto bassa e il loro valore economico è notevolmente diminuito. Le segnalazioni di documenti d'identificazione vergini o rilasciati dovrebbero essere mantenute per dieci anni, poiché il periodo di validità dei documenti è di dieci anni a partire dall'emissione. La decisione di conservare le segnalazioni di persone dovrebbe essere basata su una valutazione individuale approfondita. Gli Stati membri dovrebbero esaminare le segnalazioni di persone entro il periodo definito e tenere statistiche sul numero di segnalazioni di persone per le quali il periodo di conservazione è stato prolungato.

(30) L'inserimento e la proroga della data di scadenza di una segnalazione nel SIS dovrebbero essere soggetti a un requisito obbligatorio di proporzionalità, in base al quale si verifichi se l'adeguatezza, la pertinenza e l'importanza del caso giustifichino l'inserimento della segnalazione nel SIS. I reati di cui agli articoli 1, 2, 3 e 4 della decisione quadro 2002/475/GAI del Consiglio sulla lotta contro il terrorismo[50] costituiscono una minaccia molto grave alla pubblica sicurezza, all'integrità di vita delle persone e alla società e sono estremamente difficili da prevenire, accertare e indagare in uno spazio senza controlli di frontiera interni in cui i potenziali criminali circolano liberamente. Laddove una persona o un oggetto sia ricercato in relazione a tali reati, è sempre necessario introdurre nel SIS la corrispondente segnalazione relativa a persone ricercate nell'ambito di un procedimento giudiziario penale, a persone od oggetti ricercati ai fini di un controllo discreto, di indagine o specifico, o a oggetti ricercati a fini di sequestro, poiché nessun altro mezzo sarebbe efficace per conseguire tale scopo.

(31) È necessario fornire chiarimenti sulla cancellazione delle segnalazioni. Una segnalazione dovrebbe essere conservata solo per il periodo necessario a realizzare l'obiettivo per cui è stata effettuata. Poiché gli Stati membri seguono pratiche diverse per stabilire il momento in cui una segnalazione realizza il suo obiettivo, è opportuno fissare criteri dettagliati per ciascuna categoria di segnalazione che determinino quando debba essere cancellata dal SIS.

(32) L'integrità dei dati SIS è di primaria importanza. È opportuno quindi stabilire garanzie adeguate per il trattamento dei dati SIS a livello tanto centrale quanto nazionale, per garantire la sicurezza dei dati da un'estremità all'altra. Le autorità competenti per il trattamento dei dati dovrebbero essere vincolate ai requisiti di sicurezza previsti dal presente regolamento e soggette a una procedura uniforme di segnalazione degli incidenti.

(33) I dati trattati nel SIS in applicazione del presente regolamento non dovrebbero essere trasferiti a paesi terzi o ad organizzazioni internazionali, né messi a loro disposizione. Tuttavia, è opportuno rafforzare la cooperazione tra l'Unione europea e Interpol promuovendo un efficace scambio di informazioni relative ai passaporti. In caso di trasferimento di dati personali dal SIS a Interpol, si dovrebbe prevedere un livello

[50] 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).

adeguato di protezione di tali dati, garantito da un accordo e accompagnato da garanzie e condizioni rigorose.

(34) È opportuno accordare l'accesso al SIS alle autorità preposte all'immatricolazione di veicoli, natanti e aeromobili per consentire loro di verificare se un mezzo di trasporto sia già ricercato in uno Stato membro a scopo di sequestro o di controllo. Alle autorità che sono servizi pubblici dovrebbe essere concesso l'accesso diretto. Tale accesso dovrebbe essere limitato alle segnalazioni relative ai mezzi di trasporto di rispettiva competenza e al relativo documento di immatricolazione o alla relativa targa. È quindi opportuno inserire nel presente regolamento le disposizioni del regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio[51] e abrogare quest'ultimo.

(35) Al trattamento dei dati da parte delle autorità nazionali competenti a fini di prevenzione, indagine e accertamento di reati gravi o reati di terrorismo o di perseguimento di reati ed esecuzione di sanzioni penali, compresa la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse, si applicano le disposizioni nazionali di attuazione della direttiva (UE) 2016/680. È opportuno che nel presente regolamento siano ulteriormente specificate, ove necessario, le disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[52] e della direttiva (UE) 2016/680.

(36) Il regolamento (UE) 2016/679 dovrebbe applicarsi al trattamento dei dati personali svolto dalle autorità nazionali a norma del presente regolamento quando non si applica la direttiva (UE) 2016/680. Il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio[53] dovrebbe applicarsi al trattamento dei dati personali svolto dalle istituzioni e dagli organismi dell'Unione nell'assolvimento dei loro compiti a norma del presente regolamento.

(37) È opportuno che nel presente regolamento siano ulteriormente specificate, ove necessario, le disposizioni della direttiva (UE) 2016/680, del regolamento (UE) 2016/679 e del regolamento (CE) n. 45/2001. Al trattamento dei dati personali da parte di Europol si applica il regolamento (UE) 2016/794 che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (regolamento Europol)[54].

(38) Al trattamento dei dati SIS da parte di Eurojust si applicano le disposizioni in materia di protezione dei dati della decisione 2002/187/GAI, del 28 febbraio 2002, che

---

51 Regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'accesso al sistema d'informazione Schengen di seconda generazione (SIS II) dei servizi competenti negli Stati membri per il rilascio delle carte di circolazione (GU L 381 del 28.12.2006, pag. 1).

52 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).

53 Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

54 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 25.5.2016, pag. 53).

istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità[55], in particolare quelle relative al potere dell'autorità di controllo comune, istituita da detta decisione, di sorvegliare le attività di Eurojust e quelle relative alla responsabilità in caso di trattamento illecito dei dati personali da parte di Eurojust. Qualora le interrogazioni svolte da Eurojust nel SIS rivelino l'esistenza di una segnalazione effettuata da uno Stato membro, Eurojust non può intraprendere l'azione richiesta. Dovrebbe pertanto informare lo Stato membro interessato e permettergli di dare seguito al caso.

(39) Per quanto riguarda la riservatezza, le pertinenti disposizioni dello statuto dei funzionari e del regime applicabile agli altri agenti dell'Unione europea dovrebbero applicarsi ai funzionari o altri agenti che sono impiegati e che lavorano per il SIS.

(40) Gli Stati membri e l'agenzia dovrebbero mantenere piani di sicurezza per agevolare l'attuazione degli obblighi in materia di sicurezza e dovrebbero cooperare tra loro al fine di affrontare le questioni di sicurezza da una prospettiva comune.

(41) Le autorità nazionali di controllo indipendenti dovrebbero controllare la liceità del trattamento dei dati personali da parte degli Stati membri in relazione al presente regolamento. È opportuno stabilire i diritti degli interessati in materia di accesso, rettifica e cancellazione dei dati personali che li riguardano conservati nel SIS e i conseguenti diritti di ricorso dinanzi ai giudici nazionali, nonché il reciproco riconoscimento delle sentenze. È quindi opportuno esigere dagli Stati membri statistiche annuali.

(42) Le autorità di controllo dovrebbero provvedere affinché sia svolto un controllo delle operazioni di trattamento dei dati nel rispettivo N.SIS, conformemente alle norme di revisione internazionali, almeno ogni quattro anni. Il controllo dovrebbe essere svolto dalle autorità di controllo oppure da queste commissionato direttamente a un revisore per la protezione di dati indipendente. Il revisore indipendente dovrebbe rimanere sotto il controllo e la responsabilità della o delle autorità nazionali di controllo, che di conseguenza dovrebbero ordinare esse stesse la revisione, definirne chiaramente la finalità, il campo di applicazione e la metodologia, fornire istruzioni e supervisionare il controllo e i relativi risultati finali.

(43) A norma del regolamento (UE) 2016/794 (regolamento Europol), Europol sostiene e potenzia l'azione delle autorità competenti degli Stati membri e la loro cooperazione nel combattere il terrorismo e altre forme gravi di criminalità e fornisce analisi e valutazioni della minaccia. L'estensione dei diritti di accesso di Europol alle segnalazioni di persone scomparse nel SIS dovrebbe migliorare la capacità di Europol di fornire alle autorità di contrasto nazionali prodotti operativi e analitici completi sulla tratta di esseri umani e sullo sfruttamento sessuale dei minori, anche online. Ciò contribuirebbe a una migliore prevenzione di tali reati, alla protezione delle potenziali vittime e alle indagini sugli autori. Anche il Centro europeo per la lotta alla criminalità informatica di Europol beneficerebbe del nuovo accesso di Europol alle segnalazioni di persone scomparse nel SIS, in particolare per i casi di delinquenti sessuali itineranti e di abuso sessuale di minori online, in cui gli autori dei reati sostengono spesso di avere o di potere ottenere accesso a minori che potrebbero essere stati segnalati come

[55] Decisione 2002/187/GAI del Consiglio, del 28 febbraio 2002, che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità (GU L 63 del 6.3.2002, pag. 1).

scomparsi. Inoltre il Centro europeo contro il traffico di migranti di Europol, svolgendo un fondamentale ruolo strategico nel contrastare il favoreggiamento della migrazione irregolare, dovrebbe ottenere l'accesso alle segnalazioni di persone cui è negato l'ingresso o il soggiorno nel territorio di uno Stato membro, o per motivi di ordine penale o per mancata conformità alle condizioni relative al visto e al soggiorno.

(44) Per colmare le lacune nello scambio di informazioni sul terrorismo, in particolare sui combattenti terroristi stranieri (essendo cruciale sorvegliarne i movimenti), gli Stati membri dovrebbero scambiare con Europol informazioni su attività legate al terrorismo parallelamente all'introduzione di segnalazioni nel SIS, nonché riscontri positivi (hit) e informazioni connesse. Ciò dovrebbe consentire al Centro europeo antiterrorismo di Europol di verificare se nelle banche dati di Europol esistono informazioni contestuali complementari e di fornire analisi di elevata qualità che contribuiscano a smantellare le reti terroristiche e, se possibile, a prevenirne gli attentati.

(45) È inoltre necessario stabilire regole chiare a uso di Europol sul trattamento e sullo scaricamento dei dati SIS per consentire l'uso più ampio possibile del SIS, purché siano rispettate le norme in materia di protezione dei dati previste dal presente regolamento e dal regolamento (UE) 2016/794. Qualora le interrogazioni svolte da Europol nel SIS rivelino l'esistenza di una segnalazione effettuata da uno Stato membro, Europol non può intraprendere l'azione richiesta. Dovrebbe pertanto informare lo Stato membro interessato e permettergli di dare seguito al caso.

(46) Il regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio[56] prevede, ai fini del presente regolamento, che lo Stato membro ospitante autorizzi i membri delle squadre della guardia di frontiera e costiera europea o di squadre di personale che assolve compiti attinenti al rimpatrio, dispiegate dall'Agenzia europea della guardia di frontiera e costiera, a consultare le banche dati europee se tale consultazione è necessaria a conseguire gli obiettivi operativi specificati nel piano operativo per i controlli di frontiera, la sorveglianza di frontiera e i rimpatri. Altre agenzie dell'Unione competenti, in particolare l'Ufficio europeo di sostegno per l'asilo ed Europol, possono inviare esperti, anche se non fanno parte del personale di tali agenzie, nell'ambito delle squadre di sostegno per la gestione della migrazione. L'impiego di squadre della guardia di frontiera e costiera europea, squadre di personale che assolve compiti attinenti al rimpatrio e squadre di sostegno per la gestione della migrazione ha l'obiettivo di offrire un rinforzo operativo e tecnico agli Stati membri richiedenti, in particolare a quelli che devono affrontare sfide migratorie sproporzionate. Per adempiere i compiti loro assegnati, le squadre della guardia di frontiera e costiera europea, le squadre di personale che assolve compiti attinenti al rimpatrio e le squadre di sostegno per la gestione della migrazione hanno bisogno di accedere al SIS tramite un'interfaccia tecnica dell'Agenzia europea della guardia di frontiera e costiera connessa al SIS centrale. Qualora le interrogazioni svolte nel SIS dalla squadra o dalle squadre del personale rivelino l'esistenza di una segnalazione effettuata da uno Stato membro, il membro della squadra o del personale non può

[56] Regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio, del 14 settembre 2016, relativo alla guardia di frontiera e costiera europea e che modifica il regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio e che abroga il regolamento (CE) n. 863/2007 del Parlamento europeo e del Consiglio, il regolamento (CE) n. 2007/2004 del Consiglio e la decisione 2005/267/CE del Consiglio (GU L 251 del 16.9.2016, pag. 1).

intraprendere l'azione richiesta se non è autorizzato a farlo dallo Stato membro ospitante. Dovrebbe pertanto informare lo Stato membro interessato e permettergli di dare seguito al caso.

(47) Secondo la proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), presentata dalla Commissione[57], l'unità centrale ETIAS dell'Agenzia europea della guardia di frontiera e costiera consulterà il SIS tramite l'ETIAS per svolgere la valutazione delle domande di autorizzazione ai viaggi, per la quale è necessario controllare, fra l'altro, se il cittadino di paese terzo che chiede un'autorizzazione ai viaggi sia oggetto di una segnalazione nel SIS. A tale scopo l'unità centrale ETIAS presso l'Agenzia europea della guardia di frontiera e costiera dovrebbe avere accesso al SIS nella misura necessaria ad adempiere il suo mandato, ossia dovrebbe accedere a tutte le categorie di segnalazioni di persone e alle segnalazioni di documenti di identificazione personale vergini o rilasciati.

(48) A causa della loro tecnicità, del loro livello di dettaglio e della necessità di aggiornamenti periodici, taluni aspetti del SIS non possono essere trattati con esaustività dal presente regolamento. Si tratta, ad esempio, delle norme tecniche concernenti l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati, della qualità dei dati e delle regole di consultazione relative agli identificatori biometrici, delle norme sulla compatibilità e priorità delle segnalazioni, dell'apposizione di indicatori di validità, dell'interconnessione delle segnalazioni, della specificazione di nuove categorie di oggetti nell'ambito della categoria delle apparecchiature tecniche ed elettroniche, della data di scadenza delle segnalazioni entro il termine massimo e dello scambio di informazioni supplementari. È pertanto opportuno delegare alla Commissione competenze di esecuzione in relazione ai citati aspetti. Le norme tecniche concernenti la consultazione delle segnalazioni dovrebbero tener conto del corretto funzionamento delle applicazioni nazionali.

(49) È opportuno attribuire alla Commissione competenze di esecuzione al fine di garantire condizioni uniformi di esecuzione del presente regolamento. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011[58]. La procedura di adozione delle disposizioni di attuazione a norma del presente regolamento e del regolamento (UE) 2018/xxx (verifiche di frontiera) dovrebbe essere la stessa.

(50) Per ragioni di trasparenza è opportuno che ogni due anni l'agenzia presenti una relazione sul funzionamento tecnico del SIS centrale e dell'infrastruttura di comunicazione, compresa la sua sicurezza, e sullo scambio di informazioni supplementari. Ogni quattro anni la Commissione dovrebbe provvedere a una valutazione globale.

(51) Poiché gli obiettivi del presente regolamento, vale a dire l'istituzione e la regolamentazione di un sistema comune d'informazione e il relativo scambio di

---

57 COM (2016)731 final.

58 Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

informazioni supplementari, non possono, per loro stessa natura, essere conseguiti in misura sufficiente dagli Stati membri e possono dunque essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(52) Il presente regolamento rispetta i diritti fondamentali e osserva i principi riconosciuti in particolare dalla Carta dei diritti fondamentali dell'Unione europea. In particolare, il presente regolamento si prefigge l'obiettivo di garantire un ambiente sicuro per tutte le persone residenti sul territorio dell'Unione europea e una protezione speciale per i minori che rischiano di essere vittime di tratta o di sottrazione da parte di uno dei genitori, nel pieno rispetto della tutela dei dati personali.

(53) A norma degli articoli 1 e 2 del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non partecipa all'adozione del presente regolamento, non è da esso vincolata né è soggetta alla sua applicazione. Dato che il presente regolamento si basa sull'acquis di Schengen, la Danimarca decide, ai sensi dell'articolo 4 di tale protocollo, entro sei mesi dalla decisione del Consiglio sul presente regolamento, se intende recepirlo nel proprio diritto interno.

(54) Il Regno Unito partecipa al presente regolamento ai sensi dell'articolo 5 del protocollo n. 19 sull'acquis di Schengen integrato nell'ambito dell'Unione europea, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, e dell'articolo 8, paragrafo 2, della decisione 2000/365/CE del Consiglio, del 29 maggio 2000, riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune disposizioni dell'acquis di Schengen[59].

(55) L'Irlanda partecipa al presente regolamento ai sensi dell'articolo 5 del protocollo sull'acquis di Schengen integrato nell'ambito dell'Unione europea, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, e dell'articolo 6, paragrafo 2, della decisione 2002/192/CE del Consiglio, del 28 febbraio 2002, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'acquis di Schengen[60].

(56) Per quanto riguarda l'Islanda e la Norvegia, il presente regolamento costituisce, ai sensi dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sulla loro associazione all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen[61], uno sviluppo delle disposizioni dell'acquis di Schengen che rientrano nel settore di cui all'articolo 1, lettera G, della decisione 1999/437/CE del Consiglio relativa a talune modalità di applicazione dell'accordo[62].

(57) Per quanto riguarda la Svizzera, il presente regolamento costituisce, ai sensi dell'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera

---

59 GU L 131 dell'1.6.2000, pag. 43.
60 GU L 64 del 7.3.2002, pag. 20.
61 GU L 176 del 10.7.1999, pag. 36.
62 GU L 176 del 10.7.1999, pag. 31.

riguardante l'associazione di quest'ultima all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen, uno sviluppo delle disposizioni dell'acquis di Schengen che rientrano nel settore di cui all'articolo 1, lettera G, della decisione 1999/437/CE, in combinato disposto con l'articolo 4, paragrafo 1, delle decisioni 2004/849/CE[63] e 2004/860/CE del Consiglio[64].

(58) Per quanto riguarda il Liechtenstein, il presente regolamento costituisce, ai sensi del protocollo sottoscritto tra l'Unione europea, la Comunità europea, la Confederazione svizzera e il Principato del Liechtenstein sull'adesione del Principato del Liechtenstein all'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen[65], uno sviluppo delle disposizioni dell'acquis di Schengen che rientrano nel settore di cui all'articolo 1, lettera G, della decisione 1999/437/CE, in combinato disposto con l'articolo 3 della decisione 2011/349/UE del Consiglio[66] e con l'articolo 3 della decisione 2011/350/UE del Consiglio[67].

(59) Per quanto riguarda Bulgaria e Romania, il presente regolamento costituisce un atto basato sull'acquis di Schengen o ad esso altrimenti connesso ai sensi dell'articolo 4, paragrafo 2, dell'atto di adesione del 2005, e dovrebbe essere letto in combinato disposto con la decisione 2010/365/UE del Consiglio sull'applicazione delle disposizioni dell'acquis di Schengen relative al sistema d'informazione Schengen nella Repubblica di Bulgaria e in Romania[68].

(60) Per quanto riguarda Cipro e la Croazia, il presente regolamento costituisce un atto basato sull'acquis di Schengen o ad esso altrimenti connesso ai sensi, rispettivamente,

---

63 Decisione 2004/849/CE del Consiglio, del 25 ottobre 2004, relativa alla firma, a nome dell'Unione europea, nonché all'applicazione provvisoria di alcune disposizioni dell'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen (GU L 368 del 15.12.2004, pag. 26).

64 Decisione 2004/860/CE del Consiglio, del 25 ottobre 2004, relativa alla firma, a nome dell'Unità europea, nonché all'applicazione provvisoria di alcune disposizioni dell'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen (GU L 370 del 17.12.2004, pag. 78).

65 GU L 160 del 18.6.2011, pag. 21.

66 Decisione 2011/349/UE del Consiglio, del 7 marzo 2011, sulla conclusione, a nome dell'Unione europea, del protocollo tra l'Unione europea, la Comunità europea, la Confederazione svizzera e il Principato del Liechtenstein sull'adesione del Principato del Liechtenstein all'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen, con particolare riguardo alla cooperazione giudiziaria in materia penale e alla cooperazione di polizia (GU L 160 del 18.6.2011, pag. 1).

67 Decisione 2011/350/UE del Consiglio, del 7 marzo 2011, sulla conclusione, a nome dell'Unione europea, del protocollo tra l'Unione europea, la Comunità europea, la Confederazione svizzera e il Principato del Liechtenstein sull'adesione del Principato del Liechtenstein all'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen, con particolare riguardo alla soppressione dei controlli alle frontiere interne e alla circolazione delle persone (GU L 160 del 18.6.2011, pag. 19).

68 GU L 166 dell'1.7.2010, pag. 17.

dell'articolo 3, paragrafo 2, dell'atto di adesione del 2003, e dell'articolo 4, paragrafo 2, dell'atto di adesione del 2011.

(61) Il presente regolamento dovrebbe applicarsi all'Irlanda alle date stabilite secondo le procedure definite nei pertinenti strumenti relativi all'applicazione dell'acquis di Schengen a tale Stato.

(62) I costi stimati dell'aggiornamento dei sistemi nazionali del SIS e dell'applicazione delle nuove funzionalità, previsti dal presente regolamento, sono inferiori all'importo rimanente nella linea di bilancio per le "Frontiere intelligenti" in conformità del regolamento (UE) n. 515/2014 del Parlamento europeo e del Consiglio[69]. Di conseguenza è opportuno che il presente regolamento riassegni l'importo destinato allo sviluppo di sistemi informatici a sostegno della gestione dei flussi migratori attraverso le frontiere esterne a norma dell'articolo 5, paragrafo 5, lettera b), del regolamento (UE) n. 515/2014.

(63) La decisione 2007/533/GAI del Consiglio e la decisione 2010/261/UE della Commissione[70] dovrebbero pertanto essere abrogate.

(64) Conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001, il garante europeo della protezione dei dati è stato consultato e ha espresso un parere il […],

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1
Scopo generale del SIS

Scopo del SIS è assicurare un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione, inclusi il mantenimento della sicurezza pubblica e dell'ordine pubblico e la salvaguardia della sicurezza nel territorio degli Stati membri, e applicare le disposizioni della parte terza, titolo V, capi 4 e 5, del trattato sul funzionamento dell'Unione europea relative alla circolazione delle persone in detto territorio, avvalendosi delle informazioni trasmesse mediante tale sistema.

---

69 Regolamento (UE) n. 515/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, che istituisce, nell'ambito del Fondo sicurezza interna, lo strumento di sostegno finanziario per le frontiere esterne e i visti (GU L 150 del 20.5.2014, pag. 143).

70 Decisione 2010/261/UE della Commissione, del 4 maggio 2010, relativa al piano di sicurezza per il SIS II centrale e l'infrastruttura di comunicazione (GU L 112 del 5.5.2010, pag. 31).

Articolo 2
Ambito di applicazione

1. Il presente regolamento definisce le condizioni e le procedure applicabili all'inserimento e al trattamento nel SIS delle segnalazioni di persone e oggetti e allo scambio di informazioni supplementari e dati complementari per la cooperazione di polizia e la cooperazione giudiziaria in materia penale.

2. Il presente regolamento contempla anche disposizioni sull'architettura tecnica del SIS, sulle competenze degli Stati membri e dell'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, sulle regole generali sul trattamento dei dati, sui diritti delle persone interessate e sulla responsabilità.

Articolo 3
Definizioni

1. Ai fini del presente regolamento s'intende per:

   (a) "segnalazione": un insieme di dati, compresi gli identificatori biometrici di cui agli articoli 22 e 40, inseriti nel SIS che permette alle autorità competenti di identificare una persona o un oggetto al fine di intraprendere un'azione specifica;

   (b) "informazioni supplementari": le informazioni non facenti parte dei dati di segnalazione conservati nel SIS ma connesse alle segnalazioni del SIS, che devono essere scambiate:

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

      (2) in seguito a un riscontro positivo (hit) al fine di consentire l'azione appropriata;

      (3) quando non è possibile procedere all'azione richiesta;

      (4) con riguardo alla qualità dei dati SIS;

      (5) con riguardo alla compatibilità e alla priorità delle segnalazioni;

      (6) con riguardo ai diritti di accesso;

   (c) "dati complementari": i dati memorizzati nel SIS e connessi alle segnalazioni del SIS, che devono essere immediatamente disponibili per le autorità competenti nei casi in cui una persona i cui dati sono stati inseriti nel SIS sia localizzata grazie all'interrogazione di tale sistema;

   (d) "dati personali": qualsiasi informazione concernente una persona fisica identificata o identificabile ("l'interessato");

   (e) "persona fisica identificabile": la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo

come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

(f) "trattamento dei dati personali": 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;

(g) il "riscontro positivo" nel SIS implica:

(1) che un utente effettui un'interrogazione;

(2) che l'interrogazione riveli la presenza di una segnalazione effettuata da un altro Stato membro nel SIS;

(3) che i dati relativi alla segnalazione nel SIS corrispondano ai dati dell'interrogazione; e

(4) che sia richiesta un'ulteriore azione;

h) "indicatore di validità": sospensione della validità di una segnalazione a livello nazionale apponibile alle segnalazioni per l'arresto, alle segnalazioni di persone scomparse e alle segnalazioni ai fini di un controllo discreto, di indagine o specifico dallo Stato membro che reputi incompatibile con la legislazione nazionale, con i propri obblighi internazionali o con interessi nazionali essenziali dare seguito alla segnalazione; la presenza di un indicatore di validità in corrispondenza a una data segnalazione significa che l'azione richiesta non sarà eseguita sul territorio di detto Stato membro;

i) "Stato membro segnalante": lo Stato membro che ha inserito la segnalazione nel SIS;

j) "Stato membro di esecuzione": lo Stato membro che intraprende o ha intrapreso l'azione richiesta in seguito a un riscontro positivo;

k) "utenti finali": le autorità competenti che interrogano direttamente il CS-SIS, l'N.SIS o una loro copia tecnica;

l) "dati dattiloscopici": dati relativi alle impronte digitali e alle impronte palmari che, per il loro carattere di unicità e i punti caratteristici che contengono, permettono confronti precisi e irrefutabili sull'identità di una persona;

m) "reati gravi": i reati di cui all'articolo 2, paragrafi 1 e 2, della decisione quadro 2002/584/GAI del 13 giugno 2002[71];

[71] 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).

n) "reati di terrorismo": i reati ai sensi del diritto nazionale di cui agli articoli da 1 a 4 della decisione quadro 2002/475/GAI del 13 giugno 2002[72].

Articolo 4
Architettura tecnica e modalità operative del SIS

1. Il SIS consta di:

(a) un sistema centrale ("SIS centrale") costituito da:

– un'unità di supporto tecnico ("CS-SIS") contenente una banca dati, la "banca dati del SIS",

– un'interfaccia nazionale uniforme ("NI-SIS");

(b) un sistema nazionale ("N.SIS") in ciascuno Stato membro, consistente nei sistemi di dati nazionali che comunicano con il SIS centrale. L'N.SIS contiene un archivio di dati ("copia nazionale"), contenente a sua volta una copia completa o parziale della banca dati del SIS e una copia di riserva dell' N.SIS. L'N.SIS e la sua copia di riserva possono essere usati simultaneamente per garantire agli utenti finali una disponibilità ininterrotta;

(c) un'infrastruttura di comunicazione fra il CS-SIS e l'NI-SIS ("infrastruttura di comunicazione") che fornisce una rete virtuale cifrata dedicata ai dati SIS e provvede allo scambio di informazioni tra gli uffici SIRENE ai sensi dell'articolo 7, paragrafo 2.

2. I dati SIS sono inseriti, aggiornati, cancellati e consultati attraverso i vari N.SIS. Una copia nazionale parziale o completa è disponibile ai fini dell'interrogazione automatizzata nel territorio di ciascuno degli Stati membri che la usano. La copia nazionale parziale contiene almeno i dati di cui all'articolo 20, paragrafo 2, relativi agli oggetti, e i dati di cui all'articolo 20, paragrafo 3, lettere da a) a v), relativi alle segnalazioni di persone. Non possono essere consultati gli archivi di dati contenuti nell'N.SIS degli altri Stati membri.

3. Il CS-SIS svolge funzioni di controllo tecnico e di amministrazione e dispone di una copia di riserva in grado di assicurare tutte le funzioni del CS-SIS principale in caso di guasto. Il CS-SIS e la sua copia di riserva sono ubicati nei due siti tecnici dell'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia istituita dal regolamento (UE) n. 1077/2011 ("l'agenzia")[73]. Il CS-SIS o la sua copia di riserva possono contenere una copia aggiuntiva della banca dati del SIS e possono essere usati simultaneamente in modalità attiva purché ognuno di essi sia in grado di elaborare tutte le operazioni relative a segnalazioni nel SIS.

---

72 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).

73 Istituita dal 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).

4. Il CS-SIS fornisce i servizi necessari per l'inserimento e il trattamento dei dati SIS, compresa la consultazione della banca dati del SIS. Il CS-SIS provvede a quanto segue:

a) l'aggiornamento in linea delle copie nazionali;

b) la sincronizzazione e la coerenza tra le copie nazionali e la banca dati del SIS;

c) le funzioni di inizializzazione e ripristino delle copie nazionali;

d) la disponibilità ininterrotta.

Articolo 5
Costi

1. I costi relativi all'esercizio, alla manutenzione e all'ulteriore sviluppo del SIS centrale e dell'infrastruttura di comunicazione sono a carico del bilancio generale dell'Unione europea.

2. Tali costi includono il lavoro effettuato con riguardo al CS-SIS per garantire la fornitura dei servizi di cui all'articolo 4, paragrafo 4.

3. I costi per l'istituzione, l'esercizio, la manutenzione e l'ulteriore sviluppo di ciascun N.SIS sono a carico dello Stato membro interessato.

CAPO II

COMPETENZE DEGLI STATI MEMBRI

Articolo 6
Sistemi nazionali

Ciascuno Stato membro è competente per l'istituzione, l'esercizio, la manutenzione e l'ulteriore sviluppo del proprio N.SIS e per il collegamento del proprio N.SIS all'NI.SIS.

Spetta a ciascuno Stato membro garantire il funzionamento continuo dell'N.SIS, il suo collegamento all'NI.SIS e la disponibilità ininterrotta dei dati SIS agli utenti finali.

Articolo 7
Ufficio N.SIS e ufficio SIRENE

1. Ciascuno Stato membro designa un'autorità ("ufficio N.SIS") che ha la competenza centrale per il rispettivo N.SIS.

Tale autorità è responsabile del corretto funzionamento e della sicurezza dell'N.SIS, garantisce l'accesso delle autorità competenti al SIS e adotta le misure atte a garantire l'osservanza delle disposizioni del presente regolamento. Ha il compito di

garantire che tutte le funzionalità del SIS siano messe adeguatamente a disposizione degli utenti finali.

Ciascuno Stato membro trasmette le proprie segnalazioni per il tramite del proprio ufficio N.SIS.

2. Ciascuno Stato membro designa l'autorità competente per lo scambio e la disponibilità di tutte le informazioni supplementari ("ufficio SIRENE") conformemente alle disposizioni del manuale SIRENE di cui all'articolo 8.

Gli uffici SIRENE coordinano inoltre la verifica della qualità delle informazioni inserite nel SIS. A tali fini, essi hanno accesso ai dati trattati nel SIS.

3. Gli Stati membri comunicano all'agenzia i rispettivi ufficio N.SIS e ufficio SIRENE. L'agenzia ne pubblica l'elenco insieme all'elenco di cui all'articolo 53, paragrafo 8.

Articolo 8
Scambio di informazioni supplementari

1. Le informazioni supplementari sono scambiate conformemente alle disposizioni del manuale SIRENE e per il tramite dell'infrastruttura di comunicazione. Gli Stati membri forniscono le risorse tecniche e umane necessarie per garantire in permanenza la disponibilità e lo scambio delle informazioni supplementari. In caso di indisponibilità dell'infrastruttura di comunicazione, gli Stati membri possono usare altri mezzi tecnici adeguatamente protetti per lo scambio di informazioni supplementari.

2. Le informazioni supplementari sono usate solo al fine per cui sono state trasmesse in conformità dell'articolo 61, a meno che sia stato ottenuto il previo consenso dello Stato membro segnalante.

3. Gli uffici SIRENE svolgono il loro compito in modo rapido ed efficiente, in particolare rispondendo a una richiesta appena possibile e comunque non oltre 12 ore dopo averla ricevuta.

4. Le modalità dettagliate di scambio delle informazioni supplementari sono adottate mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2, sotto forma di un manuale detto "manuale SIRENE".

Articolo 9
Conformità tecnica e funzionale

1. Per consentire una pronta ed efficiente trasmissione dei dati, all'atto dell'istituzione del rispettivo N.SIS ciascuno Stato membro si conforma alle norme, ai protocolli e alle procedure tecniche comuni stabiliti per assicurare la compatibilità del proprio N.SIS con il CS-SIS. Tali norme, protocolli e procedure tecniche comuni sono adottati mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

2. Gli Stati membri provvedono, tramite i servizi forniti dal CS-SIS, a che i dati memorizzati nella copia nazionale siano, grazie agli aggiornamenti automatici di cui all'articolo 4, paragrafo 4, identici e coerenti con quelli della banca dati del SIS e che un'interrogazione nella copia nazionale produca risultati equivalenti a quelli di un'interrogazione effettuata nella banca dati del SIS. Gli utenti finali ricevono i dati necessari allo svolgimento dei loro compiti, in particolare tutti i dati richiesti per identificare l'interessato e intraprendere le azioni necessarie.

Articolo 10
Sicurezza – Stati membri

1. Ciascuno Stato membro, in relazione al proprio N.SIS, adotta le misure necessarie, compresi un piano di sicurezza, un piano di continuità operativa e un piano di ripristino in caso di disastro, al fine di:

(a) proteggere fisicamente i dati, tra l'altro mediante l'elaborazione di piani d'emergenza per la protezione delle infrastrutture critiche;

(b) impedire alle persone non autorizzate l'accesso alle installazioni informatiche utilizzate per il trattamento dei dati personali (controllo all'ingresso delle installazioni);

(c) impedire che i supporti di dati siano letti, copiati, modificati o rimossi senza autorizzazione (controllo dei supporti di dati);

(d) impedire che i dati siano inseriti senza autorizzazione e che i dati personali memorizzati siano visionati, modificati o cancellati senza autorizzazione (controllo dell'archiviazione);

(e) impedire che persone non autorizzate usino sistemi automatizzati di trattamento dei dati mediante apparecchiature per la trasmissione di dati (controllo degli utenti);

(f) garantire che le persone autorizzate a usare un sistema automatizzato di trattamento dei dati possano accedere solo ai dati di loro competenza attraverso identità di utente individuali e uniche ed esclusivamente con modalità di accesso riservate (controllo dell'accesso ai dati);

(g) assicurare che tutte le autorità con diritto di accedere al SIS o alle installazioni di trattamento dei dati creino profili che descrivano i compiti e le funzioni delle persone autorizzate ad accedere, inserire, aggiornare, cancellare e consultare i dati e mettano senza indugio tali profili a disposizione delle autorità nazionali di controllo di cui all'articolo 66 a richiesta di queste (profili del personale);

(h) garantire la possibilità di verificare e accertare a quali organismi possano essere trasmessi dati personali mediante apparecchiature per la trasmissione di dati (controllo della trasmissione);

(i) garantire la possibilità di verificare e accertare a posteriori quali dati personali siano stati introdotti nei sistemi automatizzati di trattamento dei dati, il

momento dell'inserimento, la persona che lo ha effettuato e lo scopo dello stesso (controllo dell'inserimento);

(j) impedire, in particolare mediante tecniche appropriate di cifratura, che all'atto del trasferimento di dati personali nonché del trasporto di supporti di dati essi possano essere letti, copiati, modificati o cancellati senza autorizzazione (controllo del trasporto);

(k) controllare l'efficacia delle misure di sicurezza di cui al presente paragrafo e adottare le necessarie misure di carattere organizzativo relative al monitoraggio interno (autocontrollo).

2. Gli Stati membri adottano misure equivalenti a quelle del paragrafo 1 per quanto riguarda la sicurezza del trattamento e degli scambi di informazioni supplementari, fra l'altro garantendo la sicurezza dei locali dell'ufficio SIRENE.

3. Gli Stati membri adottano misure equivalenti a quelle del paragrafo 1 per quanto riguarda la sicurezza del trattamento dei dati SIS da parte delle autorità di cui all'articolo 43.

Articolo 11
Riservatezza – Stati membri

Ogni Stato membro applica le proprie norme nazionali in materia di segreto professionale o altri obblighi di riservatezza equivalenti a tutti i soggetti e organismi che debbano lavorare con i dati SIS e con le informazioni supplementari, conformemente alla propria legislazione nazionale. Tale obbligo vincola tali soggetti e organismi anche dopo che hanno rispettivamente lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

Articolo 12
Tenuta dei registri a livello nazionale

1. Gli Stati membri provvedono affinché ogni accesso ai dati personali e ogni scambio dei medesimi nell'ambito del CS-SIS sia registrato nei rispettivi N.SIS per verificare la legittimità dell'interrogazione, per controllare la liceità del trattamento dei dati, ai fini dell'autocontrollo e per garantire il corretto funzionamento dell'N.SIS, l'integrità e la sicurezza dei dati.

2. I registri riportano, in particolare, la cronistoria delle segnalazioni, la data e l'ora dell'attività di trattamento dei dati, i dati usati per effettuare un'interrogazione, un riferimento ai dati trasmessi e i nomi dell'autorità competente e del responsabile del trattamento dei dati.

3. Se l'interrogazione è effettuata con i dati dattiloscopici o l'immagine facciale in conformità degli articoli 40, 41 e 42, i registri riportano, in particolare, il tipo di dati usati per effettuare l'interrogazione, un riferimento al tipo di dati trasmessi e i nomi dell'autorità competente e del responsabile del trattamento dei dati.

4. I registri possono essere usati solo ai fini di cui al paragrafo 1 e sono cancellati al più presto un anno dopo e al più tardi tre anni dopo la loro creazione.

5. I registri possono essere tenuti più a lungo se sono necessari per procedure di controllo già in corso.

6. Le autorità nazionali competenti incaricate di verificare la legittimità dell'interrogazione, di controllare la liceità del trattamento dei dati, ai fini dell'autocontrollo e per garantire il corretto funzionamento dell'N.SIS, l'integrità e la sicurezza dei dati hanno accesso a tali registri, nei limiti delle rispettive competenze e su loro richiesta, ai fini dell'assolvimento dei loro compiti.

7. Gli Stati membri che effettuano interrogazioni automatizzate mediante scansione delle targhe di veicoli a motore, ricorrendo a sistemi di riconoscimento automatico delle targhe, tengono un registro aggiornato di tali interrogazioni conformemente alle rispettive legislazioni nazionali. Il contenuto di tale registro è stabilito mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2. Quando è riscontrata una corrispondenza con dati conservati nel SIS o in una copia nazionale o tecnica dei dati del SIS, è effettuata un'interrogazione completa nel SIS per verificare che la corrispondenza sia effettiva. Tale interrogazione completa è svolta secondo le disposizioni di cui ai paragrafi da 1 a 6.

Articolo 13
Autocontrollo

Gli Stati membri provvedono affinché ogni autorità con diritto di accesso ai dati SIS adotti le misure necessarie per conformarsi al presente regolamento e cooperi, se necessario, con l'autorità nazionale di controllo.

Articolo 14
Formazione del personale

Prima di essere autorizzato a trattare dati conservati nel SIS e periodicamente dopo che è stato accordato l'accesso ai dati SIS, il personale delle autorità con diritto di accesso al SIS riceve una formazione adeguata sulle norme in materia di sicurezza e protezione dei dati e sulle procedure di trattamento dei dati previste nel manuale SIRENE. Il personale è informato dei reati e delle sanzioni pertinenti.

CAPO III

COMPETENZE DELL'AGENZIA

Articolo 15
Gestione operativa

1. L'agenzia è responsabile della gestione operativa del SIS centrale. L'agenzia, in collaborazione con gli Stati membri, provvede affinché per il SIS centrale siano

utilizzate in ogni momento le migliori tecnologie disponibili, sulla base di un'analisi costi-benefici.

2. L'agenzia è inoltre responsabile dei seguenti compiti relativi all'infrastruttura di comunicazione:

   (a) controllo;

   (b) sicurezza;

   (c) coordinamento dei rapporti tra gli Stati membri e il gestore.

3. La Commissione è responsabile di tutti gli altri compiti connessi con l'infrastruttura di comunicazione, in particolare:

   (a) compiti relativi all'esecuzione del bilancio;

   (b) acquisizione e rinnovo;

   (c) aspetti contrattuali.

4. L'agenzia è responsabile dei seguenti compiti relativi agli uffici SIRENE e alla comunicazione tra gli uffici SIRENE:

   (a) coordinamento e gestione dei collaudi;

   (b) gestione e aggiornamento di specifiche tecniche per lo scambio di informazioni supplementari tra gli uffici SIRENE e l'infrastruttura di comunicazione, e gestione dell'effetto dei cambiamenti tecnici laddove riguardino sia il SIS che lo scambio di informazioni supplementari tra gli uffici SIRENE.

5. L'agenzia sviluppa e mantiene un meccanismo e procedure per lo svolgimento dei controlli di qualità sui dati contenuti nel CS-SIS e riferisce periodicamente agli Stati membri. L'agenzia riferisce periodicamente alla Commissione in merito ai problemi incontrati, dandone comunicazione anche agli Stati membri interessati. Il meccanismo, le procedure e l'interpretazione attinenti alla conformità qualitativa dei dati sono stabiliti mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

6. La gestione operativa del SIS centrale consiste nell'insieme dei compiti necessari al funzionamento 24 ore su 24 e 7 giorni su 7 del SIS centrale e comprende in particolare le attività di manutenzione e gli adattamenti tecnici necessari per il buon funzionamento del sistema. Tali compiti comprendono anche attività di collaudo che garantiscono che il SIS centrale e i sistemi nazionali operino secondo i requisiti tecnici e funzionali di cui all'articolo 9.

Articolo 16
Sicurezza

1. L'agenzia adotta le misure necessarie, compresi un piano di sicurezza, un piano di continuità operativa e un piano di ripristino in caso di disastro per il SIS centrale e l'infrastruttura di comunicazione, al fine di:

(a) proteggere fisicamente i dati, tra l'altro mediante l'elaborazione di piani d'emergenza per la protezione delle infrastrutture critiche;

(b) impedire alle persone non autorizzate l'accesso alle installazioni informatiche utilizzate per il trattamento dei dati personali (controllo all'ingresso delle installazioni);

(c) impedire che i supporti di dati siano letti, copiati, modificati o rimossi senza autorizzazione (controllo dei supporti di dati);

(d) impedire che i dati siano inseriti senza autorizzazione e che i dati personali memorizzati siano visionati, modificati o cancellati senza autorizzazione (controllo dell'archiviazione);

(e) impedire che persone non autorizzate usino sistemi automatizzati di trattamento dei dati mediante apparecchiature per la trasmissione di dati (controllo degli utenti);

(f) garantire che le persone autorizzate a usare un sistema automatizzato di trattamento dei dati possano accedere solo ai dati di loro competenza attraverso identità di utente individuali e uniche ed esclusivamente con modalità di accesso riservate (controllo dell'accesso ai dati);

(g) creare profili che descrivano i compiti e le funzioni delle persone autorizzate ad accedere ai dati o alle installazioni informatiche e mettere senza indugio tali profili a disposizione del garante europeo della protezione dei dati di cui all'articolo 64 a richiesta di quest'ultimo (profili del personale);

(h) garantire la possibilità di verificare e accertare a quali organismi possano essere trasmessi dati personali mediante apparecchiature per la trasmissione di dati (controllo della trasmissione);

(i) garantire la possibilità di verificare e accertare a posteriori quali dati personali siano stati introdotti nei sistemi automatizzati di trattamento dei dati, il momento dell'inserimento e la persona che lo ha effettuato (controllo dell'inserimento);

(j) impedire, in particolare mediante tecniche appropriate di cifratura, che all'atto del trasferimento di dati personali nonché del trasporto di supporti di dati essi possano essere letti, copiati, modificati o cancellati senza autorizzazione (controllo del trasporto);

(k) controllare l'efficacia delle misure di sicurezza di cui al presente paragrafo e adottare le necessarie misure di carattere organizzativo relative al controllo interno per garantire l'osservanza del presente regolamento (autocontrollo).

2. L'agenzia adotta misure equivalenti a quelle del paragrafo 1 per quanto riguarda la sicurezza dell'elaborazione e degli scambi di informazioni supplementari attraverso l'infrastruttura di comunicazione.

Articolo 17
Riservatezza – l'agenzia

1. Fatto salvo l'articolo 17 dello statuto dei funzionari dell'Unione europea e regime applicabile agli altri agenti dell'Unione, l'agenzia applica norme adeguate in materia di segreto professionale o altri obblighi di riservatezza equivalenti a tutti i membri del proprio personale che debbano lavorare con i dati SIS, secondo standard equiparabili a quelli previsti all'articolo 11 del presente regolamento. Tale obbligo vincola gli interessati anche dopo che hanno lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

2. L'agenzia adotta misure equivalenti a quelle di cui al paragrafo 1 per quanto riguarda la riservatezza degli scambi di informazioni supplementari attraverso l'infrastruttura di comunicazione.

Articolo 18
Tenuta dei registri a livello centrale

1. L'agenzia provvede affinché ogni accesso a dati personali e ogni scambio dei medesimi nell'ambito del CS-SIS siano registrati ai fini di cui all'articolo 12, paragrafo 1.

2. I registri riportano, in particolare, la cronistoria delle segnalazioni, la data e l'ora della trasmissione dei dati, il tipo di dati usati per effettuare interrogazioni, il riferimento al tipo di dati trasmessi e il nome dell'autorità competente responsabile del trattamento dei dati.

3. Se l'interrogazione è effettuata con i dati dattiloscopici o l'immagine facciale in conformità degli articoli 40, 41 e 42, i registri riportano, in particolare, il tipo di dati usati per effettuare l'interrogazione, un riferimento al tipo di dati trasmessi e i nomi dell'autorità competente e del responsabile del trattamento dei dati.

4. I registri possono essere usati solo ai fini di cui al paragrafo 1 e sono cancellati al più presto un anno dopo e al più tardi tre anni dopo la loro creazione. I registri contenenti la cronistoria delle segnalazioni sono cancellati da uno a tre anni dopo la cancellazione delle segnalazioni.

5. I registri possono essere tenuti più a lungo se necessari per procedure di controllo già in corso.

6. Le autorità competenti incaricate di verificare la legittimità dell'interrogazione, di controllare la liceità del trattamento dei dati, ai fini dell'autocontrollo e per garantire il corretto funzionamento del CS-SIS, l'integrità e la sicurezza dei dati hanno accesso a tali registri, nei limiti delle rispettive competenze e su loro richiesta, ai fini dell'assolvimento dei loro compiti.

CAPO IV

INFORMAZIONE DEL PUBBLICO

Articolo 19
Campagne d'informazione sul SIS

La Commissione, in collaborazione con le autorità nazionali di controllo e con il garante europeo della protezione dei dati, svolge periodicamente campagne per informare il pubblico sugli obiettivi del SIS, sui dati ivi conservati, sulle autorità che hanno accesso al SIS e sui diritti degli interessati. Gli Stati membri, in collaborazione con le rispettive autorità nazionali di controllo, definiscono e attuano le politiche necessarie per informare i propri cittadini sul SIS in generale.

CAPO V

CATEGORIE DI DATI E INDICATORI DI VALIDITÀ

Articolo 20
Categorie di dati

1. Fatti salvi l'articolo 8, paragrafo 1, o le disposizioni del presente regolamento che prevedono la memorizzazione di dati complementari, il SIS contiene esclusivamente le categorie di dati forniti da ciascuno Stato membro che sono necessari ai fini previsti agli articoli 26, 32, 34, 36 e 38.

2. Le categorie di dati sono le seguenti:

   (a) informazioni sulle persone segnalate;

   (b) informazioni sugli oggetti di cui agli articoli 32, 36 e 38.

3. Le informazioni sulle persone segnalate contengono esclusivamente i seguenti dati:

   (a) cognome/cognomi;

   (b) nome/nomi;

   (c) nome/nomi e cognome/cognomi alla nascita;

   (d) nomi e cognomi precedenti e "alias";

   (e) segni fisici particolari, oggettivi ed inalterabili;

   (f) luogo di nascita;

   (g) data di nascita;

(h) sesso;

(i) cittadinanza/cittadinanze;

(j) l'indicazione che la persona è armata, violenta, evasa o coinvolta in una delle attività di cui agli articoli 1, 2, 3 e 4 della decisione quadro 2002/475/GAI del Consiglio sulla lotta contro il terrorismo;

(k) ragione della segnalazione;

(l) autorità che effettua la segnalazione;

(m) riferimento alla decisione che ha dato origine alla segnalazione;

(n) azione da intraprendere;

(o) connessioni con altre segnalazioni già introdotte nel SIS a norma dell'articolo 53;

(p) tipo di reato per cui è stata effettuata la segnalazione;

(q) numero di registrazione della persona in un registro nazionale;

(r) categorizzazione del tipo di caso relativo a una persona scomparsa (solo per le segnalazioni di cui all'articolo 32);

(s) categoria del documento di identificazione;

(t) paese di rilascio del documento di identificazione;

(u) numero del documento di identificazione;

(v) data di rilascio del documento di identificazione;

(w) fotografie e immagini facciali;

(x) profili DNA conformemente all'articolo 22, paragrafo 1, lettera b);

(y) dati dattiloscopici;

(z) copia a colori del documento di identificazione.

4. Le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui ai paragrafi 2 e 3 sono stabilite e sviluppate mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

5. Le norme tecniche necessarie per l'interrogazione dei dati di cui al paragrafo 3 sono stabilite e sviluppate secondo la procedura di esame di cui all'articolo 72, paragrafo 2. Tali norme tecniche sono simili per le interrogazioni nel CS-SIS, nelle copie nazionali e nelle copie tecniche di cui all'articolo 53, paragrafo 2, e sono basate su norme comuni stabilite e sviluppate mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

Articolo 21
Proporzionalità

1. Prima di effettuare una segnalazione e al momento di prolungare il periodo di validità di una segnalazione, lo Stato membro verifica se l'adeguatezza, la pertinenza e l'importanza del caso giustificano l'inserimento della segnalazione nel SIS.

2. Quando una persona o un oggetto è ricercato da uno Stato membro in relazione a un reato che rientra nell'ambito di applicazione degli articoli da 1 a 4 della decisione quadro 2002/475/GAI del Consiglio sulla lotta contro il terrorismo, lo Stato membro effettua in ogni circostanza la corrispondente segnalazione a norma, a seconda dei casi, dell'articolo 34, 36 o 38.

Articolo 22
Norme specifiche per inserire fotografie, immagini facciali, dati dattiloscopici e profili DNA

1. L'inserimento nel SIS dei dati di cui all'articolo 20, paragrafo 3, lettere w), x) e y), è soggetto alle seguenti disposizioni:

   (a) fotografie, immagini facciali, dati dattiloscopici e profili DNA sono inseriti solo previo controllo di qualità volto ad accertare che soddisfino norme minime di qualità dei dati;

   (b) un profilo DNA può essere aggiunto solo alle segnalazioni di cui all'articolo 32, paragrafo 2, lettere a) e c), e solo se non sono disponibili per l'identificazione fotografie, immagini facciali o dati dattiloscopici. I profili DNA di persone che sono ascendenti diretti, discendenti o fratelli della persona oggetto della segnalazione possono essere aggiunti alla segnalazione solo con il consenso esplicito della persona interessata. L'origine razziale della persona non è inclusa nel profilo DNA.

2. Per la conservazione dei dati di cui al paragrafo 1, lettera a), e all'articolo 40 sono stabilite norme di qualità. Tali norme sono specificate mediante misure di esecuzione e aggiornate secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

Articolo 23
Requisito per inserire una segnalazione

1. Non possono essere inserite segnalazioni di persone in mancanza dei dati di cui all'articolo 20, paragrafo 3, lettere a), g), k), m), n) e, ove applicabile, p), tranne nelle situazioni di cui all'articolo 40.

2. Se disponibili, sono inseriti anche tutti gli altri dati di cui all'articolo 20, paragrafo 3.

Articolo 24
Disposizioni generali relative agli indicatori di validità

1. Lo Stato membro che reputa che dare applicazione a una segnalazione inserita a norma degli articoli 26, 32 o 36 non sia compatibile con la legislazione nazionale, con i propri obblighi internazionali o con interessi nazionali essenziali può esigere a

posteriori che alla segnalazione sia apposto un indicatore di validità affinché non sia eseguita sul proprio territorio l'azione richiesta nella segnalazione. L'indicatore di validità è apposto dall'ufficio SIRENE dello Stato membro segnalante.

2. Per consentire agli Stati membri di esigere l'apposizione di un indicatore di validità a una segnalazione effettuata a norma dell'articolo 26, tutti gli Stati membri sono automaticamente informati di ogni nuova segnalazione di questa categoria tramite scambio di informazioni supplementari.

3. Se per ragioni particolarmente gravi e urgenti lo Stato membro segnalante chiede l'esecuzione dell'azione, lo Stato membro di esecuzione esamina se può acconsentire al ritiro dell'indicatore di validità di cui ha richiesto l'apposizione. Se vi può acconsentire, lo Stato membro di esecuzione adotta le misure necessarie per far sì che l'azione richiesta possa essere eseguita immediatamente.

Articolo 25
Indicatori di validità relativi a segnalazioni per l'arresto a fini di consegna

1. Ove si applichi la decisione quadro 2002/584/GAI, l'indicatore di validità che impedisce l'arresto è apposto a una segnalazione per l'arresto a fini di consegna solo se l'autorità giudiziaria competente in virtù della legislazione nazionale per l'esecuzione del mandato d'arresto europeo ne ha rifiutato l'esecuzione in base a motivi di non esecuzione e se l'apposizione dell'indicatore di validità è stata richiesta.

2. Tuttavia, su richiesta di un'autorità giudiziaria competente in virtù della legislazione nazionale, in base a un'istruzione generale o in un caso specifico, l'apposizione di un indicatore di validità a una segnalazione per l'arresto a fini di consegna può essere richiesta anche se risulta evidente che l'esecuzione del mandato d'arresto europeo dovrà essere rifiutata.

CAPO VI

SEGNALAZIONE DI PERSONE RICERCATE PER L'ARRESTO A FINI DI CONSEGNA O DI ESTRADIZIONE

Articolo 26
Obiettivi e condizioni delle segnalazioni

1. I dati relativi a persone ricercate per l'arresto a fini di consegna sulla scorta di un mandato d'arresto europeo, ovvero per l'arresto a fini di estradizione, sono inseriti su richiesta dell'autorità giudiziaria dello Stato membro segnalante.

2. I dati relativi a persone ricercate per l'arresto a fini di consegna sono del pari inseriti sulla scorta di mandati d'arresto emessi in conformità degli accordi conclusi tra l'Unione e paesi terzi in virtù dell'articolo 37 del trattato sull'Unione europea ai fini della consegna di persone sulla base di un mandato d'arresto che prevedono la trasmissione di detto mandato d'arresto mediante il SIS.

3. Nel presente regolamento qualsiasi riferimento alle disposizioni della decisione quadro 2002/584/GAI si intende fatto altresì alle corrispondenti disposizioni degli accordi conclusi tra l'Unione europea e paesi terzi in virtù dell'articolo 37 del trattato sull'Unione europea ai fini della consegna di persone sulla base di un mandato d'arresto che prevedono che il mandato d'arresto sia trasmesso tramite il SIS.

4. In caso di operazione di ricerca in corso e previa autorizzazione dell'autorità giudiziaria competente dello Stato membro segnalante, quest'ultimo può rendere temporaneamente non consultabile una segnalazione per l'arresto effettuata a norma del presente articolo, cosicché la segnalazione non sia consultabile dagli utenti finali e sia accessibile solo agli uffici SIRENE. Tale funzionalità è attivata per un periodo non superiore a 48 ore. Se necessario a fini operativi, l'attivazione può tuttavia essere prolungata di ulteriori periodi di 48 ore. Gli Stati membri redigono statistiche sul numero di segnalazioni in cui è stata utilizzata tale funzionalità.

Articolo 27
Dati complementari su persone ricercate per l'arresto a fini di consegna

1. Nel caso di persone ricercate per l'arresto a fini di consegna sulla scorta di un mandato d'arresto europeo, lo Stato membro segnalante inserisce nel SIS una copia del mandato d'arresto europeo.

2. Lo Stato membro segnalante può inserire una copia della traduzione del mandato d'arresto europeo in una o più lingue ufficiali delle istituzioni dell'Unione europea.

Articolo 28
Informazioni supplementari su persone ricercate per l'arresto a fini di consegna

Lo Stato membro che ha inserito nel SIS la segnalazione per l'arresto a fini di consegna comunica le informazioni di cui all'articolo 8, paragrafo 1, della decisione quadro 2002/584/GAI agli altri Stati membri tramite scambio di informazioni supplementari.

Articolo 29
Informazioni supplementari su persone ricercate per l'arresto a fini di estradizione

1. Lo Stato membro che ha inserito nel SIS la segnalazione a fini di estradizione comunica agli altri Stati membri i dati seguenti tramite scambio di informazioni supplementari:

   (a) autorità da cui proviene la richiesta di arresto;

   (b) esistenza di un mandato d'arresto o di un documento avente la medesima valenza giuridica, o di una sentenza esecutiva;

   (c) natura e qualificazione giuridica del reato;

   (d) descrizione delle circostanze in cui il reato è stato commesso, compreso il momento, il luogo e il grado di partecipazione al reato della persona segnalata;

   (e) per quanto possibile, le conseguenze del reato;

(f) qualsiasi altra informazione utile o necessaria per l'esecuzione della segnalazione.

2. I dati di cui al paragrafo 1 non sono comunicati se i dati di cui agli articoli 27 o 28 sono già stati forniti e sono considerati sufficienti per l'esecuzione della segnalazione da parte dello Stato membro interessato.

Articolo 30
Conversione delle segnalazioni su persone ricercate per l'arresto a fini di consegna o di estradizione

Se non è possibile procedere a un arresto a causa del rifiuto opposto da uno Stato membro richiesto secondo le procedure relative agli indicatori di validità di cui agli articoli 24 o 25 o, nel caso di una segnalazione per l'arresto a fini di estradizione, in quanto l'indagine non è ancora stata conclusa, lo Stato membro richiesto considera la segnalazione una segnalazione effettuata per comunicare il luogo di soggiorno della persona interessata.

Articolo 31
Esecuzione dell'azione richiesta nella segnalazione di una persona ricercata per l'arresto a fini di consegna o estradizione

1. La segnalazione inserita nel SIS a norma dell'articolo 26 unitamente ai dati complementari di cui all'articolo 27 costituisce e ha lo stesso effetto di un mandato d'arresto europeo emesso a norma della decisione quadro 2002/584/GAI, ove si applichi tale decisione quadro.

2. Ove non si applichi la decisione quadro 2002/584/GAI, la segnalazione inserita nel SIS a norma degli articoli 26 e 29 ha la stessa valenza giuridica di una richiesta di arresto provvisorio a norma dell'articolo 16 della convenzione europea di estradizione del 13 dicembre 1957 o dell'articolo 15 del trattato di estradizione e di assistenza giudiziaria in materia penale tra il Regno del Belgio, il Granducato di Lussemburgo e il Regno dei Paesi Bassi, del 27 giugno 1962.

CAPO VII

SEGNALAZIONE DI PERSONE SCOMPARSE

Articolo 32
Obiettivi e condizioni delle segnalazioni

1. I dati relativi a persone scomparse o altre persone che devono essere poste sotto protezione o il cui luogo di soggiorno deve essere accertato sono inseriti nel SIS su richiesta dell'autorità competente dello Stato membro segnalante.

2. Possono essere inserite le seguenti categorie di persone scomparse:

(a) persone scomparse che devono essere poste sotto protezione:

i) ai fini della loro tutela;

ii) per prevenire minacce;

(b) persone scomparse che non devono essere poste sotto protezione;

(c) minori a rischio di sottrazione di cui al paragrafo 4.

3. Il paragrafo 2, lettera a), si applica specialmente ai minori e a persone che devono essere internate per decisione di un'autorità competente.

4. La segnalazione di un minore di cui al paragrafo 2, lettera c), è effettuata su richiesta dell'autorità giudiziaria competente dello Stato membro competente in materia di responsabilità genitoriale conformemente al regolamento (CE) n. 2201/2003 del Consiglio[74], in caso di rischio concreto ed evidente che un minore possa essere fatto uscire in modo illecito e imminente dallo Stato membro in cui ha sede l'autorità giudiziaria competente. Negli Stati membri che sono parte della convenzione dell'Aia, del 19 ottobre 1996, sulla competenza, la legge applicabile, il riconoscimento, l'esecuzione e la cooperazione in materia di responsabilità genitoriale e di misure di protezione dei minori e in cui non si applica il regolamento (CE) n. 2201/2003 del Consiglio, sono di applicazione le disposizioni della convenzione dell'Aia.

5. Gli Stati membri assicurano che i dati inseriti nel SIS indichino in quale delle categorie di cui al paragrafo 2 rientra la persona scomparsa. Gli Stati membri assicurano inoltre che i dati inseriti nel SIS indichino il tipo di caso di persona scomparsa o vulnerabile. Le norme sulla categorizzazione dei tipi di caso e sull'inserimento di tali dati sono stabilite e sviluppate mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

6. Quattro mesi prima che il minore oggetto di segnalazione ai sensi del presente articolo raggiunga l'età adulta, il CS-SIS comunica automaticamente allo Stato membro segnalante che la ragione della richiesta e l'azione da intraprendere devono essere aggiornate o che la segnalazione dev'essere cancellata.

7. Qualora esistano indizi concreti che veicoli, natanti o aeromobili siano collegati a una persona oggetto di segnalazione a norma del paragrafo 2, possono essere effettuate segnalazioni di tali veicoli, natanti o aeromobili per localizzare la persona. In tal caso la segnalazione della persona scomparsa e la segnalazione dell'oggetto sono connesse in conformità dell'articolo 60. Le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al presente paragrafo sono stabilite mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

---

[74] Regolamento (CE) n. 2201/2003 del Consiglio, del 27 novembre 2003, relativo alla competenza, al riconoscimento e all'esecuzione delle decisioni in materia matrimoniale e in materia di responsabilità genitoriale, che abroga il regolamento (CE) n. 1347/2000 (GU L 338 del 23.12.2003, pag. 1).

Articolo 33
Esecuzione dell'azione richiesta nella segnalazione

1. In caso di reperimento di una persona di cui all'articolo 32, le autorità competenti comunicano, fatto salvo il paragrafo 2, il suo luogo di soggiorno allo Stato membro segnalante. In caso di minori scomparsi o minori che devono essere posti sotto protezione, lo Stato membro di esecuzione consulta immediatamente lo Stato membro segnalante per concordare senza indugio le misure da prendere per tutelare l'interesse superiore del minore. Nei casi di cui all'articolo 32, paragrafo 2, lettere a) e c), le autorità competenti possono, qualora la legislazione nazionale lo consenta, porre la persona sotto protezione per impedirle di proseguire il viaggio.

2. La comunicazione, diversa da quella fra le autorità competenti, dei dati relativi a una persona scomparsa maggiorenne che sia stata reperita è subordinata al consenso della persona in questione. Tuttavia, le autorità competenti possono comunicare la cancellazione della segnalazione, dovuta al reperimento della persona scomparsa, alla persona che ne ha segnalato la scomparsa.

CAPO VIII

SEGNALAZIONE DI PERSONE RICERCATE PER PRESENZIARE AD UN PROCEDIMENTO GIUDIZIARIO

Articolo 34
Obiettivi e condizioni delle segnalazioni

1. Ai fini della comunicazione della residenza o del domicilio di una persona, gli Stati membri inseriscono nel SIS, su richiesta dell'autorità competente, i dati relativi a:

   (a) testimoni;

   (b) persone citate a comparire o persone ricercate affinché si presentino dinanzi all'autorità giudiziaria nell'ambito di un procedimento penale per rispondere di fatti che sono loro ascritti;

   (c) persone alle quali deve essere notificata una sentenza penale o altri documenti connessi con un procedimento penale per rispondere di fatti che sono stati loro ascritti;

   (d) persone alle quali deve essere notificata una richiesta di presentarsi per scontare una pena privativa della libertà.

2. Qualora esistano indizi concreti che veicoli, natanti o aeromobili siano collegati a una persona oggetto di segnalazione a norma del paragrafo 1, possono essere effettuate segnalazioni di tali veicoli, natanti o aeromobili per localizzare la persona. In tal caso la segnalazione della persona scomparsa e la segnalazione dell'oggetto sono connesse in conformità dell'articolo 60. Le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al

presente paragrafo sono stabilite mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

Articolo 35
Esecuzione dell'azione richiesta nella segnalazione

Le informazioni richieste sono comunicate allo Stato membro richiedente tramite scambio di informazioni supplementari.

CAPO IX

SEGNALAZIONE DI PERSONE E OGGETTI AI FINI DI CONTROLLI DISCRETI, CONTROLLI DI INDAGINE O CONTROLLI SPECIFICI

Articolo 36
Obiettivi e condizioni delle segnalazioni

1. I dati relativi a persone o a veicoli, natanti, aeromobili e container sono inseriti, nel rispetto della legislazione nazionale dello Stato membro segnalante, ai fini di controlli discreti, controlli di indagine o controlli specifici a norma dell'articolo 37, paragrafo 4.

2. Può essere effettuata una segnalazione ai fini della repressione di reati, dell'esecuzione di condanne penali e per prevenire minacce alla sicurezza pubblica:

   (a) qualora esistano indizi concreti che la persona intenda commettere o commetta un reato grave, quali i reati di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI;

   (b) qualora le informazioni di cui all'articolo 37, paragrafo 1, siano necessarie all'esecuzione di una condanna penale per un reato grave, in particolare uno dei reati di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI; o

   (c) qualora la valutazione globale della persona, in particolare sulla base dei suoi precedenti penali, faccia supporre che commetterà anche in avvenire reati gravi, in particolare reati di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI.

3. Inoltre una segnalazione può essere effettuata conformemente alla legislazione nazionale, su richiesta delle autorità competenti per la sicurezza nazionale, qualora esistano indizi concreti che le informazioni di cui all'articolo 37, paragrafo 1, sono necessarie per prevenire una minaccia grave proveniente dalla persona interessata o altre minacce gravi per la sicurezza interna o esterna. Lo Stato membro che effettua la segnalazione a norma del presente paragrafo ne informa gli altri Stati membri. Ciascuno Stato membro stabilisce a quali autorità sono trasmesse tali informazioni.

4. Qualora esistano indizi concreti che veicoli, natanti, aeromobili e container siano collegati a reati gravi di cui al paragrafo 2 o a gravi minacce di cui al paragrafo 3, possono essere effettuate segnalazioni di tali veicoli, natanti, aeromobili e container.

5. Qualora esistano indizi concreti che documenti vergini o documenti di identità rilasciati siano collegati a reati gravi di cui al paragrafo 2 o a gravi minacce di cui al paragrafo 3, possono essere effettuate segnalazioni di tali documenti, a prescindere dall'identità dell'eventuale titolare originario del documento di identità. Le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al presente paragrafo sono stabilite e sviluppate mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

Articolo 37
Esecuzione dell'azione richiesta nella segnalazione

1. Nell'ambito dei controlli discreti, dei controlli di indagine o dei controlli specifici, le seguenti informazioni sono raccolte e trasmesse, totalmente o in parte, all'autorità segnalante in occasione di verifiche di frontiera, controlli di polizia o doganali o altre attività di contrasto svolte all'interno di uno Stato membro:

   (a) il fatto che siano stati localizzati la persona, il veicolo, il natante, l'aeromobile, il container, il documento vergine o il documento di identità rilasciato segnalati;

   (b) il luogo, l'ora e il motivo del controllo;

   (c) l'itinerario e la destinazione del viaggio;

   (d) le persone che accompagnano la persona interessata o gli occupanti del veicolo, del natante o dell'aeromobile o le persone che accompagnano il possessore del documento vergine o del documento di identità rilasciato, di cui si può ragionevolmente presumere che siano associati alla persona interessata;

   (e) l'identità rivelata e la descrizione personale della persona che usa il documento vergine o il documento di identità rilasciato oggetto della segnalazione;

   (f) il veicolo, il natante, l'aeromobile o il container usato;

   (g) gli oggetti trasportati, compresi i documenti di viaggio;

   (h) le circostanze in cui sono stati localizzati la persona o il veicolo, il natante, l'aeromobile, il container, il documento vergine o il documento di identità rilasciato.

2. Le informazioni di cui al paragrafo 1 sono comunicate tramite scambio di informazioni supplementari.

3. A seconda delle circostanze operative e conformemente alla legislazione nazionale, il controllo discreto comprende il regolare controllo di una persona o di un oggetto al

fine di raccogliere il maggior numero possibile di informazioni di cui al paragrafo 1 senza compromettere la natura discreta del controllo.

4. A seconda delle circostanze operative e conformemente alla legislazione nazionale, il controllo di indagine consiste in un controllo più approfondito e in un interrogatorio della persona. Se la legge di uno Stato membro non lo autorizza, il controllo di indagine è convertito, per quello Stato membro, in controllo discreto.

5. Nell'ambito dei controlli specifici, le persone, i veicoli, i natanti, gli aeromobili, i container e gli oggetti trasportati possono essere perquisiti conformemente alla legislazione nazionale ai fini di cui all'articolo 36. Le perquisizioni sono svolte conformemente alla legislazione nazionale. Se la legge di uno Stato membro non lo autorizza, il controllo specifico è convertito, per quello Stato membro, in controllo di indagine.

CAPO X

SEGNALAZIONE DI OGGETTI A FINI DI SEQUESTRO O DI PROVA IN UN PROCEDIMENTO PENALE

Articolo 38
Obiettivi e condizioni delle segnalazioni

1. I dati relativi agli oggetti ricercati a scopo di sequestro a fini di contrasto o di prova in un procedimento penale sono inseriti nel SIS.

2. Sono inserite le categorie di oggetti agevolmente identificabili indicate in appresso:

   (a) veicoli a motore, quali definiti dalla legislazione nazionale, a prescindere dal sistema di propulsione;

   (b) rimorchi di peso a vuoto superiore a 750 kg;

   (c) roulotte;

   (d) apparecchiature industriali;

   (e) natanti;

   (f) motori per natanti;

   (g) container;

   (h) aeromobili;

   (i) armi da fuoco;

   (j) documenti vergini rubati, altrimenti sottratti o smarriti;

(k) documenti di identità rilasciati, quali passaporti, carte d'identità, patenti di guida, titoli di soggiorno e documenti di viaggio rubati, altrimenti sottratti, smarriti o invalidati, o documenti pretesi tali ma falsificati;

(l) carte di circolazione per veicoli e targhe per veicoli rubate, altrimenti sottratte, smarrite o invalidate, o documenti pretesi tali ma falsificati;

(m) banconote (banconote registrate) e banconote falsificate;

(n) apparecchiature tecniche, prodotti informatici e altri oggetti di elevato valore facilmente identificabili;

(o) componenti identificabili di veicoli a motore;

(p) componenti identificabili di macchinari industriali.

3. La definizione di nuove sottocategorie di oggetti di cui al paragrafo 2, lettera n), e le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al paragrafo 2 sono stabilite e sviluppate mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

Articolo 39
Esecuzione dell'azione richiesta nella segnalazione

1. Qualora dall'interrogazione emerga l'esistenza di una segnalazione relativa a un oggetto reperito, l'autorità che la constata sequestra l'oggetto conformemente alla legislazione nazionale e si mette in contatto con l'autorità segnalante per concordare le misure necessarie. A tale scopo possono altresì essere trasmessi dati personali a norma del presente regolamento.

2. Le informazioni di cui al paragrafo 1 sono comunicate tramite scambio di informazioni supplementari.

3. Lo Stato membro che ha reperito l'oggetto adotta le misure richieste conformemente alla legislazione nazionale.

CAPO XI

SEGNALAZIONE DI IGNOTI RICERCATI A FINI DI IDENTIFICAZIONE IN CONFORMITÀ DELLA LEGISLAZIONE NAZIONALE E INTERROGAZIONE CON DATI BIOMETRICI

Articolo 40
Segnalazione di ignoti ricercati a fini di fermo in conformità della legislazione nazionale

Possono essere inseriti nel SIS dati dattiloscopici non collegati a persone segnalate. Tali dati dattiloscopici sono serie complete o incomplete di impronte digitali o impronte palmari

rinvenute sul luogo di un reato oggetto di indagine, un reato grave o un reato di terrorismo, qualora si possa stabilire con un elevato grado di probabilità che appartengono all'autore del reato. I dati dattiloscopici appartenenti a questa categoria sono conservati come relativi a "ignoto sospettato o ricercato", a condizione che le autorità competenti non possano stabilire l'identità della persona ricorrendo a un'altra banca dati nazionale, europea o internazionale.

Articolo 41
Esecuzione dell'azione richiesta nella segnalazione

In caso di riscontro positivo o potenziale corrispondenza con i dati conservati a norma dell'articolo 40, l'identità della persona è stabilita conformemente alla legislazione nazionale, contestualmente alla verifica che i dati dattiloscopici conservati nel SIS appartengano a tale persona. Gli Stati membri comunicano tramite scambio di informazioni supplementari per agevolare una tempestiva indagine del caso.

Articolo 42
Norme specifiche per la verifica o l'interrogazione con fotografie, immagini facciali, dati dattiloscopici e profili DNA

1. Fotografie, immagini facciali, dati dattiloscopici e profili DNA sono estratti dal SIS per verificare l'identità di una persona reperita grazie all'interrogazione del SIS con dati alfanumerici.

2. I dati dattiloscopici possono essere usati anche per identificare una persona. I dati dattiloscopici conservati nel SIS sono interrogati a fini di identificazione se l'identità della persona non può essere accertata con altri mezzi.

3. I dati dattiloscopici conservati nel SIS in relazione a segnalazioni effettuate a norma dell'articolo 26, dell'articolo 34, paragrafo 1, lettere b) e d), e dell'articolo 36 possono essere interrogati anche usando serie complete o incomplete di impronte digitali o palmari rinvenute sul luogo di un reato oggetto di indagine, qualora si possa stabilire con un elevato grado di probabilità che appartengono all'autore del reato e purché le autorità competenti non siano in grado di stabilire l'identità della persona ricorrendo a un'altra banca dati nazionale, europea o internazionale.

4. Non appena ciò diviene tecnicamente possibile, e garantendo al contempo un grado elevato di affidabilità dell'identificazione, è possibile ricorrere a fotografie e immagini facciali per identificare una persona. L'identificazione mediante fotografie o immagini facciali è effettuata solo presso valichi di frontiera regolari dove sono usati sistemi self-service e sistemi di controllo di frontiera automatizzati.

CAPO XII

DIRITTO DI ACCESSO E CONSERVAZIONE DELLE SEGNALAZIONI

Articolo 43
Autorità con diritto di accesso alle segnalazioni

1. L'accesso ai dati inseriti nel SIS e il diritto di consultarli direttamente o su una copia di dati del SIS sono riservati alle autorità responsabili:

   (a) dei controlli di frontiera, a norma del regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio, del 9 marzo 2016, che istituisce un codice unionale relativo al regime di attraversamento delle frontiere da parte delle persone (codice frontiere Schengen);

   (b) dei controlli di polizia e doganali effettuati all'interno dello Stato membro interessato e del relativo coordinamento da parte delle autorità designate;

   (c) di altre attività di contrasto svolte a fini di prevenzione, accertamento e indagine di reati nello Stato membro interessato;

   (d) dell'esame delle condizioni e dell'adozione di decisioni in materia di ingresso e soggiorno di cittadini di paesi terzi sul territorio degli Stati membri, compresi i permessi di soggiorno e i visti per soggiorni di lunga durata, e in materia di rimpatrio di cittadini di paesi terzi.

2. Il diritto di accesso ai dati inseriti nel SIS e il diritto di consultarli direttamente possono essere esercitati anche dalle autorità giudiziarie nazionali, comprese quelle competenti per l'avvio dell'azione penale e per le indagini giudiziarie prima dell'imputazione, nell'assolvimento delle loro funzioni, come previsto nella legislazione nazionale, e dalle relative autorità di coordinamento.

3. Il diritto di accesso ai dati inseriti nel SIS e il diritto di consultarli direttamente possono essere esercitati dalle autorità competenti per l'adempimento dei compiti di cui al paragrafo 1, lettera c), nello svolgimento delle loro funzioni. L'accesso da parte di tali autorità è disciplinato dalla legislazione di ciascuno Stato membro.

4. Le autorità di cui al presente articolo sono inserite nell'elenco di cui all'articolo 53, paragrafo 8.

Articolo 44
Autorità preposte all'immatricolazione dei veicoli

1. I servizi competenti negli Stati membri per il rilascio delle carte di circolazione dei veicoli ai sensi della direttiva 1999/37/CE del Consiglio[75] hanno accesso ai seguenti dati inseriti nel SIS a norma dell'articolo 38, paragrafo 2, lettere a), b), c) e l), del presente regolamento, al solo scopo di verificare che i veicoli di cui è richiesta l'immatricolazione non siano stati rubati, altrimenti sottratti o smarriti o non siano ricercati a fini di prova in un procedimento penale:

   (a) dati relativi a veicoli a motore, quali definiti dalla legislazione nazionale, a prescindere dal sistema di propulsione;

   (b) dati relativi ai rimorchi di peso a vuoto superiore a 750 kg e alle roulotte;

   (c) dati relativi a carte di circolazione per veicoli e a targhe per veicoli rubati, altrimenti sottratti, smarriti o invalidati.

   L'accesso a tali dati da parte dei servizi competenti per il rilascio delle carte di circolazione dei veicoli è disciplinato dalla legislazione nazionale dello Stato membro in questione.

2. I servizi di cui al paragrafo 1 che sono servizi pubblici hanno il diritto di consultare direttamente i dati inseriti nel SIS.

3. I servizi di cui al paragrafo 1 che non sono servizi pubblici accedono ai dati inseriti nel SIS soltanto per il tramite di un'autorità di cui all'articolo 43. Tale autorità ha il diritto di consultare tali dati direttamente e di trasmetterli al servizio competente. Lo Stato membro interessato provvede affinché il servizio in questione e il suo personale siano tenuti al rispetto di tutte le restrizioni sull'uso consentito dei dati trasmessi loro da detta autorità.

4. L'articolo 39 del presente regolamento non si applica all'accesso ottenuto a norma del presente articolo. La comunicazione alle autorità giudiziarie o di polizia, ad opera dei servizi di cui al paragrafo 1, di informazioni emerse durante la consultazione del SIS che diano motivo di sospettare che sia stato commesso un reato è disciplinata dalla legislazione nazionale.

Articolo 45
Autorità preposte all'immatricolazione di natanti e aeromobili

1. I servizi competenti negli Stati membri per il rilascio dei certificati d'immatricolazione o per la gestione del traffico di natanti, compresi i relativi motori, e di aeromobili hanno accesso ai seguenti dati inseriti nel SIS a norma dell'articolo 38, paragrafo 2, al solo scopo di verificare che i natanti, compresi i relativi motori, gli aeromobili o i container di cui è richiesta l'immatricolazione o che

[75] Direttiva 1999/37/CE del Consiglio, del 29 aprile 1999, relativa ai documenti di immatricolazione dei veicoli (GU L 138 dell'1.6.1999, pag. 57).

sono oggetto della gestione del traffico non siano stati rubati, altrimenti sottratti o smarriti o non siano ricercati a fini di prova in un procedimento penale:

(a) dati relativi a natanti;

(b) dati relativi a motori per natanti;

(c) dati relativi ad aeromobili.

Fatto salvo il paragrafo 2, la legge di ciascuno Stato membro disciplina l'accesso dei servizi di quello Stato membro a tali dati. L'accesso ai dati di cui alle lettere da a) a c) è limitato alle specifiche competenze dei servizi interessati.

2. I servizi di cui al paragrafo 1 che sono servizi pubblici hanno il diritto di consultare direttamente i dati inseriti nel SIS.

3. I servizi di cui al paragrafo 1 che non sono servizi pubblici accedono ai dati inseriti nel SIS soltanto per il tramite di un'autorità di cui all'articolo 43. Tale autorità ha il diritto di consultare i dati direttamente e di trasmetterli al servizio competente. Lo Stato membro interessato provvede affinché il servizio in questione e il suo personale siano tenuti al rispetto di tutte le restrizioni sull'uso consentito dei dati trasmessi loro da detta autorità.

4. L'articolo 39 del presente regolamento non si applica all'accesso ottenuto a norma del presente articolo. La comunicazione alle autorità giudiziarie o di polizia, ad opera dei servizi di cui al paragrafo 1, di informazioni emerse durante la consultazione del SIS che diano motivo di sospettare che sia stato commesso un reato è disciplinata dalla legislazione nazionale.

Articolo 46
Accesso di Europol ai dati SIS

1. L'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), nell'ambito del suo mandato, ha il diritto di accedere ai dati inseriti nel SIS e di consultarli.

2. Qualora un'interrogazione effettuata da Europol riveli la presenza di una segnalazione nel SIS, Europol, tramite i canali definiti dal regolamento (UE) 2016/794, informa al riguardo lo Stato membro segnalante.

3. L'uso delle informazioni ottenute tramite un'interrogazione nel SIS è soggetto al consenso dello Stato membro interessato. Se lo Stato membro acconsente all'uso di tali informazioni, il loro trattamento da parte di Europol è disciplinato dal regolamento (UE) 2016/794. Le informazioni sono trasmesse da Europol a paesi terzi e organismi terzi solo con il consenso dello Stato membro interessato.

4. Europol può chiedere ulteriori informazioni allo Stato membro interessato conformemente a quanto previsto dal regolamento (UE) 2016/794.

5. Europol:

(a) fatti salvi i paragrafi 3, 4 e 6, non collega parti del SIS, né trasferisce i dati in esso contenuti cui ha accesso, a sistemi informatici di raccolta e trattamento di dati gestiti da o presso di essa e non scarica o copia altrimenti parti del SIS;

(b) limita l'accesso ai dati inseriti nel SIS al proprio personale specificamente autorizzato;

(c) adotta e applica le misure di cui agli articoli 10 e 11;

(d) consente al garante europeo della protezione dei dati di esaminare le attività da essa svolte nell'esercizio del suo diritto di accesso ai dati inseriti nel SIS e di consultazione degli stessi.

6. I dati possono essere duplicati soltanto per fini tecnici, sempreché tale operazione sia necessaria per la consultazione diretta da parte di personale di Europol debitamente autorizzato. Le disposizioni del presente regolamento si applicano a tali copie. La copia tecnica è usata al fine di conservare i dati SIS mentre tali dati sono consultati. Una volta consultati i dati, la copia è cancellata. Tali usi non sono considerati scaricamento o duplicazione illeciti di dati SIS. Europol non copia in altri suoi sistemi dati relativi a una segnalazione né dati complementari trasmessi dagli Stati membri o dal CS-SIS.

7. Le copie di cui al paragrafo 6 che portano alla creazione di banche dati off-line possono essere conservate per un periodo non superiore a 48 ore. Tale periodo può essere prolungato in caso di emergenza, finché l'emergenza non sia cessata. Europol riferisce tali casi di prolungamento al garante europeo della protezione dei dati.

8. Europol può ricevere e trattare informazioni supplementari su segnalazioni corrispondenti nel SIS purché siano applicate, ove appropriato, le norme sul trattamento dei dati di cui ai paragrafi da 2 a 7.

9. Per verificare la liceità del trattamento dei dati, per l'autocontrollo e per garantire un'adeguata sicurezza e integrità dei dati, Europol conserva un registro di tutti gli accessi al SIS e le interrogazioni del SIS. Tali registri e tale documentazione non sono considerati scaricamenti o duplicazioni illeciti di parti del SIS.

Articolo 47
Accesso di Eurojust ai dati SIS

1. I membri nazionali di Eurojust e i loro assistenti, nell'ambito del loro mandato, hanno il diritto di accedere ai dati inseriti nel SIS e di consultarli a norma degli articoli 26, 32, 34, 38 e 40.

2. Qualora un'interrogazione effettuata da un membro nazionale di Eurojust riveli la presenza di una segnalazione nel SIS, il membro nazionale informa al riguardo lo Stato membro segnalante.

3. Il presente articolo non pregiudica in alcun modo le disposizioni della decisione 2002/187/GAI concernenti la protezione dei dati e la responsabilità in caso di trattamento di dati non autorizzato o scorretto da parte dei membri nazionali di

Eurojust o dei loro assistenti, né le competenze dell'autorità di controllo comune istituita a norma di detta decisione.

4. Ogni accesso e consultazione effettuati da un membro nazionale di Eurojust o da un suo assistente sono registrati conformemente all'articolo 12 e ogni uso dei dati ai quali hanno avuto accesso è registrato.

5. Nessuna parte del SIS è collegata a un sistema informatico di raccolta e trattamento di dati gestito da o presso Eurojust e nessun dato contenuto nel SIS a cui hanno accesso i membri nazionali o i loro assistenti può essere trasferito a tale sistema informatico. Nessuna parte del SIS può essere scaricata. La registrazione degli accessi e delle interrogazioni non è considerata scaricamento o duplicazione illeciti di dati SIS.

6. L'accesso ai dati inseriti nel SIS è limitato ai membri nazionali e ai loro assistenti e non si estende al personale di Eurojust.

7. Sono adottate e applicate le misure per garantire sicurezza e riservatezza di cui agli articoli 10 e 11.

Articolo 48

Accesso ai dati SIS da parte delle squadre della guardia di frontiera e costiera europea, di squadre di personale che assolve compiti attinenti al rimpatrio e dei membri delle squadre di sostegno per la gestione della migrazione

1. In conformità dell'articolo 40, paragrafo 8, del regolamento (UE) 2016/1624, i membri delle squadre della guardia di frontiera e costiera europea o di squadre di personale che assolve compiti attinenti al rimpatrio e i membri delle squadre di sostegno per la gestione delle migrazione hanno, nell'ambito dei rispettivi mandati, il diritto di accedere ai dati inseriti nel SIS e di consultarli.

2. I membri delle squadre della guardia di frontiera e costiera europea o di squadre di personale che assolve compiti attinenti al rimpatrio e i membri delle squadre di sostegno per la gestione delle migrazione accedono ai dati inseriti nel SIS e li consultano in conformità del paragrafo 1 tramite l'interfaccia tecnica istituita e mantenuta dall'Agenzia europea della guardia di frontiera e costiera a norma dell'articolo 49, paragrafo 1.

3. Qualora un'interrogazione effettuata da un membro delle squadre della guardia di frontiera e costiera europea o di squadre di personale che assolve compiti attinenti al rimpatrio o delle squadre di sostegno per la gestione della migrazione riveli l'esistenza di una segnalazione nel SIS, lo Stato membro segnalante ne è informato. In conformità dell'articolo 40 del regolamento (UE) 2016/1624, i membri delle squadre possono intervenire esclusivamente in risposta a una segnalazione nel SIS sotto il controllo e, di norma, in presenza di guardie di frontiera o di personale che assolve compiti attinenti al rimpatrio dello Stato membro ospitante in cui operano. Lo Stato membro ospitante può autorizzare i membri delle squadre ad agire per suo conto.

4. Ogni richiesta di accesso e ogni interrogazione effettuata da un membro delle squadre della guardia di frontiera e costiera europea o di squadre di personale che

assolve compiti attinenti al rimpatrio o delle squadre di sostegno per la gestione della migrazione è registrata secondo le disposizioni dell'articolo 12 e ogni uso dei dati a cui ha avuto accesso è registrato.

5. L'accesso ai dati inseriti nel SIS è limitato a un membro delle squadre della guardia di frontiera e costiera europea o di squadre di personale che assolve compiti attinenti al rimpatrio o delle squadre di sostegno per la gestione della migrazione e non è esteso ad altri membri della squadra.

6. Sono adottate e applicate le misure per garantire sicurezza e riservatezza di cui agli articoli 10 e 11.

Articolo 49
Accesso ai dati SIS da parte dell'Agenzia europea della guardia di frontiera e costiera

1. Ai fini dell'articolo 48, paragrafo 1, e del paragrafo 2 del presente articolo, l'Agenzia europea della guardia di frontiera e costiera istituisce e mantiene un'interfaccia tecnica che permette un collegamento diretto con il SIS centrale.

2. L'Agenzia europea della guardia di frontiera e costiera, ai fini dell'adempimento dei compiti conferitile dal regolamento che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), ha il diritto di accedere ai dati inseriti nel SIS e di consultarli in conformità degli articoli 26, 32, 34, 36 e dell'articolo 38, paragrafo 2, lettere j) e k).

3. Qualora una verifica svolta dall'Agenzia europea della guardia di frontiera e costiera riveli l'esistenza di una segnalazione nel SIS, si applica la procedura di cui all'articolo 22 del regolamento che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS).

4. Il presente articolo non pregiudica in alcun modo le disposizioni del regolamento (UE) 2016/1624 concernenti la protezione dei dati né la responsabilità per trattamenti non autorizzati o scorretti di tali dati da parte dell'Agenzia europea della guardia di frontiera e costiera.

5. Ogni richiesta di accesso e ogni interrogazione effettuata dall'Agenzia europea della guardia di frontiera e costiera è registrata secondo le disposizioni dell'articolo 12 e ogni uso dei dati a cui ha avuto accesso è registrato.

6. Tranne quando necessario per adempiere le funzioni richieste dal regolamento che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), nessuna parte del SIS è collegata a un sistema informatico di raccolta e trattamento di dati gestito da o presso l'Agenzia europea della guardia di frontiera e costiera, e nessun dato contenuto nel SIS a cui ha accesso l'Agenzia europea della guardia di frontiera e costiera è trasferito a tale sistema. Nessuna parte del SIS può essere scaricata. La registrazione degli accessi e delle interrogazioni non è considerata scaricamento o duplicazione di dati SIS.

7. L'Agenzia europea della guardia di frontiera e costiera adotta e applica le misure per garantire sicurezza e riservatezza di cui agli articoli 10 e 11.

Articolo 50
Limiti dell'accesso

Gli utenti finali, compresa Europol, i membri nazionali di Eurojust e i loro assistenti e l'Agenzia europea della guardia di frontiera e costiera possono accedere solo ai dati necessari per l'assolvimento dei loro compiti.

Articolo 51
Termini di conservazione delle segnalazioni

1. Le segnalazioni inserite nel SIS a norma del presente regolamento sono conservate esclusivamente per il periodo necessario a realizzare gli obiettivi per i quali sono state inserite.

2. Lo Stato membro che ha effettuato una segnalazione riesamina la necessità di conservarla nel SIS entro cinque anni dall'inserimento nello stesso. Le segnalazioni effettuate ai fini dell'articolo 36 sono conservate al massimo per un anno.

3. Le segnalazioni relative a documenti vergini e documenti di identità rilasciati inserite a norma dell'articolo 38 sono conservate al massimo per dieci anni. Periodi di conservazione più brevi per le categorie di segnalazioni relative a oggetti possono essere stabiliti mediante misure di esecuzione secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

4. Ciascuno Stato membro fissa, se del caso, tempi di riesame più brevi conformemente alla legislazione nazionale.

5. Qualora risulti chiaro al personale dell'ufficio SIRENE responsabile di coordinare e verificare la qualità dei dati che una segnalazione su una persona ha conseguito il suo obiettivo e dev'essere cancellata dal SIS, il personale lo comunica all'autorità segnalante per sottoporre la questione alla sua attenzione. L'autorità dispone di 30 giorni di calendario dal ricevimento di tale comunicazione per indicare che la segnalazione è stata o sarà cancellata, oppure indica i motivi della conservazione della segnalazione. In caso di mancata risposta alla scadenza del periodo di 30 giorni, la segnalazione è cancellata dal personale dell'ufficio SIRENE. Gli uffici SIRENE segnalano alla rispettiva autorità nazionale di controllo i problemi ricorrenti eventualmente incontrati in questo settore.

6. Nel periodo di riesame lo Stato membro segnalante può decidere, a seguito di una valutazione individuale globale che è registrata, di mantenere la segnalazione più a lungo, ove ciò sia necessario per gli scopi della segnalazione stessa. In tal caso il paragrafo 2 si applica anche a tale prolungamento. Ogni prolungamento di una segnalazione è comunicato al CS-SIS.

7. Le segnalazioni sono cancellate automaticamente allo scadere del periodo di riesame di cui al paragrafo 2, salvo qualora lo Stato membro segnalante abbia informato il CS-SIS del prolungamento della segnalazione a norma del paragrafo 6. Il CS-SIS segnala automaticamente agli Stati membri, con quattro mesi di anticipo, la prevista cancellazione di dati dal sistema.

8. Gli Stati membri redigono statistiche sul numero di segnalazioni il cui periodo di conservazione è stato prolungato a norma del paragrafo 6.

CAPO XIII

CANCELLAZIONE DELLE SEGNALAZIONI

Articolo 52
Cancellazione delle segnalazioni

1. Le segnalazioni per l'arresto a fini di consegna o estradizione di cui all'articolo 26 sono cancellate una volta che la persona è stata consegnata o estradata alle autorità competenti dello Stato membro segnalante. Possono essere altresì cancellate se la decisione giudiziaria su cui si basavano è stata revocata dall'autorità giudiziaria competente in conformità del diritto nazionale.

2. Le segnalazioni di persone scomparse sono cancellate secondo le seguenti regole:

   (a) per quanto riguarda i minori scomparsi di cui all'articolo 32, la segnalazione è cancellata:

   – alla risoluzione del caso, ad esempio se il minore è rimpatriato o le autorità competenti dello Stato membro di esecuzione prendono una decisione sull'affidamento del minore;

   – allo scadere del termine di validità della segnalazione conformemente all'articolo 51;

   – su decisione dell'autorità competente dello Stato membro segnalante; o

   – al reperimento del minore;

   (b) per quanto riguarda gli adulti scomparsi di cui all'articolo 32 per i quali non siano richieste misure di protezione, la segnalazione è cancellata:

   – una volta eseguita l'azione richiesta (accertamento del luogo di soggiorno da parte dello Stato membro di esecuzione);

   – allo scadere del termine di validità della segnalazione conformemente all'articolo 51; o

   – su decisione dell'autorità competente dello Stato membro segnalante;

   (c) per quanto riguarda gli adulti scomparsi di cui all'articolo 32 per i quali siano richieste misure di protezione, la segnalazione è cancellata:

   – una volta eseguita l'azione richiesta (persona posta sotto protezione);

– allo scadere del termine di validità della segnalazione conformemente all'articolo 51; o

– su decisione dell'autorità competente dello Stato membro segnalante.

Fatta salva la legislazione nazionale, qualora una persona sia internata su decisione dell'autorità competente, la segnalazione può essere mantenuta fino al suo rimpatrio.

3. Le segnalazioni di persone ricercate nell'ambito di un procedimento giudiziario sono cancellate secondo le seguenti regole:

per quanto riguarda le persone ricercate nell'ambito di un procedimento giudiziario di cui all'articolo 34, la segnalazione è cancellata:

(a) alla comunicazione del luogo di soggiorno della persona all'autorità competente dello Stato membro segnalante. Se non è possibile dare seguito alle informazioni trasmesse, l'ufficio SIRENE dello Stato membro segnalante ne informa l'ufficio SIRENE dello Stato membro di esecuzione affinché sia risolto il problema;

(b) allo scadere del termine di validità della segnalazione conformemente all'articolo 51; o

(c) su decisione dell'autorità competente dello Stato membro segnalante.

Qualora sia ottenuto un riscontro positivo in uno Stato membro e i dati riguardanti l'indirizzo siano trasmessi allo Stato membro segnalante e in quest'ultimo Stato sia ottenuto un riscontro positivo successivo che rivela gli stessi dati riguardanti l'indirizzo, il riscontro positivo è registrato nello Stato membro di esecuzione senza tuttavia che allo Stato membro segnalante siano ritrasmessi i dati riguardanti l'indirizzo o informazioni supplementari. In tali casi lo Stato membro di esecuzione informa del riscontro positivo ripetuto lo Stato membro segnalante, il quale valuta se sia necessario mantenere la segnalazione.

4. Le segnalazioni ai fini di un controllo discreto, di indagine o specifico sono cancellate secondo le seguenti regole:

per quanto riguarda le segnalazioni ai fini di un controllo discreto, di indagine o specifico di cui all'articolo 36, la segnalazione è cancellata:

(a) allo scadere del termine di validità della segnalazione conformemente all'articolo 51;

(b) su decisione dell'autorità competente dello Stato membro segnalante.

5. Le segnalazioni di oggetti a fini di sequestro o di prova sono cancellate secondo le seguenti regole:

per quanto riguarda le segnalazioni di oggetti a fini di sequestro o di prova di cui all'articolo 38, la segnalazione è cancellata:

(a) non appena l'oggetto sia posto sotto sequestro o misura equivalente, una volta che sia avvenuto il necessario successivo scambio di informazioni

supplementari tra uffici SIRENE o che l'oggetto sia sottoposto ad altra procedura giudiziaria o amministrativa;

(b) allo scadere del termine di validità della segnalazione; o

(c) su decisione dell'autorità competente dello Stato membro segnalante.

6. Le segnalazioni di ignoti ricercati di cui all'articolo 40 sono cancellate secondo le seguenti regole:

7. (a) quando è identificata la persona; o

8. (b) allo scadere del termine di validità della segnalazione.

CAPO XIV

REGOLE GENERALI SUL TRATTAMENTO DEI DATI

Articolo 53
Trattamento dei dati SIS

1. Gli Stati membri possono trattare i dati di cui all'articolo 20 solo ai fini enunciati per ciascuna delle categorie di segnalazioni di cui agli articoli 26, 32, 34, 36, 38 e 40.

2. I dati possono essere duplicati soltanto per fini tecnici, sempreché tale operazione sia necessaria per la consultazione diretta da parte delle autorità di cui all'articolo 43. Le disposizioni del presente regolamento si applicano a tali copie. Lo Stato membro non copia dal suo N.SIS o dal CS-SIS in altri archivi di dati nazionali dati relativi a segnalazioni o dati complementari inseriti da un altro Stato membro.

3. Le copie tecniche di cui al paragrafo 2 che portano alla creazione di banche dati off-line possono essere conservate per un periodo non superiore a 48 ore. Tale periodo può essere prolungato in caso di emergenza, finché l'emergenza non sia cessata.

4. Gli Stati membri tengono un inventario aggiornato di tali copie, lo rendono accessibile alla rispettiva autorità nazionale di controllo e assicurano che le disposizioni del presente regolamento, in particolare quelle dell'articolo 10, siano applicate a tali copie.

5. L'accesso ai dati è autorizzato esclusivamente nei limiti delle competenze delle autorità nazionali di cui all'articolo 43 e riservato al personale debitamente autorizzato.

6. Per quanto riguarda le segnalazioni di cui agli articoli 26, 32, 34, 36, 38 e 40, ogni trattamento delle informazioni in esse contenute per fini diversi da quelli per i quali sono state inserite nel SIS deve essere connesso a un caso specifico e giustificato dalla necessità di prevenire una minaccia grave imminente per l'ordine pubblico e la

sicurezza pubblica, da fondati motivi di sicurezza nazionale o ai fini della prevenzione di un reato grave. A tale scopo è ottenuta l'autorizzazione preventiva dello Stato membro segnalante.

7. Qualsiasi uso dei dati non conforme ai paragrafi da 1 a 6 è considerato un abuso ai sensi della legislazione di ciascuno Stato membro.

8. Ciascuno Stato membro invia all'agenzia l'elenco delle proprie autorità competenti autorizzate a consultare direttamente i dati inseriti nel SIS a norma del presente regolamento e le eventuali modifiche apportate all'elenco. L'elenco indica, per ciascuna autorità, i dati che essa può consultare e a quali fini. L'agenzia provvede alla pubblicazione annuale dell'elenco nella *Gazzetta ufficiale dell'Unione europea*.

9. Sempreché il diritto dell'Unione non preveda disposizioni particolari, la legislazione di ciascuno Stato membro si applica ai dati inseriti nel rispettivo N.SIS.

Articolo 54
Dati SIS e archivi nazionali

1. L'articolo 53, paragrafo 2, non pregiudica il diritto di uno Stato membro di conservare nel proprio archivio nazionale i dati SIS in collegamento con i quali è stata svolta un'azione nel suo territorio. Tali dati sono conservati negli archivi nazionali per un periodo massimo di tre anni, a meno che disposizioni specifiche di diritto nazionale prevedano un periodo di conservazione più lungo.

2. L'articolo 53, paragrafo 2, non pregiudica il diritto di uno Stato membro di conservare nel proprio archivio nazionale i dati contenuti in una segnalazione particolare effettuata nel SIS da quello stesso Stato membro.

Articolo 55
Informazione in caso di mancata esecuzione di una segnalazione

Se l'azione richiesta non può essere eseguita, lo Stato membro richiesto ne informa senza indugio lo Stato membro segnalante.

Articolo 56
Qualità dei dati trattati nel SIS

1. Lo Stato membro segnalante è responsabile dell'esattezza e dell'attualità dei dati e della liceità del loro inserimento nel SIS.

2. Solo lo Stato membro segnalante è autorizzato a modificare, completare, rettificare, aggiornare o cancellare i dati che ha inserito.

3. Se uno Stato membro diverso da quello che ha effettuato la segnalazione è in possesso di elementi che dimostrano che detti dati contengono errori di fatto o sono stati archiviati illecitamente, ne informa quanto prima, tramite scambio di informazioni supplementari ed entro dieci giorni dacché è in possesso di detti elementi, lo Stato membro segnalante. Lo Stato membro segnalante verifica la comunicazione e, se necessario, rettifica o cancella senza indugio i dati in questione.

4. Se, entro due mesi dal momento in cui sono emersi gli elementi ai sensi del paragrafo 3, gli Stati membri non giungono a un accordo, lo Stato membro che non ha effettuato la segnalazione sottopone la questione all'autorità nazionale di controllo affinché prenda una decisione.

5. Gli Stati membri si scambiano informazioni supplementari se una persona presenta un ricorso nel quale fa valere di non essere la persona oggetto della segnalazione. Se dalla verifica risulta che si tratta in effetti di due persone distinte, il ricorrente è informato delle misure previste all'articolo 59.

6. Se una persona è già segnalata nel SIS, lo Stato membro che introduce un'altra segnalazione si accorda in merito a tale inserimento con lo Stato membro che ha effettuato la prima segnalazione. L'accordo è raggiunto sulla base di uno scambio di informazioni supplementari.

Articolo 57
Incidenti di sicurezza

1. È considerato incidente di sicurezza l'evento che ha o può avere ripercussioni sulla sicurezza del SIS e può causare danni o perdite ai dati SIS, in particolare quando possono essere stati consultati dati o quando sono state o possono essere state compromesse la disponibilità, l'integrità e la riservatezza dei dati.

2. Gli incidenti di sicurezza sono gestiti in modo tale da garantire una risposta rapida, efficace e adeguata.

3. Gli Stati membri comunicano gli incidenti di sicurezza alla Commissione, all'agenzia e all'autorità nazionale di controllo. L'agenzia comunica gli incidenti di sicurezza alla Commissione e al garante europeo della protezione dei dati.

4. Le informazioni su un incidente di sicurezza che ha o può avere ripercussioni sul funzionamento del SIS in uno Stato membro o nell'agenzia, o sulla disponibilità, integrità e riservatezza dei dati inseriti o inviati da altri Stati membri, sono trasmesse agli Stati membri e registrate secondo il piano di gestione degli incidenti stabilito dall'agenzia.

Articolo 58
Distinzione tra persone con caratteristiche simili

Quando, inserendo una nuova segnalazione, risulta evidente che nel SIS è già registrata una persona che possiede gli stessi elementi di descrizione dell'identità, si applica la procedura seguente:

(a) l'ufficio SIRENE si mette in contatto con l'autorità richiedente allo scopo di verificare se la segnalazione riguardi o meno la stessa persona;

(b) se da tale controllo incrociato risulta che la persona oggetto di una nuova segnalazione e quella già registrata nel SIS sono effettivamente la stessa persona, l'ufficio SIRENE applica la procedura per l'inserimento di segnalazioni multiple di cui all'articolo 56, paragrafo 6. Qualora si stabilisca che si tratta di due persone

diverse, l'ufficio SIRENE convalida la richiesta di inserimento della seconda segnalazione aggiungendo gli elementi necessari per evitare errori di identificazione.

Articolo 59
Dati complementari per trattare i casi di usurpazione di identità

1. Quando sono possibili confusioni fra la persona effettivamente oggetto di una segnalazione e una persona la cui identità è stata usurpata, lo Stato membro segnalante aggiunge alla segnalazione, con il consenso esplicito della persona interessata, dati che la riguardano per evitare le conseguenze negative di un errore di identificazione.

2. I dati relativi alla vittima dell'usurpazione di identità sono usati soltanto ai seguenti fini:

   (a) consentire all'autorità competente di distinguere la persona la cui identità è stata usurpata dalla persona effettivamente oggetto della segnalazione;

   (b) permettere alla persona la cui identità è stata usurpata di dimostrare la propria identità e di stabilire di essere stata vittima di un'usurpazione di identità.

3. Ai fini del presente articolo possono essere inseriti e successivamente trattati nel SIS soltanto i seguenti dati personali:

   (a) cognome/cognomi;

   (b) nome/nomi;

   (c) nome/nomi e cognome/cognomi alla nascita;

   (d) eventuali nomi e cognomi precedenti e "alias", eventualmente registrati a parte;

   (e) segni fisici particolari, oggettivi ed inalterabili;

   (f) luogo di nascita;

   (g) data di nascita;

   (h) sesso;

   (i) fotografie e immagini facciali;

   (j) impronte digitali;

   (k) cittadinanza/cittadinanze;

   (l) categoria del documento di identità;

   (m) paese di rilascio del documento di identità;

   (n) numero del documento di identità;

(o) data di rilascio del documento di identità;

(p) indirizzo della vittima;

(q) nome del padre della vittima;

(r) nome della madre della vittima.

4. Le norme tecniche necessarie per l'inserimento e l'ulteriore trattamento dei dati di cui al paragrafo 3 sono stabilite mediante misure di esecuzione adottate e sviluppate secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

5. I dati di cui al paragrafo 3 sono cancellati insieme con la segnalazione corrispondente o prima su richiesta dell'interessato.

6. Possono accedere ai dati di cui al paragrafo 3 soltanto le autorità che hanno diritto di accesso alla segnalazione corrispondente. Esse possono accedervi all'unico scopo di evitare errori di identificazione.

Articolo 60
Connessioni fra segnalazioni

1. Uno Stato membro può creare una connessione tra segnalazioni che introduce nel SIS. Effetto della connessione è istaurare un nesso fra due o più segnalazioni.

2. La creazione di una connessione non incide sulla specifica azione da intraprendere sulla base di ciascuna segnalazione interconnessa né sul rispettivo termine di conservazione.

3. La creazione di una connessione non incide sui diritti di accesso previsti nel presente regolamento. Le autorità che non hanno diritto di accesso a talune categorie di segnalazioni non sono in grado di visualizzare la connessione a una segnalazione cui non hanno accesso.

4. Uno Stato membro crea una connessione tra segnalazioni solo se sussiste un'esigenza operativa.

5. Uno Stato membro, qualora ritenga che la creazione di una connessione tra segnalazioni da parte di un altro Stato membro sia incompatibile con la sua legislazione nazionale o i suoi obblighi internazionali, può adottare le necessarie disposizioni affinché non sia possibile accedere alla connessione dal suo territorio nazionale o per le sue autorità dislocate al di fuori del suo territorio.

6. Le norme tecniche necessarie per la connessione tra segnalazioni sono stabilite e sviluppate secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

Articolo 61
Finalità e termini di conservazione delle informazioni supplementari

1. Gli Stati membri conservano un riferimento alle decisioni che danno origine a una segnalazione presso l'ufficio SIRENE, a sostegno dello scambio di informazioni supplementari.

2. I dati personali archiviati dall'ufficio SIRENE in seguito allo scambio di informazioni sono conservati soltanto per il tempo necessario a conseguire gli scopi per i quali sono stati forniti. Essi sono in ogni caso cancellati al più tardi un anno dopo che è stata cancellata dal SIS la relativa segnalazione.

3. Il paragrafo 2 non pregiudica il diritto dello Stato membro di conservare negli archivi nazionali i dati relativi a una determinata segnalazione da esso effettuata o a una segnalazione in collegamento con la quale è stata intrapresa un'azione nel suo territorio. Il periodo per cui tali dati possono essere conservati in tali archivi è disciplinato dalla legislazione nazionale.

Articolo 62
Trasferimento di dati personali a terzi

I dati trattati nel SIS e le relative informazioni supplementari a norma del presente regolamento non sono trasferiti a paesi terzi o ad organizzazioni internazionali, né sono messi a loro disposizione.

Articolo 63
Scambio di dati con Interpol sui passaporti rubati, altrimenti sottratti, smarriti o invalidati

1. In deroga all'articolo 62 il numero, il paese di rilascio e la tipologia dei passaporti rubati, altrimenti sottratti, smarriti o invalidati inseriti nel SIS possono essere scambiati con membri di Interpol stabilendo un collegamento tra il SIS e la banca dati di Interpol sui documenti di viaggio rubati o smarriti, a condizione che sia concluso un accordo tra Interpol e l'Unione europea. In base a tale accordo la trasmissione di dati inseriti da uno Stato membro è soggetta al consenso di tale Stato membro.

2. L'accordo di cui al paragrafo 1 prevede che i dati condivisi siano accessibili solo a membri di Interpol di paesi che assicurano un adeguato livello di protezione dei dati personali. Prima di concludere l'accordo, il Consiglio chiede il parere della Commissione sull'adeguatezza del livello di protezione dei dati personali e di rispetto dei diritti e delle libertà fondamentali per quanto riguarda il trattamento automatizzato dei dati personali da parte di Interpol e da parte dei paesi che hanno distaccato membri presso Interpol.

3. L'accordo di cui al paragrafo 1 può anche prevedere che gli Stati membri abbiano accesso, attraverso il SIS, ai dati della banca dati di Interpol sui documenti di viaggio rubati o smarriti, in conformità delle pertinenti disposizioni del presente regolamento che disciplinano le segnalazioni sui passaporti rubati, altrimenti sottratti, smarriti o invalidati inserite nel SIS.

CAPO XV

PROTEZIONE DEI DATI

Articolo 64
Legislazione applicabile

1. Il regolamento (CE) n. 45/2001 si applica al trattamento dei dati personali da parte dell'agenzia in conformità del presente regolamento.

2. Il regolamento (UE) 2016/679 si applica al trattamento dei dati personali laddove non si applicano le disposizioni nazionali di attuazione della direttiva (UE) 2016/680.

3. Al trattamento dei dati da parte delle autorità nazionali competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, compresa la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse, si applicano le disposizioni nazionali di attuazione della direttiva (UE) 2016/680.

Articolo 65
Diritto di accesso, rettifica di dati inesatti e cancellazione di dati archiviati illecitamente

1. Il diritto dell'interessato di accedere ai dati che lo riguardano inseriti nel SIS e di ottenerne la rettifica o la cancellazione è esercitato nel rispetto della legislazione dello Stato membro presso il quale l'interessato lo fa valere.

2. Ove previsto dalla legislazione nazionale, l'autorità nazionale di controllo decide se e in base a quali modalità devono essere comunicate informazioni.

3. Uno Stato membro diverso da quello che ha effettuato la segnalazione può comunicare informazioni su tali dati soltanto se dà prima la possibilità allo Stato membro segnalante di prendere posizione. A ciò si provvede tramite lo scambio di informazioni supplementari.

4. Gli Stati membri possono decidere di non comunicare informazioni all'interessato, del tutto o in parte, in conformità della legislazione nazionale, nella misura e per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata, al fine di:

   (a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;

   (b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;

   (c) proteggere la sicurezza pubblica;

(d) proteggere la sicurezza nazionale;

(e) proteggere i diritti e le libertà altrui.

5. Chiunque ha il diritto di far rettificare dati che lo riguardano contenenti errori di fatto o di far cancellare dati che lo riguardano inseriti illecitamente.

6. L'interessato è informato non appena possibile e comunque non oltre 60 giorni dalla data in cui ha chiesto l'accesso o prima, se la legislazione nazionale lo prevede.

7. L'interessato è informato del seguito dato all'esercizio del suo diritto di rettifica e cancellazione non appena possibile e comunque non oltre tre mesi dalla data in cui ha chiesto la rettifica o la cancellazione o prima, se la legislazione nazionale lo prevede.

Articolo 66
Mezzi di impugnazione

1. Chiunque può adire il giudice o l'autorità competente in base alla legislazione di qualsiasi Stato membro, per accedere, rettificare, cancellare o ottenere informazioni o per ottenere un indennizzo relativamente a una segnalazione che lo riguarda.

2. Gli Stati membri si impegnano reciprocamente ad eseguire le decisioni definitive emesse dai giudici o dalle autorità di cui al paragrafo 1, fatte salve le disposizioni dell'articolo 70.

3. Per ottenere un coerente quadro di insieme del funzionamento dei mezzi di impugnazione, le autorità nazionali elaborano un sistema statistico standard per produrre relazioni annuali su:

(a) il numero di richieste di accesso presentate dagli interessati al titolare del trattamento e il numero di casi in cui è stato accordato l'accesso ai dati;

(b) il numero di richieste di accesso presentate dagli interessati all'autorità nazionale di controllo e il numero di casi in cui è stato accordato l'accesso ai dati;

(c) il numero di richieste di rettifica di dati inesatti e cancellazione di dati archiviati illecitamente presentate al titolare del trattamento e il numero di casi in cui i dati sono stati rettificati o cancellati;

(d) il numero di richieste di rettifica di dati inesatti e di cancellazioni di dati archiviati illecitamente presentate all'autorità nazionale di controllo;

(e) il numero di cause pendenti dinanzi ai giudici;

(f) il numero di cause in cui il giudice ha statuito a favore del ricorrente in qualsiasi aspetto della causa;

(g) eventuali osservazioni sui casi di riconoscimento reciproco delle decisioni definitive adottate da giudici o autorità di altri Stati membri su segnalazioni create dallo Stato membro segnalante.

Le relazioni delle autorità nazionali di controllo sono trasmesse al meccanismo di cooperazione di cui all'articolo 69.

Articolo 67
Controllo dell'N.SIS

1. Ogni Stato membro garantisce che l'autorità o le autorità nazionali di controllo in esso designate e investite dei poteri di cui al capo VI della direttiva (UE) 2016/680 o al capo VI del regolamento (UE) 2016/679 controllino in indipendenza la liceità del trattamento dei dati personali SIS nel territorio di appartenenza e della loro trasmissione da detto territorio, nonché lo scambio e il successivo trattamento di informazioni supplementari.

2. L'autorità nazionale di controllo provvede affinché sia svolto un controllo delle operazioni di trattamento dei dati nell'N.SIS del proprio paese, conformemente alle norme di revisione internazionali, almeno ogni quattro anni. Il controllo è svolto dalle autorità nazionali di controllo oppure da queste commissionato direttamente a un revisore per la protezione di dati indipendente. L'autorità nazionale di controllo mantiene in qualsiasi momento il controllo sul revisore indipendente e la responsabilità del suo operato.

3. Gli Stati membri provvedono affinché la rispettiva autorità nazionale di controllo disponga di risorse sufficienti per assolvere i compiti ad essa assegnati a norma del presente regolamento.

Articolo 68
Controllo dell'agenzia

1. Il garante europeo della protezione dei dati garantisce che le attività di trattamento dei dati personali da parte dell'agenzia siano effettuate in conformità del presente regolamento. Si applicano di conseguenza le funzioni e le competenze di cui agli articoli 46 e 47 del regolamento (CE) n. 45/2001.

2. Il garante europeo della protezione dei dati provvede affinché sia svolto un controllo delle attività di trattamento dei dati personali effettuate dall'agenzia, conformemente alle norme di revisione internazionali, almeno ogni quattro anni. Una relazione su tale controllo è trasmessa al Parlamento europeo, al Consiglio, all'agenzia, alla Commissione e alle autorità nazionali di controllo. L'agenzia ha l'opportunità di presentare le sue osservazioni prima dell'adozione della relazione.

Articolo 69
Cooperazione tra le autorità nazionali di controllo e il garante europeo della protezione dei dati

1. Le autorità nazionali di controllo e il garante europeo della protezione dei dati, ciascuno nell'ambito delle proprie competenze, cooperano attivamente nel quadro delle rispettive responsabilità e assicurano il controllo coordinato del SIS.

2. Se necessario, ciascuno nell'ambito delle proprie competenze, essi si scambiano informazioni pertinenti, si assistono vicendevolmente nello svolgimento di revisioni e ispezioni, esaminano difficoltà di interpretazione o applicazione del presente regolamento e di altri atti giuridici dell'Unione applicabili, studiano i problemi emersi nell'esercizio di un controllo indipendente o nell'esercizio dei diritti degli interessati, elaborano proposte armonizzate per soluzioni congiunte di eventuali problemi e promuovono la sensibilizzazione del pubblico in materia di diritti di protezione dei dati.

3. Ai fini di cui al paragrafo 2, le autorità nazionali di controllo e il garante europeo della protezione dei dati si incontrano almeno due volte l'anno nell'ambito del comitato europeo per la protezione dei dati istituito dal regolamento (UE) 2016/679. I costi di tali riunioni e la gestione delle stesse sono a carico del comitato istituito dal regolamento (UE) 2016/679. Nella prima riunione è adottato un regolamento interno. Ulteriori metodi di lavoro sono elaborati congiuntamente, se necessario.

4. Ogni due anni il comitato istituito dal regolamento (UE) 2016/679 trasmette al Parlamento europeo, al Consiglio e alla Commissione una relazione congiunta sulle attività inerenti al controllo coordinato.

CAPO XVI

RESPONSABILITÀ

Articolo 70
Responsabilità

1. Ciascuno Stato membro è responsabile dei danni causati a una persona in seguito all'uso dell'N.SIS. La disposizione si applica anche ai danni causati dallo Stato membro segnalante, ove abbia inserito dati contenenti errori di fatto o archiviato i dati in modo illecito.

2. Se lo Stato membro contro il quale è promossa un'azione non è lo Stato membro segnalante, quest'ultimo è tenuto al rimborso, su richiesta, delle somme versate a titolo di risarcimento, a meno che l'uso dei dati da parte dello Stato membro che ha chiesto il rimborso violi il presente regolamento.

3. Se l'inosservanza da parte di uno Stato membro degli obblighi derivanti dal presente regolamento causa danni al SIS, tale Stato membro ne risponde, a meno che e nella misura in cui l'agenzia o un altro Stato membro partecipante al SIS non abbia omesso di adottare le misure ragionevolmente necessarie a evitare tali danni o a minimizzarne gli effetti.

CAPO XVII

DISPOSIZIONI FINALI

Articolo 71
Monitoraggio e statistiche

1. L'agenzia provvede affinché siano attivate procedure atte a controllare il funzionamento del SIS in rapporto a obiettivi di risultato, economicità, sicurezza e qualità del servizio.

2. Ai fini della manutenzione tecnica, delle relazioni e delle statistiche, l'agenzia ha accesso alle informazioni necessarie riguardanti le operazioni di trattamento effettuate nel SIS centrale.

3. L'agenzia pubblica statistiche giornaliere, mensili e annuali relative al numero di registrazioni per categoria di segnalazione, al numero annuo di riscontri positivi per categoria di segnalazione, al numero di interrogazioni del SIS e di accessi al SIS per l'inserimento, l'aggiornamento o la cancellazione di una segnalazione, in totale e per ciascuno Stato membro. Le statistiche prodotte non contengono dati personali. La relazione statistica annuale è pubblicata. L'agenzia pubblica inoltre statistiche annuali sull'uso della funzionalità che consiste nel rendere temporaneamente non consultabile una segnalazione effettuata a norma dell'articolo 26, in totale e per ciascuno Stato membro, comprese eventuali estensioni del periodo di conservazione di 48 ore.

4. Gli Stati membri, Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera forniscono all'agenzia e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai paragrafi 3, 7 e 8. Tali informazioni comprendono statistiche distinte sul numero di interrogazioni effettuate dai o per conto dei servizi competenti negli Stati membri per il rilascio delle carte di circolazione dei veicoli e dai servizi competenti negli Stati membri per il rilascio di certificati di immatricolazione o per la gestione del traffico di natanti, compresi i relativi motori, aeromobili e container. Le statistiche riportano anche il numero di riscontri positivi per categoria di segnalazione.

5. L'agenzia trasmette agli Stati membri, alla Commissione, a Europol, a Eurojust e all'Agenzia europea della guardia di frontiera e costiera tutte le relazioni statistiche che produce. Per controllare l'attuazione degli atti giuridici nell'Unione, la Commissione può chiedere all'agenzia di fornire specifiche relazioni statistiche aggiuntive, periodicamente o ad hoc, sulle prestazioni o sull'uso del SIS e sulla comunicazione tramite SIRENE.

6. Ai fini dei paragrafi 3, 4 e 5 e dell'articolo 15, paragrafo 5, l'agenzia istituisce, attua e ospita un archivio centrale nei suoi siti tecnici contenente i dati di cui al paragrafo 3 e all'articolo 15, paragrafo 5, che non consentono l'identificazione delle persone fisiche e permettono alla Commissione e alle agenzie di cui paragrafo 5 di ottenere relazioni e statistiche personalizzate. L'agenzia accorda agli Stati membri, alla

Commissione, a Europol, a Eurojust e all'Agenzia europea della guardia di frontiera e costiera l'accesso all'archivio centrale mediante un accesso protetto tramite l'infrastruttura di comunicazione, con controllo dell'accesso e specifici profili di utente, unicamente ai fini dell'elaborazione di relazioni e statistiche.

Le modalità dettagliate di funzionamento dell'archivio centrale e le norme sulla protezione dei dati e sulla sicurezza applicabili all'archivio sono stabilite mediante misure di esecuzione adottate secondo la procedura di esame di cui all'articolo 72, paragrafo 2.

7. Due anni dopo l'inizio delle attività del SIS e successivamente ogni due anni l'agenzia presenta al Parlamento europeo e al Consiglio una relazione sul funzionamento tecnico del SIS centrale e dell'infrastruttura di comunicazione, compresa la sicurezza degli stessi, e sullo scambio bilaterale e multilaterale di informazioni supplementari fra Stati membri.

8. Tre anni dopo l'inizio delle attività del SIS e successivamente ogni quattro anni, la Commissione presenta una valutazione globale del SIS centrale e dello scambio bilaterale e multilaterale di informazioni supplementari fra Stati membri. Tale valutazione globale comprende un'analisi dei risultati conseguiti in relazione agli obiettivi e una valutazione circa la validità dei principi di base, l'applicazione del presente regolamento con riguardo al SIS centrale, la sicurezza del SIS centrale e le eventuali implicazioni per le attività future. La Commissione trasmette la valutazione al Parlamento europeo e al Consiglio.

Articolo 72
Procedura di comitato

1. La Commissione è assistita da un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

Articolo 73
Modifiche del regolamento (UE) n. 515/2014

Il regolamento (UE) n. 515/2014[76] è così modificato:

All'articolo 6 è aggiunto il seguente paragrafo 6:

"6. Durante la fase di sviluppo gli Stati membri ricevono una dotazione supplementare di 36,8 milioni di EUR da distribuire tramite una somma forfettaria in aggiunta alla loro dotazione di base e destinano interamente tale finanziamento ai sistemi nazionali del SIS per garantirne un aggiornamento rapido ed efficace in linea con l'attuazione del SIS centrale, come previsto dal regolamento (UE) 2018/...* e dal regolamento (UE) 2018/...**

[76] Regolamento (UE) n. 515/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, che istituisce, nell'ambito del Fondo sicurezza interna, lo strumento di sostegno finanziario per le frontiere esterne e i visti (GU L 150 del 20.5.2014, pag. 143).

[*]Regolamento 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 (GU….).

[**] Regolamento (UE) 2018/... sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera (GU…)."

Articolo 74
Abrogazione

Alla data di applicazione del presente regolamento sono abrogati i seguenti atti giuridici:

regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'accesso al sistema d'informazione Schengen di seconda generazione (SIS II) dei servizi competenti negli Stati membri per il rilascio delle carte di circolazione;

decisione 533/2007/GAI del Consiglio, del 12 luglio 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II);

decisione 2010/261/UE della Commissione, del 4 maggio 2010, relativa al piano di sicurezza per il SIS II centrale e l'infrastruttura di comunicazione[77].

Articolo 75
Entrata in vigore e applicazione

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.

2. Esso si applica a decorrere dalla data fissata dalla Commissione dopo che:

   (a) saranno state adottate le necessarie misure di esecuzione;

   (b) gli Stati membri avranno notificato alla Commissione di aver preso le disposizioni tecniche e giuridiche necessarie per trattare i dati SIS e scambiare informazioni supplementari a norma del presente regolamento;

   (c) l'agenzia avrà comunicato alla Commissione il completamento di tutte le attività di collaudo relative al CS-SIS e all'interazione tra CS-SIS e N.SIS.

3. Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri conformemente al trattato sul funzionamento dell'Unione europea.

[77] Decisione 2010/261/UE della Commissione, del 4 maggio 2010, relativa al piano di sicurezza per il SIS II centrale e l'infrastruttura di comunicazione (GU L 112 del 5.5.2010, pag. 31).

Fatto a Bruxelles, il

Per il Parlamento europeo
Il presidente

Per il Consiglio
Il presidente

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

1.2. Settore/settori interessati nella struttura ABM/ABB

1.3. Natura della proposta/iniziativa

1.4. Obiettivi

1.5. Motivazione della proposta/iniziativa

1.6. Durata e incidenza finanziaria

1.7. Modalità di gestione previste

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

2.2. Sistema di gestione e di controllo

2.3. Misure di prevenzione delle frodi e delle irregolarità

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

3.2.2. Incidenza prevista sugli stanziamenti operativi

3.2.3. Incidenza prevista sugli stanziamenti di natura amministrativa

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

3.2.5. Partecipazione di terzi al finanziamento

3.3. Incidenza prevista sulle entrate

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di regolamento del Parlamento europeo e del Consiglio 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 il regolamento (UE) n. 515/2014 e abroga il regolamento (CE) n. 1986/2006, la decisione 2007/533/GAI del Consiglio e la decisione 2010/261/UE della Commissione.

1.2. Settore/settori interessati nella struttura ABM/ABB[78]

Settore: Migrazione e affari interni (titolo 18)

1.3. Natura della proposta/iniziativa

☐ La proposta/iniziativa riguarda **una nuova azione**

☐ La proposta/iniziativa riguarda **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[79]

☑ La proposta/iniziativa riguarda **la proroga di un'azione esistente**

☐ La proposta/iniziativa riguarda **un'azione riorientata verso una nuova azione**

1.4. Obiettivi

1.4.1. Obiettivi strategici pluriennali della Commissione oggetto della proposta/iniziativa

Obiettivo – "Contrastare la criminalità organizzata"

Obiettivo – "Una risposta forte dell'UE per combattere il terrorismo e prevenire la radicalizzazione"

La necessità di rivedere la base giuridica del SIS per affrontare le nuove sfide in materia di sicurezza e migrazione è stata sottolineata a più riprese dalla Commissione. Ad esempio, nell'"Agenda europea sulla sicurezza"[80] la Commissione ha annunciato l'intenzione di valutare il SIS nel periodo 2015-2016 e verificare l'esistenza di nuove esigenze operative che richiedano cambiamenti legislativi. Inoltre, l'Agenda sulla sicurezza sottolinea che il SIS è al centro dello scambio d'informazioni della polizia e va rafforzato. Più di recente, nella comunicazione "Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza"[81], la

78 ABM: activity-based management (gestione per attività) ABB: ABB: activity-based budgeting (bilancio per attività).

79 A norma dell'articolo 54, paragrafo 2, lettera a) o b), del regolamento finanziario.

80 COM(2015) 185 final.

81 COM(2016) 205 final.

Commissione ha affermato che avrebbe valutato la possibilità di aumentare le funzionalità del sistema sulla base della relazione di valutazione generale, per presentare proposte di revisione della base giuridica del SIS. Infine il 20 aprile 2016, nella comunicazione "Attuare l'Agenda europea sulla sicurezza per combattere il terrorismo e preparare il terreno per l'Unione della sicurezza"[82], la Commissione ha proposto una serie di cambiamenti del SIS per migliorarne il valore aggiunto a fini di contrasto.

La valutazione generale svolta dalla Commissione ha confermato che il SIS costituisce un successo dal punto di vista operativo. Nonostante i suoi risultati positivi, tuttavia, la valutazione ha portato anche a una serie di raccomandazioni volte a rafforzare l'efficacia e l'efficienza tecnica e operativa del sistema.

Sulla base delle raccomandazioni formulate nella relazione di valutazione generale e in piena coerenza con gli obiettivi annunciati dalla Commissione nelle suddette comunicazioni e con il piano strategico 2016-2020 della DG Migrazione e Affari interni[83], la presente proposta intende realizzare:

- l'intenzione espressa dalla Commissione di migliorare il valore aggiunto del SIS a fini di contrasto per rispondere alle nuove minacce;
- le raccomandazioni relative a modifiche tecniche e procedurali risultanti da una valutazione globale del SIS;
- le richieste di miglioramenti tecnici del SIS da parte degli utenti finali;
- le conclusioni provvisorie del gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità per quanto riguarda la qualità dei dati.

1.4.2. Obiettivi specifici e attività ABM/ABB interessate

Obiettivo specifico n.

Piano di gestione 2017 della DG Migrazione e affari interni

Obiettivo specifico 2.1 – Una risposta forte dell'UE per combattere il terrorismo e prevenire la radicalizzazione

Obiettivo specifico 2.2 – Contrastare la criminalità transfrontaliera grave e organizzata

Attività ABM/ABB interessate

Capitolo 18 02 – Sicurezza interna

82 COM(2016) 230 final.
83 Ares(2016)2231546 – 12.5.2016.

1.4.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

L'obiettivo primario delle proposte modifiche giuridiche e tecniche del SIS è rendere il sistema più efficace sotto il profilo operativo. Nella valutazione generale del SIS svolta dalla DG HOME nel periodo 2015-2016 sono stati raccomandati miglioramenti tecnici del sistema e un'armonizzazione delle procedure nazionali nel settore della cooperazione a fini di contrasto.

La nuova proposta introduce misure che rispondono alle esigenze operative e tecniche degli utenti finali. In particolare, i nuovi campi di dati per le segnalazioni esistenti permetteranno alle forze di polizia di disporre di tutte le informazioni necessarie per adempiere in modo efficace ai loro compiti. Inoltre, la proposta sottolinea specificamente l'importanza di una disponibilità ininterrotta del SIS, poiché le inattività possono incidere in misura significativa sull'operato delle autorità di contrasto. Per di più, la presente proposta prevede modifiche tecniche che renderanno il sistema più efficiente e semplice.

Una volta adottate e applicate, queste proposte aumenteranno anche la continuità operativa, in quanto gli Stati membri saranno obbligati a tenere una copia nazionale completa o parziale e una copia di riserva. Ciò permetterà al sistema di rimanere pienamente funzionale e operativo per gli operatori attivi sul terreno.

La proposta introduce nuovi identificatori biometrici: impronte palmari, immagini facciali e profili DNA in casi specifici e limitati. Questo, insieme ai cambiamenti previsti degli articoli 32 e 33 (segnalazioni di persone scomparse) per consentire l'inserimento di segnalazioni preventive e la categorizzazione di casi di persone scomparse, in primo luogo rafforzeranno notevolmente la protezione dei minori non accompagnati e, in secondo luogo, ne permetteranno l'identificazione sulla base del loro profilo DNA o quello dei genitori e/o fratelli (previo consenso).

Le autorità degli Stati membri potranno inoltre effettuare segnalazioni di ignoti ricercati per un reato esclusivamente sulla base di impronte digitali o palmari latenti o rilevate sul luogo del reato. Ciò non è consentito dal vigente quadro giuridico e tecnico e pertanto rappresenta un importante sviluppo.

1.4.4. Indicatori di risultato e di incidenza

Precisare gli indicatori che permettono di seguire l'attuazione della proposta/iniziativa.

Durante l'aggiornamento del sistema

Una volta approvata la proposta e adottate le specifiche tecniche, il SIS sarà aggiornato per armonizzare meglio le procedure nazionali di uso del sistema, ampliarne il campo di applicazione aggiungendo nuovi elementi alle categorie di segnalazione esistenti, e introdurre cambiamenti tecnici per migliorare la sicurezza e contribuire a ridurre gli oneri amministrativi. eu-LISA coordinerà la gestione del progetto di aggiornamento del sistema. eu-LISA stabilirà una struttura di gestione del progetto e fisserà scadenze dettagliate con tappe per attuare i cambiamenti proposti,

che consentiranno alla Commissione di monitorare attentamente la realizzazione della proposta.

Obiettivo specifico – entrata in funzione delle funzionalità aggiornate del SIS nel 2020.

Indicatore – conclusione positiva del collaudo globale del sistema aggiornato prima che sia avviato.

Una volta che il sistema sarà operativo

Quando il sistema sarà in funzione, eu-LISA provvederà affinché siano attivate procedure atte a controllare il funzionamento del SIS in rapporto a obiettivi di risultati, economicità, sicurezza e qualità del servizio. Due anni dopo l'inizio delle attività del SIS e successivamente ogni due anni, eu-LISA dovrà presentare al Parlamento europeo e al Consiglio una relazione sul funzionamento tecnico del SIS centrale e dell'infrastruttura di comunicazione, compresa la sicurezza degli stessi, e sullo scambio bilaterale e multilaterale di informazioni supplementari fra Stati membri. Inoltre, eu-LISA pubblicherà statistiche giornaliere, mensili e annuali relative al numero di registri per categoria di segnalazione, al numero annuo di riscontri positivi (hit) per categoria di segnalazione, al numero di interrogazioni del SIS e di accessi al medesimo per l'inserimento, l'aggiornamento o la cancellazione di una segnalazione, in totale e per ciascuno Stato membro. L'agenzia pubblicherà altresì statistiche annuali sull'uso della funzionalità che consiste nel rendere temporaneamente non consultabile una segnalazione effettuata a norma dell'articolo 26 del presente regolamento, in totale e per ciascuno Stato membro, comprese eventuali estensioni del periodo di conservazione di 48 ore.

Tre anni dopo l'inizio delle attività del SIS e successivamente ogni quattro anni, la Commissione presenterà una valutazione globale del SIS centrale e dello scambio bilaterale e multilaterale di informazioni supplementari fra Stati membri. Tale valutazione globale comprenderà un'analisi dei risultati conseguiti in relazione agli obiettivi e una valutazione circa la validità dei principi di base, l'applicazione del presente regolamento con riguardo al SIS centrale, la sicurezza del SIS centrale e le eventuali implicazioni per attività future. La Commissione trasmetterà la valutazione al Parlamento europeo e al Consiglio.

Obiettivo specifico 1 – Contrastare la criminalità organizzata

Indicatore – Uso dei meccanismi di scambio d'informazioni dell'UE. La realizzazione dell'obiettivo può essere misurata tramite un aumento del numero di riscontri positivi nel SIS. Gli indicatori sono le relazioni statistiche pubblicate da eu-LISA e dagli Stati membri, che permetteranno alla Commissione di valutare come sono usate le nuove funzionalità del sistema.

Obiettivo specifico 2 – Una risposta forte dell'UE per combattere il terrorismo e prevenire la radicalizzazione

Indicatore – Aumento del numero di segnalazioni e riscontri positivi, specialmente in relazione all'articolo 36, paragrafo 3, della proposta, che riguarda le segnalazioni di persone e oggetti nell'ambito di controlli discreti, di indagine e specifici.

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine

1. Contribuire a mantenere un elevato livello di sicurezza nello spazio di libertà, sicurezza e giustizia dell'UE.

2. Armonizzare meglio le procedure nazionali di uso del SIS.

3. Ampliare l'elenco di utenti istituzionali con accesso ai dati SIS accordando pieno accesso al sistema a Europol e alla nuova guardia di frontiera e costiera europea.

4. Aggiungere nuovi elementi alle segnalazioni SIS e nuove funzionalità per ampliare il campo di applicazione del sistema, permettere a quest'ultimo di affrontare l'attuale situazione in materia di sicurezza, rafforzare la cooperazione tra le autorità di contrasto e di sicurezza degli Stati membri e ridurre gli oneri amministrativi.

5. Trattare l'uso completo del SIS da un'estremità all'altra, non limitandosi a occuparsi dei sistemi centrale e nazionali, ma garantendo anche che gli utenti finali ricevano tutti i dati necessari per adempiere le loro funzioni.

6. Aumentare la continuità operativa e garantire il funzionamento ininterrotto del SIS a livello centrale e nazionale.

7. Rafforzare la lotta alla criminalità internazionale, al terrorismo e alla criminalità informatica in quanto settori connessi tra loro con una forte dimensione transfrontaliera.

1.5.2. Valore aggiunto dell'intervento dell'Unione europea

Il SIS è la principale banca dati per la sicurezza in Europa. In mancanza di controlli alle frontiere interne, la lotta efficace contro la criminalità e il terrorismo ha assunto una dimensione europea. Gli obiettivi della proposta riguardano miglioramenti tecnici per rafforzare l'efficienza e l'efficacia del sistema e armonizzarne l'uso negli Stati membri partecipanti. Data la natura transnazionale di questi obiettivi, e considerata la sfida di garantire un efficace scambio di informazioni per contrastare minacce sempre più diversificate, l'UE è nella posizione migliore per proporre soluzioni a tali problemi. Gli obiettivi di rafforzare l'efficienza e armonizzare ulteriormente l'uso del SIS, con un aumento in termini di volume, qualità e velocità dello scambio d'informazioni tramite un sistema d'informazione centralizzato su larga scala gestito da un'agenzia di regolamentazione (eu-LISA), non possono essere conseguiti dai soli Stati membri e richiedono un intervento a livello di UE. Se gli attuali problemi non sono affrontati, il SIS continuerà a funzionare secondo le norme vigenti e perderà quindi le opportunità di diventare più efficiente e aumentare il suo valore aggiunto UE che sono state individuate grazie alla valutazione del SIS e del suo uso da parte degli Stati membri.

Nel solo 2015 le autorità competenti degli Stati membri hanno avuto accesso al sistema quasi 2,9 miliardi di volte: una chiara dimostrazione del contributo vitale del sistema alla cooperazione nelle attività di contrasto nello spazio Schengen. Non sarebbe stato possibile raggiungere un livello così alto di scambio di informazioni tra

Stati membri tramite soluzioni nazionali decentrate, né conseguire risultati simili a livello degli Stati membri. Inoltre, il SIS si è dimostrato il più efficace strumento di scambio di informazioni a fini di lotta contro il terrorismo e presenta un valore aggiunto UE in quanto consente ai servizi di sicurezza nazionali di cooperare in modo rapido, riservato ed efficace. Le nuove proposte favoriranno ulteriormente lo scambio di informazioni e la cooperazione tra gli Stati membri dell'UE. Inoltre Europol e la nuova Agenzia europea della guardia di frontiera e costiera avranno pieno accesso al sistema entro i limiti delle loro competenze: un chiaro segnale del valore aggiunto della partecipazione dell'UE.

1.5.3. Insegnamenti tratti da esperienze analoghe

1. La fase di sviluppo dovrebbe iniziare solo una volta definite pienamente le necessità operative e le esigenze degli utenti finali. Lo sviluppo potrà avvenire solo quando saranno stati adottati in via definitiva gli strumenti giuridici che stabiliranno le finalità, l'ambito di applicazione, le funzioni e le particolarità tecniche.

2. La Commissione ha svolto (e continua a svolgere) consultazioni continue con i portatori di interessi, compresi delegati del comitato SISVIS nell'ambito della procedura di comitatologia. Tale comitato comprende i rappresentanti degli Stati membri competenti sia per questioni operative di SIRENE (cooperazione transfrontaliera in relazione al SIS), sia per questioni tecniche inerenti allo sviluppo e alla manutenzione del SIS e alla relativa applicazione SIRENE. I cambiamenti proposti dal presente regolamento sono stati discussi in modo molto trasparente ed esaustivo in apposite riunioni e seminari. A livello interno la Commissione ha istituito un gruppo direttivo interservizi composto dal segretariato generale e dalle direzioni generali Migrazione e affari interni, Giustizia e consumatori, Risorse umane e sicurezza, e Informatica. Il gruppo direttivo ha monitorato il processo di valutazione e fornito orientamenti ove necessario.

3. La Commissione ha inoltre fatto ricorso a perizie esterne tramite due studi, i cui risultati sono stati inseriti negli sviluppi della presente proposta:

- Valutazione tecnica del SIS: la valutazione ha identificato i problemi principali inerenti al SIS e le future esigenze da considerare, sottolineando la necessità di aumentare la continuità operativa e di garantire che l'architettura complessiva possa adattarsi ai crescenti requisiti di capacità.

- TIC – Valutazione d'impatto di possibili miglioramenti all'architettura del SIS II: lo studio ha valutato l'attuale costo del funzionamento del SIS a livello nazionale e tre possibili soluzioni tecniche per il miglioramento del sistema; tutte le soluzioni comprendono una serie di proposte tecniche finalizzate a migliorare il sistema centrale e l'architettura generale.

1.5.4. Compatibilità ed eventuale sinergia con altri strumenti pertinenti

La presente proposta va considerata quale applicazione delle azioni contenute nella comunicazione del 6 aprile 2016 "Sistemi d'informazione più solidi e intelligenti per

le frontiere e la sicurezza"[84], in cui si sottolinea l'esigenza che l'UE rafforzi e migliori i suoi sistemi d'informazione, l'architettura dei dati e lo scambio d'informazioni nelle attività di contrasto alla criminalità, nella lotta contro il terrorismo e nella gestione delle frontiere.

La presente proposta è inoltre strettamente collegata ad altre politiche dell'Unione e le completa. Si tratta in particolare delle seguenti politiche:

a) sicurezza interna (come indicato nell'Agenda europea sulla sicurezza)[85]: prevenire, accertare e indagare reati di terrorismo e altri reati gravi permettendo alle autorità di contrasto di trattare i dati personali di persone sospettate di coinvolgimento in atti di terrorismo o in altri reati gravi;

b) protezione dei dati: la presente proposta garantisce la tutela dei diritti fondamentali delle persone i cui dati personali sono trattati nel SIS.

La proposta è altresì compatibile con la legislazione vigente dell'Unione europea, in particolare:

a) la guardia di frontiera e costiera europea[86] per quanto riguarda, in primo luogo, la possibilità per il personale dell'Agenzia di svolgere analisi dei rischi e in secondo luogo il suo accesso al SIS ai fini del proposto ETIAS. La proposta intende anche fornire un'interfaccia tecnica per l'accesso al SIS alle squadre della guardia di frontiera e costiera europea, alle squadre di personale che assolve compiti attinenti al rimpatrio e ai membri delle squadre di sostegno per la gestione delle migrazione hanno, nell'ambito dei rispettivi mandati, che acquistano il diritto di accedere ai dati inseriti nel SIS e di consultarli;

b) Europol, a cui la presente proposta accorda diritti aggiuntivi di accedere ai dati inseriti nel SIS e consultarli nell'ambito del suo mandato;

c) Prüm[87], nella misura in cui gli sviluppi previsti dalla presente proposta che consentono di identificare le persone mediante le impronte digitali (nonché le immagini facciali e i profili DNA) completano le vigenti disposizioni Prüm sull'accesso reciproco in linea transfrontaliero a banche dati nazionali designate del DNA e a sistemi automatizzati di identificazione delle impronte digitali.

La proposta è altresì compatibile con la futura legislazione dell'Unione europea, in particolare:

---

84 COM(2016) 205 final.

85 COM(2015) 185 final.

86 Regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio, del 14 settembre 2016, relativo alla guardia di frontiera e costiera europea e che modifica il regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio e che abroga il regolamento (CE) n. 863/2007 del Parlamento europeo e del Consiglio, il regolamento (CE) n. 2007/2004 del Consiglio e la decisione 2005/267/CE del Consiglio (GU L 251 del 16.9.2016, pag. 1).

87 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); e 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).

a) Gestione delle frontiere esterne: la proposta completa il nuovo principio previsto nel codice frontiere Schengen sulle verifiche sistematiche nelle banche dati pertinenti di tutti i viaggiatori, compresi i cittadini dell'UE, all'ingresso nello spazio Schengen e all'uscita dal medesimo, principio istituito in reazione al fenomeno dei terroristi combattenti stranieri.

b) Sistema di ingressi/uscite[88] (EES): la proposta cerca di riflettere l'uso proposto di una combinazione di impronte digitali e immagine facciale come identificatori biometrici per il funzionamento dell'EES.

c) ETIAS: la proposta tiene conto del proposto sistema ETIAS che prevede una valutazione accurata sotto il profilo della sicurezza, compresa una verifica nel SIS, dei cittadini di paesi terzi che intendono recarsi nell'Unione europea.

[88] Proposta di regolamento del Parlamento europeo e del Consiglio 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 dell'Unione europea e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica il regolamento (CE) n. 767/2008 (COM(2016) 194 final).

1.6. Durata e incidenza finanziaria

☐ Proposta/iniziativa di **durata limitata**

– ☐ Proposta/iniziativa in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

– ☐ Incidenza finanziaria dal AAAA al AAAA

☑ Proposta/iniziativa di **durata illimitata**

–Periodo preparatorio: 2017

– Attuazione con un periodo di avviamento dal 2018 al 2020

– e successivo funzionamento a pieno ritmo.

1.7. Modalità di gestione previste[89]

☑ **Gestione diretta** a opera della Commissione

– ☑ a opera dei suoi servizi, compreso il personale delle delegazioni dell'Unione;

– ☐ a opera delle agenzie esecutive.

☑ **Gestione concorrente** con gli Stati membri

☑ **Gestione indiretta** con compiti di esecuzione del bilancio affidati:

– ☐ a paesi terzi o organismi da questi designati;

– ☐ a organizzazioni internazionali e rispettive agenzie (specificare);

– ☐ alla BEI e al Fondo europeo per gli investimenti;

– ☑ agli organismi di cui agli articoli 208 e 209 del regolamento finanziario;

– ☐ a organismi di diritto pubblico;

– ☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui presentano sufficienti garanzie finanziarie;

– ☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che presentano sufficienti garanzie finanziarie;

– ☐ alle persone incaricate di attuare azioni specifiche nel settore della PESC a norma del titolo V del TUE, che devono essere indicate nel pertinente atto di base.

– *Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".*

[89] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

Osservazioni

Alla Commissione spetterà la gestione generale della politica ed eu-LISA sarà competente per lo sviluppo, il funzionamento e la manutenzione del sistema.

Il SIS costituisce un sistema d'informazione unico. Di conseguenza, le spese previste in due delle proposte (la presente e la proposta di regolamento sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera) non vanno considerate due importi separati ma un unico importo. L'incidenza sul bilancio delle modifiche necessarie per attuare entrambe le proposte è compresa in un'unica scheda finanziaria legislativa.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

La Commissione, gli Stati membri e l'agenzia dovranno riesaminare periodicamente e monitorare l'uso del SIS, per verificare che continui a funzionare in modo efficace ed efficiente. La Commissione sarà assistita dal comitato per l'attuazione delle misure tecniche e operative previste dalla presente proposta.

Il proposto regolamento prevede inoltre all'articolo 71, paragrafi 7 e 8, una revisione formale periodica e un processo di valutazione.

Ogni due anni eu-LISA riferirà al Parlamento europeo e al Consiglio in merito al funzionamento tecnico del SIS (compresa la sicurezza), all'infrastruttura di comunicazione su cui si basa e allo scambio bilaterale e multilaterale di informazioni supplementari fra gli Stati membri.

Inoltre, ogni quattro anni la Commissione è tenuta ad effettuare e trasmettere al Parlamento europeo e al Consiglio una valutazione globale del SIS e dello scambio di informazioni tra gli Stati membri, al fine di:

a) analizzare i risultati conseguiti in relazione agli obiettivi;

b) valutare se restino validi i principi di base del sistema;

c) esaminare il modo in cui il regolamento è applicato al sistema centrale;

d) valutare la sicurezza del sistema centrale;

e) valutare le implicazioni per il futuro funzionamento del sistema.

eu-LISA è inoltre tenuta a pubblicare statistiche giornaliere, mensili e annuali sull'uso del SIS e a provvedere al monitoraggio permanente del sistema e del suo funzionamento in relazione agli obiettivi.

2.2. Sistema di gestione e di controllo

2.2.1. Rischi individuati

Sono stati individuati i seguenti rischi:

1. eu-LISA potrebbe sperimentare difficoltà nel gestire gli sviluppi presentati nella presente proposta parallelamente agli altri sviluppi in corso (ad esempio l'attuazione del sistema AFIS nel SIS) e futuri (ad esempio il sistema di ingressi/uscite, l'ETIAS e l'aggiornamento dell'Eurodac). Questo rischio potrebbe essere attenuato garantendo che eu-LISA disponga di personale e risorse sufficienti per svolgere tali compiti e la gestione corrente del contratto di mantenimento del funzionamento operativo (MWO).

2. Difficoltà per gli Stati membri

2.1 Tali difficoltà sono innanzitutto di natura finanziaria. Ad esempio, la proposta legislativa comprende lo sviluppo obbligatorio di una copia parziale nazionale in ogni N.SIS II. Gli Stati membri che non l'hanno ancora sviluppata dovranno investire a questo scopo. Analogamente, l'attuazione nazionale del documento di controllo dell'interfaccia dovrebbe costituire un'attuazione completa. Gli Stati membri che non hanno ancora proceduto in questo senso dovranno prendere provvedimenti a tale scopo nei bilanci dei ministeri competenti. Questo rischio potrebbe essere attenuato prevedendo finanziamenti dell'UE per gli Stati membri, ad esempio a carico della componente "Frontiere" del Fondo sicurezza interna (ISF).

2.2. I sistemi nazionali devono essere allineati ai requisiti centrali e le discussioni in proposito con gli Stati membri possono ritardare l'evoluzione. Questo rischio potrebbe essere attenuato affrontando la questione per tempo con gli Stati membri in modo da poter agire al momento opportuno.

2.2.2. Informazioni riguardanti il sistema di controllo interno istituito

Le competenze relative alle componenti centrali del SIS spettano a eu-LISA. Per monitorare meglio l'uso del SIS nell'analisi delle tendenze relative alla pressione migratoria, alla gestione delle frontiere e ai reati, eu-LISA dovrebbe essere in grado di sviluppare una capacità avanzata di fornire statistiche agli Stati membri e alla Commissione.

I conti di eu-LISA saranno soggetti all'approvazione della Corte dei conti e alla procedura di scarico. Il servizio di audit interno della Commissione svolgerà i suoi audit in cooperazione con il revisore interno di eu-LISA.

2.2.3. Stima dei costi e dei benefici dei controlli e valutazione del previsto livello di rischio di errore

n.p.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste.

Le misure previste per combattere le frodi, previste all'articolo 35 del regolamento (UE) n. 1077/2011, sono le seguenti.

1. Ai fini della lotta contro la frode, la corruzione e ogni altra attività illecita si applica il regolamento (CE) n. 1073/1999.

2. L'agenzia aderisce all'accordo interistituzionale relativo alle indagini interne svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e adotta immediatamente le opportune disposizioni, applicabili a tutto il suo personale.

3. Le decisioni concernenti il finanziamento e i correlati accordi e strumenti di attuazione stabiliscono espressamente che la Corte dei conti e l'OLAF possono svolgere, se necessario, controlli in loco presso i beneficiari dei finanziamenti dell'agenzia e gli agenti responsabili della loro assegnazione.

Conformemente a tale disposizione, il 28 giugno 2012 è stata adottata la decisione del consiglio di amministrazione dell'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia relativa ai termini e alle condizioni delle indagini interne in materia di lotta contro le frodi, la corruzione e ogni altra attività illecita lesiva degli interessi finanziari degli interessi finanziari dell'Unione.

Si applicherà la strategia della DG HOME in materia di prevenzione e individuazione delle frodi.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio esistenti

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Rubrica 3 – Sicurezza e cittadinanza	Diss./Non diss[90].	di paesi EFTA[91]	di paesi candidati[92]	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
	18.0208 – Sistema di informazione Schengen	Diss.	NO	NO	SÌ	NO
	18.020101 – Sostegno alla gestione delle frontiere e a una politica comune dei visti per facilitare la libera circolazione delle persone per scopi legittimi	Diss.	NO	NO	SÌ	NO
	18.0207 – Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA).	Diss.	NO	NO	SÌ	NO

[90] Diss. = stanziamenti dissociati / Non-diss. = stanziamenti non dissociati.
[91] EFTA: Associazione europea di libero scambio.
[92] Paesi candidati e, se del caso, paesi potenziali candidati dei Balcani occidentali.

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

Rubrica del quadro finanziario pluriennale	3	Sicurezza e cittadinanza

DG HOME			Anno **2018**	Anno **2019**	Anno **2020**	**TOTALE**
• Stanziamenti operativi						
18.0208 – Sistema di informazione Schengen	Impegni	(1)	6,234	1,854	1,854	**9,942**
	Pagamenti	(2)	6,234	1,854	1,854	**9,942**
18.020101 (Frontiere e visti)	Impegni	(1)		18,405	18,405	**36,810**
	Pagamenti	(2)		18,405	18,405	**36,810**
TOTALE degli stanziamenti per la DG HOME	Impegni	=1+1a +3	6,234	20,259	20,259	**46,752**
	Pagamenti	=2+2a +3	6,234	20,259	20,259	**46,752**

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	3	Sicurezza e cittadinanza

eu-LISA			Anno **2018**	Anno **2019**	Anno **2020**	**TOTALE**
• Stanziamenti operativi						
Titolo 1: Spese di personale	Impegni	(1)	0,210	0,210	0,210	**0,630**
	Pagamenti	(2)	0,210	0,210	0,210	**0,630**
Titolo 2: Spesa per infrastrutture e spesa di funzionamento	Impegni	(1a)	0	0	0	**0**
	Pagamenti	(2a)	0	0	0	**0**
Titolo 3: Spese operative	Impegni	(1a)	12,893	2,051	1,982	**16,926**
	Pagamenti	(2a)	2,500	7,893	4,651	**15,044**
TOTALE degli stanziamenti per eu-LISA	Impegni	=1+1a +3	13,103	2,261	2,192	**17,556**
	Pagamenti	=2+2a +3	2,710	8,103	4,861	**15,674**

3.2.2. Incidenza prevista sugli stanziamenti operativi

• TOTALE degli stanziamenti operativi	Impegni	(4)								
	Pagamenti	(5)								

• TOTALE degli stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici		(6)								
TOTALE degli stanziamenti per la RUBRICA <….> del quadro finanziario pluriennale	Impegni	=4+ 6								
	Pagamenti	=5+ 6								

Se la proposta/iniziativa incide su più rubriche:

• TOTALE degli stanziamenti operativi	Impegni	(4)							
	Pagamenti	(5)							
• TOTALE degli stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici		(6)							
TOTALE degli stanziamenti per le RUBRICHE da 1 a 4 del quadro finanziario pluriennale (importo di riferimento)	Impegni	=4+ 6	19,337	22,520	22,451				**64,308**
	Pagamenti	=5+ 6	8,944	28,362	25,120				**62,426**

3.2.3. Incidenza prevista sugli stanziamenti di natura amministrativa

Rubrica del quadro finanziario pluriennale	**5**	"Spese amministrative"

		Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			**TOTALE**
DG: <…….>									
•Risorse umane									
•Altre spese amministrative									
TOTALE DG <…….>	Stanziamenti								

Mio EUR (al terzo decimale)

TOTALE degli stanziamenti per la RUBRICA 5 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)								

Mio EUR (al terzo decimale)

		Anno **N**[93]	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			**TOTALE**
TOTALE degli stanziamenti per le RUBRICHE da 1 a 5 del quadro finanziario pluriennale	Impegni								
	Pagamenti								

[93] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa.

3.2.3.1. Incidenza prevista sugli stanziamenti della DG HOME

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

– ☑ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Specificare gli obiettivi e i risultati			Anno **2018**		Anno **2019**		Anno **2020**		Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)						**TOTALE**			
	RISULTATI																	
⇩	Tipo[94]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[95] Sviluppo del sistema nazionale			1		1	1,221	1	1,221										2,442
OBIETTIVO SPECIFICO 2 Infrastrutture			1		1	17,184	1	17,184										34,368
COSTO TOTALE						18,405		18,405										36,810

94 I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strade costruiti ecc.).

95 Come descritto nella sezione 1.4.2. "Obiettivi specifici ...".

3.2.3.2. Incidenza prevista sugli stanziamenti operativi di eu-LISA

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

– ☑ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati			Anno **2018**		Anno **2019**		Anno **2020**		Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)						**TOTALE**			
	RISULTATI																	
⇩	Tipo[96]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[97] Sviluppo sistema centrale																		
- Appaltatore			1	5,013														5,013
- Software			1	4,050														4,050
- Hardware			1	3,692														3,692
Totale parziale dell'obiettivo specifico 1				12,755														12,755
OBIETTIVO SPECIFICO 2 Manutenzione sistema centrale																		
- Appaltatore			1	0	1	0,365	1	0,365										0,730
Software			1	0	1	0,810	1	0,810										1,620

[96] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strade costruiti ecc.).

[97] Come descritto nella sezione 1.4.2. "Obiettivi specifici ...".

Hardware			1	0	1	0,738	1	0,738										1,476
Totale parziale dell'obiettivo specifico 2						1,913		1,913										3,826
OBIETTIVO SPECIFICO 3 Riunioni/formazione																		
Attività di formazione			1	0,138	1	0,138	1	0,069										0,345
Totale parziale dell'obiettivo specifico 3				0,138		0,138		0,069										0,345
Costo totale				12,893		2,051		1,982										16,926

3.2.3.3. Incidenza prevista sulle risorse umane di eu-LISA

Sintesi

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti di natura amministrativa.

– ☑ La proposta/iniziativa comporta l'utilizzo di stanziamenti di natura amministrativa, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **2018**	Anno **2019**	Anno **2020**	**TOTALE**
Funzionari (gradi AD)				
Funzionari (gradi AST)				
Agenti contrattuali	0,210	0,210	0,210	0,630
Agenti temporanei				
Esperti nazionali distaccati				
TOTALE	**0,210**	**0,210**	**0,210**	**0,630**

Le assunzioni sono previste per gennaio 2018. Tutto il personale dev'essere disponibile a partire da inizio 2018 per consentire di iniziare lo sviluppo in tempo utile affinché la rifusione del SIS II entri in funzione nel 2020. I 3 nuovi agenti contrattuali sono necessari per sopperire alle esigenze relative all'attuazione del progetto e per il sostegno operativo e la manutenzione dopo l'inizio della produzione. Tali risorse saranno impiegate per:

- sostenere l'attuazione del progetto in qualità di membri del team di progetto, con attività come: definizione di requisiti e specifiche tecniche, cooperazione e sostegno agli Stati membri nella fase di attuazione, aggiornamento del documento di controllo dell'interfaccia (ICD), monitoraggio delle forniture contrattuali, la consegna della documentazione ecc.;

- sostegno alle attività di transizione per rendere operativo il sistema in cooperazione con l'appaltatore (follow-up delle versioni, aggiornamenti del processo operativo, formazioni, comprese le attività di formazione degli Stati membri) ecc.;

- sostegno alle attività a più lungo termine, definizione delle specifiche, attività di preparazione contrattuale in caso di variazione dell'ingegneria del sistema (ad esempio per il riconoscimento d'immagini) o qualora il contratto di mantenimento

del funzionamento operativo (MWO) del nuovo SIS debba essere modificato per tener conto di cambiamenti aggiuntivi (di ordine tecnico e di bilancio);

- attuazione del sostegno di secondo livello in seguito all'entrata in funzione, nel corso della manutenzione continua e delle operazioni.

Va notato che le tre nuove risorse (agenti contrattuali ETP) si aggiungeranno alle risorse interne delle squadre che saranno anch'esse dedicate alle attività progettuali/contrattuali e di follow-up finanziario/operative. Grazie al ricorso ad agenti contrattuali i contratti avranno durata e continuità adeguate per garantire la continuità operativa e le stesse persone specializzate potranno essere impiegate per attività di sostegno operativo dopo la conclusione del progetto. Inoltre, le attività di sostegno operativo richiedono l'accesso all'ambiente di produzione che non può essere accordato a personale a contratto o personale esterno.

3.2.3.4. Fabbisogno previsto di risorse umane

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

– ☐ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in equivalenti a tempo pieno

	Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)		
• Posti della tabella dell'organico (funzionari e agenti temporanei)							
XX 01 01 01 (in sede e negli uffici di rappresentanza della Commissione)							
XX 01 01 02 (delegazioni)							
XX 01 05 01 (ricerca indiretta)							
10 01 05 01 (ricerca diretta)							
• Personale esterno (in equivalenti a tempo pieno: ETP)[98]							
XX 01 02 01 (AC, END e INT della dotazione globale)							
XX 01 02 02 (AC, AL, END, INT e JED nelle delegazioni)							
XX 01 04 **yy** [99] - in sede							
XX 01 04 **yy** [99] - nelle delegazioni							
XX 01 05 02 (AC, END e INT – ricerca indiretta)							
10 01 05 02 (AC, END e INT – ricerca diretta)							
Altre linee di bilancio (specificare)							
TOTALE							

XX è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	
Personale esterno	

98 AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JED = giovane esperto in delegazione (jeune expert en délégation).

99 Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

– ☐ La proposta/iniziativa è compatibile con il quadro finanziario pluriennale attuale.

– ☑ La proposta/iniziativa richiede una riprogrammazione della pertinente rubrica del quadro finanziario pluriennale.

È prevista una riprogrammazione della dotazione rimanente per le "Frontiere intelligenti" del Fondo sicurezza interna, per applicare le funzionalità e le modifiche contenute nelle due proposte. Il regolamento ISF-Frontiere è lo strumento finanziario in cui è stato inserito il bilancio per l'attuazione del pacchetto "Frontiere intelligenti". All'articolo 5 esso prevede che 791 milioni di EUR siano destinati a un programma per lo sviluppo di sistemi informatici a sostegno della gestione dei flussi migratori attraverso le frontiere esterne alle condizioni previste all'articolo 15. Di questi 791 milioni di EUR, 480 sono riservati allo sviluppo del sistema di ingressi/uscite e 210 allo sviluppo del sistema europeo di informazione e autorizzazione ai viaggi (ETIAS). I restanti 100,828 milioni di EUR saranno usati in parte per coprire i costi dei cambiamenti relativi al miglioramento delle funzionalità del SIS II, previsti nelle due proposte.

– ☐ La proposta/iniziativa richiede l'applicazione dello strumento di flessibilità o la revisione del quadro finanziario pluriennale.

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate e gli importi corrispondenti.

3.2.5. Partecipazione di terzi al finanziamento

– ☑La proposta/iniziativa non prevede cofinanziamenti da terzi.

– La proposta/iniziativa prevede il cofinanziamento indicato di seguito:

Stanziamenti in Mio EUR (al terzo decimale)

	Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			Totale
Specificare l'organismo di cofinanziamento								
TOTALE degli stanziamenti cofinanziati								

3.3. Incidenza prevista sulle entrate

– ☐ La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

– ☑ La proposta/iniziativa ha la seguente incidenza finanziaria:

– – ☐ sulle risorse proprie

– – ☑ sulle entrate varie

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Stanziamenti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa[100]						
		2018	2019	2020	2021	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)		
Articolo 6313 – contributi dei paesi associati a Schengen (CH, NO, LI, IS).		p.m.	p.m.	p.m.	p.m.			

Per quanto riguarda le entrate varie con destinazione specifica, precisare la o le linee di spesa interessate.

18.02.08 (sistema d'informazione Schengen), 18.02.07 (eu-LISA)

Precisare il metodo di calcolo dell'incidenza sulle entrate.

Il bilancio comprende un contributo da parte dei paesi associati all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen.

[100] Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 25% per spese di riscossione.