REGOLAMENTO (UE) 2018/1862 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 28 novembre 2018

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

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 ([1]),

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, sostenendo la cooperazione operativa tra le autorità nazionali competenti, in particolare guardie di frontiera, autorità di polizia e doganali, autorità competenti per l'immigrazione e autorità competenti a fini di prevenzione, accertamento, indagine o perseguimento di reati o esecuzione di sanzioni penali.

(2) Inizialmente 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 ([2]), firmata il 19 giugno 1990 (la «convenzione di applicazione dell'accordo di Schengen»). L'incarico di sviluppare il SIS di seconda generazione (SIS II) è stato affidato alla Commissione in virtù del regolamento (CE) n. 2424/2001 del Consiglio ([3]) e della decisione 2001/886/GAI del Consiglio ([4]). Il SIS II è stato successivamente istituito con regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio ([5]) e con la decisione 2007/533/GAI del Consiglio ([6]). Il SIS II ha sostituito il SIS istituito sulla base della convenzione di applicazione dell'accordo di Schengen.

(3) Tre anni dopo l'entrata in funzione del SIS II, la Commissione ha svolto una valutazione del sistema ai sensi del regolamento (CE) n. 1987/2006 e della decisione 2007/533/GAI. Il 21 dicembre 2016 la Commissione ha presentato la relazione di valutazione del Sistema d'informazione Schengen di seconda generazione (SIS II) conformemente 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 66, paragrafo 5, della decisione 2007/533/GAI, unitamente a un documento di lavoro dei servizi del Parlamento europeo e del Consiglio. Le raccomandazioni espresse in tali documenti dovrebbero essere recepite, se del caso, nel presente regolamento.

(4) Il presente regolamento costituisce la base giuridica per il SIS nelle materie rientranti nell'ambito di applicazione della parte terza, titolo V, capi 4 e 5, del trattato sul funzionamento dell'Unione europea (TFUE). Il regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio ([7]) costituisce la base giuridica per il SIS nelle materie rientranti nell'ambito di applicazione della parte terza, titolo V, capo 2, TFUE.

([1]) Posizione del Parlamento europeo del 24 ottobre 2018 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 19 novembre 2018.

([2]) GU L 239 del 22.9.2000, pag. 19.

([3]) Regolamento (CE) n. 2424/2001 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. 4).

([4]) 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).

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

([6]) 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).

([7]) Regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006 (cfr. pagina 14 della presente Gazzetta ufficiale).

(5) Il fatto che la base giuridica per il SIS consti di strumenti distinti non pregiudica il principio secondo il quale il SIS costituisce un unico sistema d'informazione che dovrebbe operare in quanto tale. Esso dovrebbe includere un'unica rete di uffici nazionali denominati uffici SIRENE al fine di garantire lo scambio di informazioni supplementari. È pertanto opportuno che alcune disposizioni di tali strumenti siano identiche.

(6) È necessario specificare gli obiettivi del SIS, alcuni elementi della sua architettura tecnica e del suo finanziamento, fissare regole relative al suo esercizio e uso da un'estremità all'altra e definire le competenze. È altresì necessario determinare le categorie di dati da inserire nel sistema, le finalità dell'inserimento e del trattamento dei dati e i relativi criteri. Sono altresì necessarie norme concernenti la cancellazione delle segnalazioni, le autorità abilitate ad accedere ai dati, l'uso di dati biometrici, nonché norme che specifichino ulteriormente le norme sulla protezione dei dati e sul trattamento dei dati.

(7) Le segnalazioni nel SIS contengono solo le informazioni necessarie per identificare una persona o un oggetto e l'azione da intraprendere. Pertanto, gli Stati membri dovrebbero, all'occorrenza, scambiare informazioni supplementari relative alle segnalazioni.

(8) Il SIS consta di un sistema centrale (SIS centrale) e di sistemi nazionali. I sistemi nazionali potrebbero contenere una copia completa o parziale della banca dati del SIS che può essere condivisa da due o più Stati membri. Poiché il SIS è il più importante strumento di scambio di informazioni in Europa volto a garantire la sicurezza e una gestione efficace delle frontiere, è necessario garantirne il funzionamento ininterrotto a livello sia centrale sia nazionale. La disponibilità del SIS dovrebbe essere soggetta a un attento monitoraggio a livello centrale e degli Stati membri e ogni incidente che implichi un'indisponibilità per gli utenti finali dovrebbe essere registrato e comunicato ai portatori di interesse a livello nazionale e dell'Unione. Ogni Stato membro dovrebbe creare una copia di riserva (backup) per il proprio sistema nazionale. Gli Stati membri dovrebbero inoltre garantire una connettività senza interruzioni al SIS centrale con punti di connessione duplicati e separati fisicamente e geograficamente. Il SIS centrale e l'infrastruttura di comunicazione dovrebbero essere gestiti in modo da assicurarne il funzionamento 24 ore su 24 e 7 giorni su 7. Per questo motivo, l'agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia («eu-LISA»), istituita dal regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio [1] dovrebbe mettere in atto soluzioni tecniche volte a rafforzare la disponibilità ininterrotta del SIS, fatte salve una valutazione d'impatto indipendente e un'analisi costi-benefici.

(9) È necessario tenere un manuale aggiornato recante le modalità dettagliate di scambio di informazioni supplementari relative alle azioni da intraprendere in seguito alle segnalazioni (il «manuale SIRENE»). Gli uffici SIRENE dovrebbero garantire lo scambio di tali informazioni in modo rapido ed efficace.

(10) Per provvedere a uno scambio efficace di informazioni supplementari, anche riguardo alle 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.

(11) Gli Stati membri dovrebbero assicurare che il personale del proprio ufficio SIRENE possieda le competenze linguistiche e la conoscenza del diritto e delle norme procedurali pertinenti necessarie allo svolgimento dei suoi compiti.

(12) Per poter beneficiare pienamente delle funzionalità del SIS, gli Stati membri dovrebbero provvedere a che gli utenti finali e il personale degli uffici SIRENE ricevano periodicamente una formazione, anche in materia di sicurezza e protezione dei dati nonché di qualità dei dati. Gli uffici SIRENE dovrebbero essere coinvolti nell'elaborazione dei programmi di formazione. Per quanto possibile, gli uffici SIRENE dovrebbero inoltre prevedere scambi di personale con altri uffici SIRENE almeno una volta all'anno. Gli Stati membri sono incoraggiati ad adottare misure adeguate per evitare che la rotazione del personale comporti perdite di competenze e di esperienza.

(13) La gestione operativa delle componenti centrali del SIS è esercitata dall'eu-LISA. Per consentire all'eu-LISA di dedicare le risorse finanziarie e umane necessarie a coprire tutti gli aspetti della gestione operativa del SIS centrale e dell'infrastruttura di comunicazione, il presente regolamento dovrebbe stabilirne dettagliatamente i compiti, in particolare riguardo agli aspetti tecnici dello scambio di informazioni supplementari.

(14) Fatti salvi la responsabilità degli Stati membri riguardo all'esattezza dei dati inseriti nel SIS e il ruolo degli uffici SIRENE quali coordinatori della qualità, l'eu-LISA dovrebbe assumere la competenza di migliorare la qualità dei dati introducendo uno strumento di monitoraggio centrale della qualità dei dati e dovrebbe presentare a intervalli

[1] Regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo all'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), che modifica il regolamento (CE) n. 1987/2006 e la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (UE) n. 1077/2011 (GU L 295 del 21.11.2018, pag. 99).

regolari relazioni alla Commissione e agli Stati membri. La Commissione dovrebbe riferire al Parlamento europeo e al Consiglio sui problemi di qualità dei dati incontrati. Per migliorare ulteriormente la qualità dei dati inseriti nel SIS, l'eu-LISA dovrebbe inoltre offrire una formazione sull'uso del SIS agli organismi nazionali di formazione e, nella misura del possibile, agli uffici SIRENE e agli utenti finali.

(15) Per consentire di monitorare meglio l'uso del SIS e analizzare le tendenze relative ai reati, l'eu-LISA dovrebbe essere in grado di sviluppare una capacità avanzata di fornire statistiche agli Stati membri, al Parlamento europeo, al Consiglio, alla Commissione, a Europol, a Eurojust e all'Agenzia europea della guardia di frontiera e costiera, senza compromettere l'integrità dei dati. È opportuno pertanto istituire un archivio centrale. Le statistiche contenute nell'archivio o prodotte dallo stesso non dovrebbero contenere dati personali. Nell'ambito della cooperazione tra le autorità di controllo e il garante europeo della protezione dei dati ai sensi del presente regolamento, gli Stati membri dovrebbero comunicare statistiche relative all'esercizio del diritto di accesso, rettifica di dati inesatti e cancellazione di dati archiviati illecitamente.

(16) È opportuno introdurre nuove categorie di dati nel SIS per consentire agli utenti finali di adottare decisioni informate sulla base di una segnalazione senza perdere tempo. Di conseguenza, per facilitare l'identificazione delle persone e individuare i casi di identità molteplici, la segnalazione dovrebbe includere, se tale informazione fosse disponibile, un riferimento al documento d'identificazione personale della persona interessata o al numero di identificazione personale e una copia, possibilmente a colori, di tale documento.

(17) Le autorità competenti dovrebbero avere la possibilità, se strettamente necessario, di inserire nel SIS informazioni specifiche relative a qualsiasi caratteristica fisica particolare, oggettiva e inalterabile di una persona, quali tatuaggi, cicatrici o altri segni.

(18) Laddove disponibili, tutti i dati pertinenti, in particolare il nome della persona interessata, dovrebbero essere inseriti in fase di creazione di una segnalazione, per ridurre al minimo il rischio di falsi riscontri positivi (hit) e attività operative non necessarie.

(19) 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 dei sistemi nazionali nonchè l'integrità e la sicurezza dei dati.

(20) Per contribuire alla corretta identificazione degli interessati, il SIS dovrebbe consentire il trattamento di dati biometrici. Qualsiasi inserimento nel SIS di fotografie, immagini del volto o dati dattiloscopici, così come l'utilizzo di tali dati, dovrebbe essere limitato a quanto necessario ai fini degli obiettivi perseguiti, dovrebbe essere autorizzato dal diritto dell'Unione, dovrebbe avvenire nel rispetto dei diritti fondamentali, in particolare dell'interesse superiore del minore, e dovrebbe essere conforme alla normativa dell'Unione in materia di protezione dei dati, ivi incluse le pertinenti disposizioni sulla protezione dei dati previste dal presente regolamento. Nella stessa ottica, per evitare i disagi causati da errori di identificazione, il SIS dovrebbe inoltre consentire il trattamento di dati relativi a persone la cui identità è stata usurpata, nel rispetto di adeguate garanzie, quale il consenso dell'interessato per ciascuna categoria di dati, in particolare per le impronte palmari, e la rigorosa limitazione delle finalità per cui tali dati personali possono essere lecitamente trattati.

(21) Gli Stati membri dovrebbero adottare le disposizioni tecniche necessarie affinché gli utenti finali, ogni volta che sono autorizzati a consultare una banca dati della polizia nazionale o dell'immigrazione, consultino parallelamente anche il SIS nel rispetto dei principi di cui all'articolo 4 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([1]) e all'articolo 5 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([2]). 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.

(22) È opportuno che il presente regolamento stabilisca le condizioni per l'uso dei dati dattiloscopici, delle fotografie e delle immagini del volto a fini di identificazione e di verifica. L'uso di immagini del volto e di fotografie a fini di identificazione dovrebbe inizialmente aver luogo solo presso i valichi di frontiera regolari. Tale uso dovrebbe essere oggetto di una relazione della Commissione che confermi che la tecnologia necessaria è disponibile, pronta ad essere usata e affidabile.

([1]) 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).

([2]) 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).

(23) L'introduzione di un servizio automatizzato di identificazione delle impronte digitali nel SIS integra l'attuale meccanismo di Prüm sul reciproco accesso in linea transfrontaliero a banche dati nazionali del DNA designate e a sistemi automatizzati per il riconoscimento delle impronte digitali, di cui alla decisione 2008/615/GAI del Consiglio ([1]) e alla decisione 2008/616/GAI del Consiglio ([2]). L'interrogazione dei dati dattiloscopici del SIS permette di ricercare attivamente l'autore di un reato. Dovrebbe quindi essere possibile caricare i dati dattiloscopici dell'autore ignoto di un reato nel SIS, purché la persona a cui appartengono quei dati possa essere identificata con un grado di probabilità molto elevato come autore di un reato grave o di un atto di terrorismo. Ciò vale in particolare nei casi in cui sono rilevati dati dattiloscopici su un'arma o altro corpo del reato. La mera presenza di dati dattiloscopici sul luogo del reato non dovrebbe essere considerata indicazione di un grado di probabilità molto elevato che i dati dattiloscopici siano quelli dell'autore del reato. Un'ulteriore condizione per effettuare tale segnalazione dovrebbe consistere nell'impossibilità di stabilire l'identità del sospettato sulla base di dati di altre pertinenti banche dati nazionali, dell'Unione o internazionali. Se dalla consultazione dei dati dattiloscopici dovesse risultare una potenziale corrispondenza, lo Stato membro dovrebbe svolgere ulteriori verifiche con la partecipazione di esperti, per stabilire se le impronte conservate nel SIS appartengano alla persona in questione, di cui dovrebbe altresì stabilire l'identità. La procedura dovrebbe essere soggetta al diritto nazionale. Una tale identificazione potrebbe contribuire notevolmente all'indagine e portare all'arresto se ne sussistono tutte le condizioni.

(24) È opportuno permettere di ricercare dati dattiloscopici conservati nel SIS con serie complete o incomplete di impronte digitali o impronte palmari rilevate sul luogo di un reato se si può stabilire con un grado molto elevato di probabilità che appartengono all'autore di un reato grave o di un reato di terrorismo,purché un'interrogazione sia effettuata simultaneamente nelle pertinenti banche dati nazionali di impronte digitali. È opportuno rivolgere un'attenzione particolare alla definizione di norme di qualità applicabili alla conservazione dei dati biometrici, inclusi i dati dattiloscopici latenti.

(25) Allorché l'identità di una persona non possa essere accertata con altri mezzi, si dovrebbero utilizzare i dati dattiloscopici per l'identificazione. Dovrebbe essere consentito in tutti i casi identificare una persona utilizzando dati dattiloscopici.

(26) Dovrebbe essere possibile aggiungere un profilo DNA ad una segnalazione in casi ben definiti in cui i dati dattiloscopici non siano disponibili. Tale profilo DNA dovrebbe essere accessibile soltanto agli utenti autorizzati. I profili DNA dovrebbero facilitare l'identificazione di persone scomparse bisognose di protezione e specialmente di minori scomparsi, in particolare autorizzando l'uso di profili DNA di ascendenti e discendenti diretti, o fratelli e sorelle per consentire l'identificazione. I dati DNA dovrebbero contenere solo le informazioni minime necessarie per l'identificazione della persona scomparsa.

(27) I profili DNA dovrebbero essere estratti dal SIS esclusivamente quando l'identificazione sia necessaria e proporzionata ai fini previsti dal presente regolamento. I profili DNA non dovrebbero essere estratti o trattati per finalità diverse da quelle per le quali sono stati inseriti nel SIS. Dovrebbero applicarsi le disposizioni sulla protezione dei dati e sulla sicurezza previste dal presente regolamento. Quando si utilizzano profili DNA si dovrebbero, se necessario, predisporre salvaguardie aggiuntive al fine di evitare i rischi di false corrispondenze, accessi abusivi e condivisione non autorizzata con parti terze.

(28) Il SIS dovrebbe contenere segnalazioni di persone ricercate per l'arresto a fini di consegna e ricercate per l'arresto a fini di estradizione. Oltre alle segnalazioni, è opportuno prevedere lo scambio tramite gli uffici SIRENE di informazioni supplementari necessarie ai fini delle procedure di consegna ed estradizione. In particolare, è opportuno che i dati di cui all'articolo 8 della decisione quadro 2002/584/GAI del Consiglio ([3]) siano trattati nel SIS. 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 oggetto del mandato d'arresto europeo sia intensamente e attivamente ricercata e gli utenti finali che non partecipano alla concreta operazione di ricerca rischino di comprometterne il successo. In linea di principio, la temporanea sospensione della disponibilità di tali segnalazioni non dovrebbe superare le 48 ore.

(29) È opportuno prevedere 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.

([1]) 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).

([2]) 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).

([3]) 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).

(30) Il SIS dovrebbe contenere segnalazioni di persone scomparse o di persone vulnerabili a cui deve essere impedito di viaggiare al fine di tutelarle o di prevenire minacce alla pubblica sicurezza o all'ordine pubblico. Quando si tratta di minori, tali segnalazioni e le corrispondenti procedure dovrebbero tener conto dell'interesse superiore del minore, in conformità dell'articolo 24 della Carta dei diritti fondamentali dell'Unione europea e dell'articolo 3 della Convenzione delle Nazioni Unite sui diritti del fanciullo del 20 novembre 1989. Le azioni e le decisioni delle autorità competenti, comprese le autorità giudiziarie, in seguito alla segnalazione di un minore dovrebbero essere adottate in cooperazione con le autorità per la tutela dei minori. È opportuno, se del caso, informare la linea nazionale di assistenza telefonica diretta per minori scomparsi.

(31) Le segnalazioni di persone scomparse che devono essere poste sotto protezione dovrebbero essere inserite su richiesta dell'autorità competente. Tutti i minori scomparsi dalle strutture di accoglienza degli Stati membri dovrebbero essere oggetto di segnalazione nel SIS come persone scomparse.

(32) Le segnalazioni di minori a rischio di sottrazione da parte di uno dei genitori dovrebbero essere inserite nel SIS su richiesta delle autorità competenti, incluse le autorità giudiziarie competenti in materia di responsabilità genitoriale conformemente al diritto nazionale. Le segnalazioni di minori a rischio di sottrazione da parte di uno dei genitori dovrebbero essere inserite nel SIS laddove tale rischio sia concreto ed evidente, e in limitate circostanze. É pertanto necessario prevedere garanzie rigorose e adeguate. Nel verificare se sussista un rischio concreto ed evidente che un minore possa essere fatto uscire in modo illecito e imminente da uno Stato membro, l'autorità competente dovrebbe tenere conto della situazione personale del minore e dell'ambiente a cui è esposto.

(33) Il presente regolamento dovrebbe stabilire una nuova categoria di segnalazioni per determinate categorie di persone vulnerabili a cui deve essere impedito di viaggiare. Dovrebbero essere considerate persone vulnerabili le persone che, a causa della loro età, disabilità, o circostanze familiari, necessitano di tutela.

(34) Le segnalazioni di minori a cui, ai fini della loro tutela, deve essere impedito di viaggiare dovrebbero essere inserite nel SIS in caso di rischio concreto ed evidente che essi siano fatti uscire dal territorio di uno Stato membro o che lo lascino. Tali segnalazioni dovrebbero essere inserite nel caso in cui il viaggio li esponga al rischio di diventare vittime della tratta di esseri umani o di matrimonio forzato, di mutilazione genitale femminile o altre forme di violenza di genere, o di diventare vittime di reati di terrorismo o di esservi coinvolti, o di essere reclutati o arruolati in gruppi armati, o di essere costretti a partecipare attivamente ad ostilità.

(35) Le segnalazioni di adulti vulnerabili a cui, ai fini della loro tutela, deve essere impedito di viaggiare, dovrebbero essere inserite qualora il viaggio li esponga al rischio di diventare vittime della tratta di esseri umani o di violenza di genere.

(36) Al fine di garantire salvaguardie rigorose e appropriate le segnalazioni di minori o altre persone vulnerabili a cui deve essere impedito di viaggiare dovrebbero, se richiesto a norma del diritto nazionale, essere inserite nel SIS in seguito ad una decisione di un'autorità giudiziaria o ad una decisione di un'autorità competente confermata da un'autorità giudiziaria.

(37) È opportuno introdurre una nuova azione da intraprendere per consentire di fermare e interrogare una persona al fine di fornire allo Stato membro segnalante le informazioni più precise possibili. Tale azione dovrebbe essere applicata per i casi in cui, sulla base di indizi concreti, si sospetti che una persona intenda commettere o abbia commesso uno dei reati di cui all'articolo 2, paragrafi 1 e 2, della decisione quadro 2002/584/GAI qualora siano necessarie informazioni supplementari per eseguire una pena detentiva o una misura di sicurezza privativa della libertà nei confronti di una persona condannata per uno dei reati di cui all'articolo 2, paragrafi 1 e 2, della decisione quadro 2002/584/GAI, o qualora vi sia motivo di ritenere che intenda commettere uno di tali reati. Tale azione da intraprendere dovrebbe, inoltre, lasciare impregiudicati i meccanismi di assistenza giudiziaria reciproca esistenti. Essa dovrebbe fornire informazioni sufficienti per decidere se intraprendere ulteriori azioni. Questa nuova azione non dovrebbe comportare la perquisizione o l'arresto della persona. I diritti procedurali di indagati e imputati a norma del diritto dell'Unione e nazionale dovrebbero essere preservati, compreso il loro diritto ad avvalersi di un difensore in conformità della direttiva 2013/48/UE del Parlamento europeo e del Consiglio ([1]).

(38) Nel caso di segnalazioni di oggetti a fini di sequestro o di prova in un procedimento penale, gli oggetti in questione dovrebbero essere sequestrati in conformità del diritto nazionale che stabilisce se e a quali condizioni un oggetto debba essere sequestrato, in particolare se è in possesso del suo legittimo proprietario.

(39) Il SIS dovrebbe contenere nuove categorie di oggetti di valore elevato, quali prodotti informatici, che possono essere identificati e consultati con un numero di identificazione unico.

([1]) Direttiva 2013/48/UE del Parlamento europeo e del Consiglio, del 22 ottobre 2013, relativa al diritto di avvalersi di un difensore nel procedimento penale e nel procedimento di esecuzione del mandato d'arresto europeo, al diritto di informare un terzo al momento della privazione della libertà personale e al diritto delle persone private della libertà personale di comunicare con terzi e con le autorità consolari (GU L 294 del 6.11.2013, pag. 1).

(40) Per quanto concerne le segnalazioni inserite nel SIS sui documenti a fini di sequestro o di prova in un procedimento penale, il termine «falso» dovrebbe essere inteso come riferito sia ai documenti falsi sia a quelli contraffatti.

(41) Gli Stati membri dovrebbero avere la possibilità di apporre su una segnalazione un'indicazione detta «indicatore di validità», affinché non sia eseguita sul proprio territorio l'azione richiesta dalla segnalazione. Nel caso di segnalazioni inserite a scopo di arresto a fini di consegna nulla nel presente regolamento dovrebbe essere interpretato come una deroga alle disposizioni della decisione quadro 2002/584/GAI o ostativo alla loro applicazione. La decisione di apporre un indicatore di validità su una segnalazione in vista della non esecuzione di un mandato d'arresto europeo dovrebbe essere basata unicamente sui motivi di rifiuto previsti dalla suddetta decisione quadro.

(42) 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, il luogo di soggiorno della persona 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.

(43) Gli Stati membri dovrebbero avere la possibilità di stabilire connessioni fra le segnalazioni nel SIS. La creazione di connessioni fra due o più segnalazioni non dovrebbe incidere sull'azione da intraprendere, né sui termini di riesame della segnalazione o sui diritti di accesso alle segnalazioni.

(44) Le segnalazioni non dovrebbero essere conservate nel SIS oltre il periodo necessario per la realizzazione delle finalità specifiche per le quali sono state inserite. I periodi di riesame delle diverse categorie di segnalazioni dovrebbero essere adeguati in considerazione delle loro finalità. Le segnalazioni di oggetti collegate alla segnalazione di una persona dovrebbero essere conservate solo finché è conservata la segnalazione di persona. La decisione di conservare le segnalazioni di persone dovrebbe essere basata su una valutazione individuale approfondita. Gli Stati membri dovrebbero riesaminare le segnalazioni di persone e oggetti entro i periodi di riesame prestabiliti e dovrebbero tenere statistiche sul numero di segnalazioni per le quali il periodo di conservazione è stato prorogato.

(45) L'inserimento di una segnalazione nel SIS e la proroga della data di scadenza di una segnalazione nel SIS dovrebbero essere soggetti a un requisito di proporzionalità, che consiste nel verificare se l'adeguatezza, la pertinenza e l'importanza del caso giustifichino l'inserimento della segnalazione nel SIS. Nell'ipotesi di reati di terrorismo, il caso dovrebbe essere ritenuto adeguato, pertinente e sufficientemente importante da giustificare l'esistenza di una segnalazione nel SIS. Per motivi di sicurezza pubblica o nazionale, gli Stati membri dovrebbero poter eccezionalmente astenersi dall'inserire una segnalazione nel SIS qualora la stessa rischi di ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari.

(46) È necessario stabilire regole sulla cancellazione delle segnalazioni. Una segnalazione dovrebbe essere conservata solo per il periodo necessario a realizzare la finalità per la quale è stata inserita. Poiché gli Stati membri seguono pratiche diverse per stabilire il momento in cui una segnalazione ha realizzato la sua finalità, è opportuno fissare criteri dettagliati per ciascuna categoria di segnalazione che consentano di determinare quando debba essere cancellata.

(47) L'integrità dei dati SIS è di primaria importanza. È opportuno pertanto stabilire garanzie adeguate per il trattamento dei dati SIS a livello sia centrale sia 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 dovrebbero essere soggette a una procedura uniforme di segnalazione degli incidenti. Il loro personale dovrebbe essere adeguatamente formato e informato di eventuali reati e sanzioni al riguardo.

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

(49) È opportuno accordare l'accesso al SIS ai servizi preposti all'immatricolazione di veicoli, natanti e aeromobili per consentire loro di verificare se il mezzo di trasporto in questione sia già ricercato negli Stati membri a scopo di sequestro. È altresì opportuno accordare l'accesso al SIS ai servizi preposti alla registrazione di armi da fuoco per consentire loro di verificare se l'arma da fuoco in questione sia ricercata negli Stati membri a scopo di sequestro o se vi sia una segnalazione relativa alla persona che ne richiede la registrazione.

(50) L'accesso diretto al SIS dovrebbe essere concesso soltanto ai servizi pubblici competenti. 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 oppure alle armi da fuoco e alle persone che ne richiedano la registrazione. I servizi pubblici summenzionati dovrebbero comunicare i riscontri positivi (hit) nel SIS alle autorità di polizia, che dovrebbero provvedere alle azioni ulteriori in linea con la segnalazione particolare nel SIS e comunicheranno il riscontro positivo (hit) allo Stato membro segnalante tramite gli uffici SIRENE.

(51) Fatte salve le norme più specifiche di cui al presente regolamento, le leggi, i regolamenti e le disposizioni amministrative nazionali adottati a norma della direttiva (UE) 2016/680 dovrebbbero applicarsi al trattamento, comprese la raccolta e la comunicazione dei dati personali a norma del presente regolamento, da parte delle autorità nazionali competenti a fini di prevenzione, accertamento, indagine o perseguimento di reati di terrorismo o di altri reati gravi o esecuzione di sanzioni penali. L'accesso ai dati inseriti nel SIS e il diritto di consultazione degli stessi da parte delle autorità nazionali competenti a fini di prevenzione, accertamento, indagine o perseguimento di reati di terrorismo o di altri reati gravi o esecuzione di sanzioni penali sono subordinati a tutte le pertinenti disposizioni del presente regolamento e a quelle della direttiva (UE) 2016/680 recepite nel diritto interno, e in particolare alla sorveglianza delle autorità di cui alla direttiva (UE) 2016/680.

(52) Fatte salve le norme più specifiche di cui al presente regolamento concernenti il trattamento dei dati personali, al trattamento dei dati personali da parte degli Stati membri ai sensi del presente regolamento si dovrebbe applicare il regolamento (UE) 2016/679, a meno che tale trattamento sia effettuato dalle autorità nazionali competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati di terrorismo o di altri reati gravi.

(53) Il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([1]) dovrebbe applicarsi al trattamento dei dati personali effettuato dalle istituzioni e dagli organismi dell'Unione nell'assolvimento dei loro compiti a norma del presente regolamento.

(54) Il regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio ([2]) dovrebbe applicarsi al trattamento dei dati personali effettuato da Europol a norma del presente regolamento.

(55) Qualora le interrogazioni svolte in SIS dai membri nazionali di Eurojust e dai rispettivi assistenti rivelino l'esistenza di una segnalazione inserita da uno Stato membro, Eurojust non può intraprendere l'azione richiesta. Dovrebbe pertanto informare lo Stato membro interessato per permettergli di dare seguito al caso.

(56) Quando utilizzano il SIS, le autorità competenti dovrebbero assicurare il rispetto della dignità e dell'integrità della persona i cui dati sono trattati. Il trattamento di dati personali ai fini del presente regolamento non deve dar luogo a discriminazioni nei confronti delle persone fondate sul sesso, sulla razza o sull'origine etnica, sulla religione o sulle convinzioni personali, sulla disabilità, sull'età o sull'orientamento sessuale.

(57) Per quanto riguarda la riservatezza, le pertinenti disposizioni dello statuto dei funzionari dell'Unione europea e del regime applicabile agli altri agenti dell'Unione, stabilite nel regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio ([3]) («Statuto dei funzionari») dovrebbero applicarsi ai funzionari o altri agenti che sono impiegati e che lavorano per il SIS.

(58) Sia gli Stati membri sia l'eu-LISA 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.

(59) Le autorità nazionali di controllo indipendenti di cui al regolamento (UE) 2016/679 e alla direttiva (UE) 2016/680 («autorità di controllo») dovrebbero controllare la liceità del trattamento dei dati personali da parte degli Stati membri ai sensi del presente regolamento, incluso lo scambio di informazioni supplementari. Le autorità di controllo dovrebbero essere dotate di risorse sufficienti per svolgere detto compito. 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 altresì opportuno esigere dagli Stati membri statistiche annuali.

(60) Le autorità di controllo dovrebbero provvedere affinché sia svolto un controllo delle operazioni di trattamento dei dati nei sistemi nazionali dei rispettivi Stati membri, conformemente alle norme di revisione internazionali, almeno ogni quattro anni. Il controllo dovrebbe essere svolto dalle autorità di controllo oppure le autorità di controllo dovrebbero commissionare il controllo direttamente a un revisore indipendente nel settore della protezione dei dati. Il revisore indipendente dovrebbe rimanere sotto il controllo e la responsabilità della o delle autorità di controllo in questione, che di conseguenza dovrebbero commissionare esse stesse la revisione, definirne chiaramente la finalità, l'ambito di applicazione e la metodologia, fornire istruzioni e supervisionare il controllo e i relativi risultati finali.

([1]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, nonché la libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

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

([3]) GU L 56 del 4.3.1968, pag. 1.

(61) Il Garante europeo della protezione dei dati dovrebbe controllare le attività delle istituzioni e degli organismi dell'Unione relative al trattamento dei dati personali a norma del presente regolamento. Il Garante europeo della protezione dei dati e le autorità di controllo dovrebbero cooperare nel controllo del SIS.

(62) Al Garante europeo della protezione dei dati dovrebbero essere fornite risorse sufficienti per assolvere i compiti assegnatigli a norma del presente regolamento, compresa l'assistenza da parte di persone competenti in materia di dati biometrici.

(63) A norma del regolamento (UE) 2016/794, Europol deve sostenere e potenziare l'azione delle autorità nazionali competenti e la loro cooperazione nel combattere il terrorismo e altre forme gravi di criminalità e nel fornire analisi e valutazioni della minaccia. L'estensione dei diritti di accesso di Europol alle segnalazioni nel SIS di persone scomparse dovrebbe migliorare la capacità di Europol di fornire alle autorità di contrasto nazionali apporti 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 dei reati in questione. Anche il Centro europeo per la lotta alla criminalità informatica di Europol beneficerebbe del nuovo accesso di Europol alle segnalazioni di persone scomparse, 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 scomparsi.

(64) Per colmare le lacune nella condivisione di informazioni sul terrorismo, in particolare sui combattenti terroristi stranieri - di cui è cruciale sorvegliare i movimenti - gli Stati membri sono incoraggiati a condividere con Europol informazioni su attività legate al terrorismo. È opportuno che tale condivisione di informazioni sia effettuata mediante lo scambio di informazioni supplementari con Europol sulle segnalazioni pertinenti. A tale scopo Europol dovrebbe istituire una connessione con l'infrastruttura di comunicazione.

(65) È inoltre necessario stabilire regole chiare a uso di Europol sul trattamento e sullo scaricamento dei dati del SIS per consentire un ampio uso 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 inserita da uno Stato membro, Europol non può intraprendere l'azione richiesta. Dovrebbe pertanto informare lo Stato membro interessato tramite lo scambio di informazioni supplementari con il rispettivo ufficio SIRENE per consentire a tale Stato membro di dare seguito al caso.

(66) Il regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio ([1]) prevede, ai fini di tale regolamento, che lo Stato membro ospitante autorizzi i membri delle squadre di cui all'articolo 2, punto 8), di tale regolamento dispiegate dall'Agenzia europea della guardia di frontiera e costiera a consultare le banche dati dell'Unione, 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 altresì distaccare esperti che non fanno parte del personale di tali agenzie dell'Unione presso le squadre di sostegno per la gestione della migrazione. L'impiego delle squadre di cui all'articolo 2, punti 8) e 9), di tale regolamento 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 assolvere i compiti loro assegnati, le squadre di cui all'articolo 2, punti 8) e 9), di tale regolamento hanno bisogno di accedere al SIS tramite un'interfaccia tecnica dell'Agenzia europea della guardia di frontiera e costiera connessa al SIS centrale. Qualora interrogazioni svolte nel SIS dalla squadra o dalle squadre del personale di cui all'articolo 2, punti 8) e 9), del regolamento (UE) 2016/1624 rivelino l'esistenza di una segnalazione inserita da uno Stato membro, il membro della squadra o del personale non può intraprendere l'azione richiesta se non è autorizzato a farlo dallo Stato membro ospitante. Dovrebbe pertanto informare lo Stato membro ospitante al fine di dare seguito al caso. Lo Stato membro ospitante dovrebbe comunicare il riscontro positivo (hit) allo Stato membro segnalante tramite lo scambio di informazioni supplementari.

(67) Taluni aspetti del SIS non possono essere trattati con esaustività dal presente regolamento a causa della loro tecnicità, del loro livello di dettaglio e della necessità di aggiornamenti periodici. Tali aspetti includono, ad esempio, delle norme tecniche concernenti l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati, la qualità dei dati,le regole relative ai dati biometrici, le norme sulla sull'ordine delle priorità delle

([1]) Regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio, del 14 settembre 2016, relativo alla guardia di frontiera e costiera europea 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).

segnalazioni, l'interconnessione delle segnalazioni, la data di scadenza delle segnalazioni entro il termine massimo e lo scambio di informazioni supplementari. È pertanto opportuno attribuire 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.

(68) 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 del Parlamento europeo e del Consiglio ([1]). La procedura di adozione degli atti di esecuzione a norma del presente regolamento e del regolamento (UE) 2018/1861 dovrebbe essere la stessa.

(69) Per ragioni di trasparenza è opportuno che due anni dopo l'entrata in funzione del SIS a norma del presente regolamento l'eu-LISA presenti una relazione sul funzionamento tecnico del SIS centrale e dell'infrastruttura di comunicazione, compresa la relativa sicurezza, e sullo scambio bilaterale e multilaterale di informazioni supplementari. Ogni quattro anni la Commissione dovrebbe provvedere a una valutazione globale.

(70) Al fine di garantire il corretto funzionamento del SIS, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE riguardo alle nuove sottocategorie di oggetti ricercati nell'ambito di segnalazioni di oggetti a fini di sequestro o di prova in un procedimento penale e alla determinazione dei casi in cui è possibile ricorrere a fotografie e immagini del volto per identificare le persone in un contesto diverso da quello dei valichi di frontiera regolari. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale del 13 aprile 2016 «Legiferare meglio» ([2]). In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(71) Poiché gli obiettivi del presente regolamento, vale a dire l'istituzione e la regolamentazione di un sistema d'informazione dell'Unione e il relativo scambio di informazioni supplementari, non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della loro stessa natura, possono 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 (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(72) 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 rispetta pienamente la tutela dei dati personali in conformità dell'articolo 8 della Carta dei diritti fondamentali dell'Unione europea prefiggendosi nel contempo l'obiettivo di garantire un ambiente sicuro per tutte le persone residenti sul territorio dell'Unione e una protezione speciale per i minori che rischiano di essere vittime di tratta o di sottrazione. Nei casi relativi ai minori l'interesse superiore del minore dovrebbe costituire una considerazione preminente.

(73) A norma degli articoli 1 e 2 del protocollo n. 22 sulla posizione della Danimarca, allegato al TUE e al TFUE, 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 un periodo di sei mesi dalla decisione del Consiglio sul presente regolamento, se intende recepirlo nel proprio diritto interno.

(74) Il Regno Unito partecipa al presente regolamento ai sensi dell'articolo 5, paragrafo 1, del protocollo n. 19 sull'*acquis* di Schengen integrato nell'ambito dell'Unione europea, allegato al TUE e al TFUE, e dell'articolo 8, paragrafo 2, della decisione 2000/365/CE del Consiglio ([3]).

(75) L'Irlanda partecipa al presente regolamento ai sensi dell'articolo 5, paragrafo 1, del protocollo n. 19 allegato al TUE e al TFUE, e dell'articolo 6, paragrafo 2, della decisione 2002/192/CE del Consiglio ([4]).

([1]) 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).

([2]) GU L 123 del 12.5.2016, pag. 1.

([3]) 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 (GU L 131 dell'1.6.2000, pag. 43).

([4]) Decisione 2002/192/CE del Consiglio, del 28 febbraio 2002, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'*acquis* di Schengen (GU L 64 del 7.3.2002, pag. 20).

(76) 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 ([1]), 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 ([2]).

(77) Per quanto riguarda la Svizzera, il presente regolamento costituisce, ai sensi dell'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione di quest'ultima all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen ([3]), 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, in combinato disposto con l'articolo 3 della decisione 2008/149/GAI del Consiglio ([4]).

(78) Per quanto riguarda il Liechtenstein, il presente regolamento costituisce, ai sensi 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 ([5]), 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, in combinato disposto con l'articolo 3 della decisione 2011/349/UE del Consiglio ([6]).

(79) Per quanto riguarda Bulgaria e Romania, il presente regolamento costituisce un atto basato sull'*acquis* di Schengen o a esso altrimenti connesso ai sensi dell'articolo 4, paragrafo 2, dell'atto di adesione del 2005, e dovrebbe essere letto in combinato disposto con le decisioni 2010/365/UE ([7]) e (UE) 2018/934 del Consiglio ([8]).

(80) Per quanto riguarda la Croazia, il presente regolamento costituisce un atto basato sull'*acquis* di Schengen o ad esso altrimenti connesso/correlato ai sensi dell'articolo 4, paragrafo 2, dell'atto di adesione del 2011, e dovrebbe essere letto in combinato disposto con la decisione (UE) 2017/733 del Consiglio ([9]).

(81) Per quanto riguarda Cipro, il presente regolamento costituisce un atto basato sull'*acquis* di Schengen o ad esso altrimenti connesso ai sensi dell'articolo 3, paragrafo 2, dell'atto di adesione del 2003.

(82) 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.

(83) Il presente regolamento introduce una serie di miglioramenti al SIS che accresceranno la sua efficacia, rafforzeranno la protezione dei dati ed estenderanno i diritti di accesso. Alcuni di questi miglioramenti non richiedono sviluppi tecnici complessi, mentre altri richiedono modifiche tecniche di varia entità. Affinché i miglioramenti del sistema possano essere messi a disposizione degli utenti finali il prima possibile, il presente regolamento introduce modifiche alla decisione 2007/533/GAI in diverse tappe. Vari miglioramenti al sistema dovrebbero applicarsi immediatamente al momento dell'entrata in vigore del presente regolamento, mentre altri dovrebbero applicarsi uno o due anni dopo la sua entrata in vigore. Il presente regolamento dovrebbe applicarsi in tutti i suoi elementi entro tre anni dalla sua entrata in vigore. Al fine di evitare ritardi nella sua applicazione, l'attuazione per tappe del presente regolamento dovrebbe essere oggetto di attento monitoraggio.

([1]) GU L 176 del 10.7.1999, pag. 36.

([2]) Decisione 1999/437/CE del Consiglio, del 17 maggio 1999, relativa a talune modalità di applicazione dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sull'associazione di questi due Stati all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen (GU L 176 del 10.7.1999, pag. 31).

([3]) GU L 53 del 27.2.2008, pag. 52.

([4]) Decisione 2008/149/GAI del Consiglio, del 28 gennaio 2008, relativa alla conclusione, a nome dell'Unione europea, 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 53 del 27.2.2008, pag. 50).

([5]) GU L 160 del 18.6.2011, pag. 21.

([6]) 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).

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

([8]) Decisione (UE) 2018/934 del Consiglio, del 25 giugno 2018, relativa all'attuazione delle rimanenti disposizioni dell'*acquis* di Schengen concernenti il sistema d'informazione Schengen nella Repubblica di Bulgaria e in Romania (GU L 165 del 2.7.2018, pag. 37).

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

(84) È opportuno abrogare il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio ([1]), la decisione 2007/533/GAI e la decisione 2010/261/UE della Commissione ([2]) con effetto dalla data di piena applicazione del presente regolamento.

(85) Il Garante europeo della protezione dei dati è stato consultato a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ([3]) e ha espresso un parere il 3 maggio 2017,

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 garantire l'applicazione delle disposizioni della parte terza, titolo V, capi 4 e 5, TFUE relative alla circolazione delle persone in detto territorio, avvalendosi delle informazioni trasmesse mediante tale sistema.

Articolo 2

Oggetto

1. Il presente regolamento stabilisce 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 prevede anche disposizioni sull'architettura tecnica del SIS, sulle competenze degli Stati membri e dell'agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia («eu-LISA»), sulle regole sul trattamento dei dati, sui diritti delle persone interessate e sulla responsabilità.

Articolo 3

Definizioni

Ai fini del presente regolamento s'intende per:

1) «segnalazione»: un insieme di dati inseriti nel SIS che permette alle autorità competenti di identificare una persona o un oggetto al fine di intraprendere un'azione specifica;

2) «informazioni supplementari»: le informazioni non facenti parte dei dati di segnalazione conservati nel SIS ma connesse alle segnalazioni inserite nel SIS, che devono essere scambiate tramite gli uffici SIRENE:

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

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

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

   d) con riguardo alla qualità dei dati SIS;

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

   f) con riguardo ai diritti di accesso;

3) «dati complementari»: i dati memorizzati nel SIS e connessi alle segnalazioni nel 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 del SIS;

([1]) 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).

([2]) 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).

([3]) 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).

4) «dati personali»: i dati personali quali definiti all'articolo 4, punto 1), del regolamento (UE) 2016/679;

5) «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 memorizzazione, 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;

6) «corrispondenza»: il verificarsi, nell'ordine, di quanto segue:

   a) un utente finale ha effettuato un'interrogazione;

   b) l'interrogazione ha rivelato la presenza di una segnalazione inserita nel SIS da un altro Stato membro; e

   c) i dati relativi alla segnalazione nel SIS corrispondono ai dati dell'interrogazione;

7) «riscontro positivo (hit)»: una corrispondenza che soddisfi i seguenti criteri:

   a) è stata confermata da:

      i) l'utente finale; oppure

      ii) l'autorità competente conformemente alle procedure nazionali, qualora la corrispondenza in questione si basi sul raffronto di dati biometrici;

      e

   b) sono richieste ulteriori azioni;

8) «indicatore di validità»: la sospensione della validità di una segnalazione a livello nazionale apponibile alle segnalazioni per l'arresto, alle segnalazioni di persone scomparse e vulnerabili e alle segnalazioni ai fini di un controllo discreto, di indagine o specifico;

9) «Stato membro segnalante»: lo Stato membro che ha inserito la segnalazione nel SIS;

10) «Stato membro di esecuzione»: lo Stato membro che intraprende o ha intrapreso l'azione richiesta in seguito a un riscontro positivo (hit);

11) «utente finale»: un membro del personale di un'autorità competente autorizzato ad interrogare direttamente il CS-SIS, l'N.SIS o una loro copia tecnica;

12) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche o fisiologiche di una persona fisica che ne consentono o confermano l'identificazione univoca, vale a dire fotografie, immagini del volto, dati dattiloscopici e profilo DNA;

13) «dati dattiloscopici»: i 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;

14) «immagine del volto»: le immagini digitali del volto caratterizzate da sufficiente risoluzione e qualità dell'immagine per essere utilizzate in un raffronto biometrico automatizzato;

15) «profilo DNA»: un codice alfanumerico che rappresenta una serie di caratteristiche identificative della parte non codificante di un campione di DNA umano analizzato, vale a dire la struttura molecolare particolare dei vari loci del DNA;

16) «reati di terrorismo»: i reati previsti dal diritto nazionale di cui agli articoli da 3 a 14 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio ([1]), o equivalenti a uno di tali reati per gli Stati membri che non sono vincolati da detta direttiva;

17) «minaccia per la salute pubblica»: una minaccia per la salute pubblica quale definita all'articolo 2, punto 21), del regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio ([2]).

([1]) Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio (GU L 88 del 31.3.2017, pag. 6).

([2]) 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) (GU L 77 del 23.3.2016, pag. 1).

Articolo 4

Architettura tecnica e modalità operative del SIS

1. Il SIS consta di:

a) un sistema centrale («SIS centrale») costituito da:

   i) un'unità di supporto tecnico («CS-SIS») contenente una banca dati, la («banca dati del SIS»), compresa una copia di riserva del CS-SIS,

   ii) un'interfaccia nazionale uniforme («NI-SIS»);

b) un sistema nazionale («N.SIS») in ciascuno Stato membro, composto dei sistemi di dati nazionali che comunicano con il SIS centrale, ivi compreso almeno un N.SIS di riserva nazionale o condiviso (sito backup), e

c) un'infrastruttura di comunicazione fra il CS-SIS, il CS-SIS di riserva 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.

Un N.SIS di cui alla lettera b) può contenere un archivio di dati («copia nazionale»), contenente a sua volta una copia completa o parziale della banca dati del SIS. Due o più Stati membri possono creare una copia condivisa in uno dei loro N.SIS, che può essere usata congiuntamente da tali Stati membri. Tale copia condivisa è considerata la copia nazionale di ciascuno di tali Stati membri.

Un N.SIS di riserva condiviso di cui alla lettera b) può essere usato congiuntamente da due o più Stati membri. In tal caso, il N.SIS. di riserva condiviso è considerato l'N.SIS di riserva di ciascuno di tali Stati membri. L'N.SIS e la sua copia di riserva possono essere usati simultaneamente per garantire agli utenti finali una disponibilità ininterrotta.

Gli Stati membri che intendono creare una copia condivisa o un N.SIS di riserva condiviso da utilizzare congiuntamente definiscono le rispettive responsabilità in un accordo scritto. Essi notificano il proprio accordo alla Commissione.

L'infrastruttura di comunicazione sostiene e contribuisce a garantire la disponibilità ininterrotta del SIS. Essa comprende percorsi ridondanti e separati per le connessioni tra il CS-SIS e il CS-SIS di riserva, oltre che percorsi ridondanti e separati per le connessioni tra ciascun punto di accesso nazionale alla rete SIS e il CS-SIS e il CS-SIS di riserva.

2. Gli Stati membri inseriscono, aggiornano, cancellano e consultano i dati SIS attraverso il proprio N.SIS. Gli Stati membri che utilizzano una copia nazionale parziale o completa, o una copia condivisa parziale o completa rendono disponibile tale copia ai fini dell'interrogazione automatizzata nel territorio di ciascuno di tali Stati membri. La copia nazionale o condivisa parziale contiene almeno i dati di cui all'articolo 20, paragrafo 3, lettere da a) a v). Non possono essere consultati gli archivi di dati contenuti nell'N.SIS degli altri Stati membri, salvo in caso di copie condivise.

3. Il CS-SIS svolge funzioni di controllo tecnico e di gestione e dispone di una copia di riserva del CS-SIS in grado di assicurare tutte le funzionalità del CS-SIS principale in caso di guasto di tale sistema. Il CS-SIS e il CS-SIS di riserva sono ubicati nei due siti tecnici dell'eu-LISA.

4. L'eu-LISA mette in atto soluzioni tecniche volte a rafforzare la disponibilità ininterrotta del SIS o mediante il funzionamento simultaneo del CS-SIS e il CS-SIS di riserva, purché il CS-SIS di riserva sia in grado di assicurare il funzionamento del SIS in caso di guasto del CS-SIS, o mediante la duplicazione del sistema o delle sue componenti. In deroga ai requisiti procedurali di cui all'articolo 10 del regolamento (UE) 2018/1726 l'eu-LISA elabora, al più tardi il 28 dicembre 2019, uno studio sulle opzioni per le soluzioni tecniche, contenente una valutazione d'impatto indipendente e un'analisi costi-benefici.

5. In circostanze eccezionali, l'eu-LISA può, se necessario, creare temporaneamente una copia supplementare della banca dati del CS-SIS.

6. Il CS-SIS fornisce i servizi necessari per l'inserimento e il trattamento dei dati SIS, compresa la consultazione della banca dati del SIS. Per gli Stati membri che usano una copia nazionale o condivisa, il CS-SIS provvede a:

a) fornire aggiornamenti in linea delle copie nazionali;

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

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

7. Il CS-SIS assicura una 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. Tali costi includono il lavoro effettuato con riguardo al CS-SIS per garantire la fornitura dei servizi di cui all'articolo 4, paragrafo 6.

2. 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.

Ciascuno Stato membro è responsabile di garantire la disponibilità ininterrotta dei dati SIS agli utenti finali.

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

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 del presente regolamento. Ha il compito di garantire che tutte le funzionalità del SIS siano messe adeguatamente a disposizione degli utenti finali.

2. Ciascuno Stato membro designa un'autorità nazionale, operativa 24 ore su 24 e 7 giorni su 7, che garantisca lo scambio e la disponibilità di tutte le informazioni supplementari («ufficio SIRENE») conformemente al manuale SIRENE. Ogni ufficio SIRENE funge da punto di contatto unico per il proprio Stato membro per lo scambio di informazioni supplementari sulle segnalazioni e per agevolare l'adozione delle azioni richieste quando sono inserite nel SIS segnalazioni relative a persone o oggetti e tali persone o oggetti sono localizzati in seguito a un riscontro positivo (hit).

Ogni ufficio SIRENE dispone, in conformità del diritto nazionale, di un facile accesso diretto o indiretto a tutte le informazioni nazionali pertinenti, comprese le banche dati nazionali e tutte le informazioni sulle segnalazioni degli Stati membri, nonché alla consulenza di esperti per essere in grado di reagire alle richieste di informazioni supplementari in modo rapido ed entro i termini di cui all'articolo 8.

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

3. Gli Stati membri forniscono all'eu-LISA gli estremi dei rispettivi uffici N. SIS e SIRENE. L'eu-LISA pubblica l'elenco degli uffici N. SIS e degli uffici SIRENE insieme all'elenco di cui all'articolo 56, paragrafo 7.

Articolo 8

Scambio di informazioni supplementari

1. Le informazioni supplementari sono scambiate conformemente alle disposizioni del manuale SIRENE e tramite l'infrastruttura di comunicazione. Gli Stati membri forniscono le risorse tecniche e umane necessarie per garantire in permanenza la disponibilità e lo scambio tempestivo ed efficace delle informazioni supplementari. In caso di indisponibilità dell'infrastruttura di comunicazione, gli Stati membri usano altri mezzi tecnici adeguatamente protetti per lo scambio di informazioni supplementari. Un elenco di mezzi tecnici adeguatamente protetti è riportato nel manuale SIRENE.

2. Le informazioni supplementari sono usate solo per le finalità per le quali sono state trasmesse in conformità dell'articolo 64, a meno che non sia stato ottenuto il previo consenso per un uso ulteriore dallo Stato membro segnalante.

3. Gli uffici SIRENE svolgono il loro compito in modo rapido ed efficiente, in particolare rispondendo a una richiesta di informazioni supplementari appena possibile e comunque entro 12 ore dal ricevimento della richiesta. In caso di segnalazioni relative a reati di terrorismo, di segnalazioni di persone ricercate per l'arresto a fini di consegna o di estradizione e in caso di segnalazioni concernenti minori di cui all'articolo 32, paragrafo 1, lettera c), gli uffici SIRENE intervengono immediatamente.

Le richieste di informazioni supplementari da trattare con la massima priorità possono recare la dicitura «URGENT» (urgente) nei formulari SIRENE, seguita dalla specificazione dei motivi dell'urgenza.

4. La Commissione adotta atti di esecuzione al fine di stabilire modalità dettagliate per i compiti degli uffici SIRENE ai sensi del presente regolamento e per lo scambio di informazioni supplementari sotto forma di un manuale intitolato «manuale SIRENE». Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

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 SIS centrale.

2. In caso di uso di una copia nazionale, lo Stato membro interessato assicura, tramite i servizi forniti dal CS-SIS e gli aggiornamenti automatici di cui all'articolo 4, paragrafo 6, che i dati memorizzati nella copia nazionale siano 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.

3. Gli utenti finali ricevono i dati necessari allo svolgimento dei loro compiti, in particolare e se necessario, tutti i dati disponibili che consentano di identificare l'interessato e di intraprendere le azioni necessarie.

4. Gli Stati membri e l'eu-LISA effettuano prove regolari per verificare la conformità tecnica delle copie nazionali di cui al paragrafo 2. I risultati di tali prove sono presi in considerazione nel quadro del meccanismo istituito dal regolamento (UE) n. 1053/2013 del Consiglio ([1]).

5. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme, i protocolli e le procedure tecniche comuni di cui al paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

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 di 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) impedire che i dati siano trattati nel SIS senza autorizzazione e che i dati trattati nel SIS siano modificati o cancellati senza autorizzazione (controllo dell'inserimento dei dati);

g) garantire che le persone autorizzate a usare un sistema automatizzato di trattamento dei dati possano accedere solo ai dati previsti dalla loro autorizzazione di accesso attraverso identificatori di utente individuali e unici ed esclusivamente con modalità di accesso riservate (controllo dell'accesso ai dati);

([1]) 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).

h) assicurare che tutte le autorità con diritto di accesso 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 di controllo di cui all'articolo 69, paragrafo 1, a richiesta di queste (profili del personale);

i) 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);

j) 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 la finalità dello stesso (controllo dell'inserimento);

k) 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);

l) controllare l'efficacia delle misure di sicurezza di cui al presente paragrafo e adottare le necessarie misure di carattere organizzativo relative al monitoraggio interno per garantire il rispetto del presente regolamento(autocontrollo);

m) garantire che, in caso di interruzione, i sistemi installati possano essere ripristinati (ripristino); e

n) garantire che il SIS esegua le sue funzioni correttamente, che gli errori siano segnalati (affidabilità) e che i dati personali conservati nel SIS non possano essere falsati da un errore di funzionamento del sistema (integrità).

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 degli uffici SIRENE.

3. Gli Stati membri adottano misure equivalenti a quelle del paragrafo 1 del presente articolo per quanto riguarda la sicurezza del trattamento dei dati SIS da parte delle autorità di cui all'articolo 44.

4. Le misure descritte nei paragrafi 1, 2 e 3 possono rientrare in un approccio alla sicurezza e in un piano di sicurezza generici a livello nazionale comprendenti molteplici sistemi informatici. In tali casi, i requisiti di cui al presente articolo e la relativa applicabilità al SIS sono chiaramente identificabili in tale piano e garantiti dallo stesso.

Articolo 11

Riservatezza – Stati membri

1. Ogni Stato membro applica le proprie norme 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 al proprio diritto interno. Tale obbligo vincola detti soggetti e organismi anche dopo che hanno rispettivamente lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

2. Qualora collabori con contraenti esterni per un qualsiasi compito relativo al SIS, lo Stato membro monitora attentamente le attività del contraente per garantire il rispetto di tutte le disposizioni del presente regolamento, comprese in particolare la sicurezza, la riservatezza e la protezione dei dati.

3. La gestione operativa dell'N.SIS o delle copie tecniche non può essere affidata a imprese o organizzazioni private.

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 siano registrati nei rispettivi N.SIS per verificare la legittimità dell'interrogazione, per controllare la liceità del trattamento dei dati, ai fini dell'autocontrollo, per garantire il corretto funzionamento dell'N.SIS, nonché per l'integrità e la sicurezza dei dati. Tale requisito non si applica ai processi automatici di cui all'articolo 4, paragrafo 6, lettere a), b) e c).

2. I registri riportano, in particolare, la cronistoria della segnalazione, la data e l'ora dell'attività di trattamento dei dati, i dati usati per effettuare un'interrogazione, un riferimento ai dati trattati e gli identificatori di utente individuali e unici dell'autorità competente e della persona che effettua il trattamento dei dati.

3. In deroga al paragrafo 2 del presente articolo, se l'interrogazione è effettuata con dati dattiloscopici o un'immagine del volto in conformità dell'articolo 43, i registri riportano il tipo di dati usati per effettuare l'interrogazione anziché i dati effettivi.

4. I registri sono usati solo ai fini di cui al paragrafo 1 e sono cancellati tre anni dopo la loro creazione. I registri contenenti la cronistoria delle segnalazioni sono cancellati tre anni dopo la cancellazione delle segnalazioni.

5. I registri possono essere tenuti più a lungo dei termini di cui al paragrafo 4 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 e 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, in conformità del diritto nazionale, effettuano interrogazioni automatizzate mediante scansione delle targhe di veicoli a motore, ricorrendo a sistemi di riconoscimento automatico delle targhe, tengono un registro di tali interrogazioni conformemente al rispettivo diritto interno. Se necessario, può essere effettuata un'interrogazione completa nel SIS per verificare se sia stato ottenuto un riscontro positivo (hit). I paragrafi da 1 a 6 si applicano a qualsiasi interrogazione completa.

8. La Commissione adotta atti di esecuzione al fine di stabilire il contenuto del registro di cui al paragrafo 7 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

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

1. 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 sulla sicurezza dei dati, sui diritti fondamentali, comprese le norme sulla protezione dei dati, nonché sulle procedure di trattamento dei dati previste nel manuale SIRENE. Il personale è informato delle disposizioni relative ai reati e alle sanzioni pertinenti, comprese quelle stabilite all'articolo 73.

2. Gli Stati membri dispongono di un programma nazionale di formazione sul SIS che comprende una formazione per gli utenti finali e per il personale degli uffici SIRENE.

Tale programma di formazione può rientrare in un programma di formazione generale a livello nazionale comprendente la formazione in altri settori pertinenti.

3. Almeno una volta l'anno sono organizzati corsi comuni di formazione a livello dell'Unione per rafforzare la cooperazione tra gli uffici SIRENE.

CAPO III

Competenze dell'eu-LISA

Articolo 15

Gestione operativa

1. L'eu-LISA è responsabile della gestione operativa del SIS centrale. L'eu-LISA, in collaborazione con gli Stati membri, provvede affinché per il SIS centrale siano utilizzate in ogni momento le migliori tecnologie disponibili, fatta salva un'analisi costi-benefici.

2. L'eu-LISA 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;

d) compiti relativi all'esecuzione del bilancio;

e) acquisizione e rinnovo; e

f) aspetti contrattuali.

3. L'eu-LISA è inoltre responsabile dei seguenti compiti relativi agli uffici SIRENE e alla comunicazione tra gli uffici SIRENE:

a) coordinamento, gestione e sostegno delle attività di collaudo;

b) gestione e aggiornamento di specifiche tecniche per lo scambio di informazioni supplementari tra gli uffici SIRENE e l'infrastruttura di comunicazione; e

c) gestione dell'effetto dei cambiamenti tecnici laddove riguardino sia il SIS che lo scambio di informazioni supplementari tra gli uffici SIRENE.

4. L'eu-LISA sviluppa e gestisce un meccanismo e procedure per lo svolgimento dei controlli di qualità sui dati contenuti nel CS-SIS. A tale riguardo essa riferisce periodicamente agli Stati membri.

L'eu-LISA riferisce periodicamente alla Commissione in merito ai problemi incontrati e agli Stati membri interessati.

La Commissione presenta una relazione periodica al Parlamento europeo e al Consiglio in merito ai problemi di qualità dei dati incontrati.

5. L'eu-LISA svolge anche compiti relativi all'offerta di formazione sull'uso tecnico del SIS e sulle misure atte a migliorare la qualità dei dati SIS.

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 in conformità del presente regolamento, e comprende in particolare le attività di manutenzione e gli adattamenti tecnici necessari per il buon funzionamento del sistema. Tali compiti comprendono anche il coordinamento, la gestione e il sostegno delle attività di collaudo per il SIS centrale e i gli N.SIS che garantiscono che il SIS centrale e gli N.SIS operino secondo i requisiti tecnici e funzionali di cui all'articolo 9.

7. La Commissione adotta atti di esecuzione al fine di stabilire i requisiti tecnici dell'infrastruttura di comunicazione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

Articolo 16

Sicurezza – eu-LISA

1. L'eu-LISA 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 di 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) impedire che i dati siano trattati nel SIS senza autorizzazione e che i dati trattati nel SIS siano modificati o cancellati senza autorizzazione (controllo dell'inserimento dei dati);

g) garantire che le persone autorizzate a usare un sistema automatizzato di trattamento dei dati possano accedere solo ai dati previsti dalla loro autorizzazione di accesso attraverso identificatori di utente individuali e unici ed esclusivamente con modalità di accesso riservate (controllo dell'accesso ai dati);

h) 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 a richiesta di quest'ultimo (profili del personale);

i) 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);

j) 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);

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

l) 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).

m) garantire che, in caso di interruzione delle operazioni, i sistemi installati possano essere ripristinati (ripristino);

n) garantire che il SIS esegua le sue funzioni correttamente, che gli errori siano segnalati (affidabilità) e che i dati personali conservati nel SIS non possano essere falsati da un errore di funzionamento del sistema (integrità); e

o) garantire la sicurezza dei suoi siti tecnici.

2. L'eu-LISA 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 – eu-LISA

1. Fatto salvo l'articolo 17 dello statuto dei funzionari, l'eu-LISA 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 dall'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'eu-LISA 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.

3. Se collabora con contraenti esterni per un qualsiasi compito relativo al SIS, l'eu-LISA monitora attentamente le attività del contraente per garantire il rispetto di tutte le disposizioni del presente regolamento, in particolare per quanto concerne la sicurezza, la riservatezza e la protezione dei dati.

4. La gestione operativa del CS-SIS non può essere affidata a imprese o organizzazioni private.

Articolo 18

Tenuta dei registri a livello centrale

1. L'eu-LISA 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 della segnalazione, la data e l'ora dell'attività di trattamento dei dati, i dati usati per effettuare un'interrogazione, un riferimento ai dati trattati e gli identificatori di utente individuali e unici dell'autorità competente che effettua il trattamento dei dati.

3. In deroga al paragrafo 2 del presente articolo, se l'interrogazione è effettuata con dati dattiloscopici o immagini del volto in conformità dell'articolo 43, i registri riportano il tipo di dati usati per effettuare l'interrogazione anziché i dati effettivi.

4. I registri sono usati solo ai fini di cui al paragrafo 1 e sono cancellati tre anni dopo la loro creazione. I registri contenenti la cronistoria delle segnalazioni sono cancellati tre anni dopo la cancellazione delle segnalazioni.

5. I registri possono essere tenuti più a lungo del termine di cui al paragrafo 4 se necessari per procedure di controllo già in corso.

6. Ai fini dell'autocontrollo e per garantire il corretto funzionamento del CS-SIS nonché l'integrità e la sicurezza dei dati, l'eu-LISA ha accesso ai registri nei limiti delle sue competenze.

Il Garante europeo della protezione dei dati ha accesso a tali registri, nei limiti delle sue competenze e su sua richiesta, ai fini dell'assolvimento dei suoi compiti.

CAPO IV

Informazione del pubblico

Articolo 19

Campagne d'informazione sul SIS

All'inizio dell'applicazione del presente regolamento, la Commissione, in collaborazione con le autorità di controllo e con il Garante europeo della protezione dei dati, svolge una campagna per informare il pubblico sugli obiettivi del SIS, sui dati ivi conservati, sulle autorità che hanno accesso al SIS e sui diritti degli interessati. La Commissione ripete siffatte campagne a intervalli regolari in collaborazione con le autorità di controllo e con il Garante europeo della protezione dei dati. La Commissione mantiene un sito web a disposizione del pubblico attraverso cui fornire tutte le informazioni pertinenti relative al SIS. Gli Stati membri, in collaborazione con le rispettive autorità di controllo, definiscono e attuano le politiche necessarie per informare i propri cittadini e residenti 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 dagli articoli 26, 32, 34, 36, 38 e 40.

2. Le categorie di dati sono le seguenti:

a) informazioni sulle persone segnalate;

b) informazioni sugli oggetti di cui agli articoli 26, 32, 34, 36 e 38.

3. Le segnalazioni nel SIS che includono informazioni su persone contengono esclusivamente i seguenti dati:

a) cognomi;

b) nomi;

c) nomi e cognomi alla nascita;

d) nomi e cognomi precedenti e alias;

e) segni fisici particolari, oggettivi ed inalterabili;

f) il luogo di nascita;

g) la data di nascita;

h) il genere;

i) tutte le cittadinanze possedute;

j) l'indicazione che la persona:

   i) è armata;

   ii) è violenta;

   iii) è fuggita o evasa;

   iv) è a rischio suicidio;

   v) pone una minaccia per la salute pubblica; oppure

   vi) è coinvolta in un'attività di cui agli articoli da 3 a 14 della direttiva (UE) 2017/541;

k) la ragione della segnalazione;

l) l'autorità autrice della segnalazione;

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

n) l'azione da intraprendere in caso di riscontro positivo (hit);

o) le connessioni con altre segnalazioni a norma dell'articolo 63;

p) il tipo di reato;

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

r) per le segnalazioni di cui all'articolo 32, paragrafo 1, una categorizzazione del tipo di caso;

s) la categoria dei documenti di identificazione della persona;

t) il paese di rilascio dei documenti di identificazione della persona;

u) il numero dei documenti di identificazione della persona;

v) la data di rilascio dei documenti di identificazione della persona;

w) le fotografie e le immagini del volto;

x) in conformità dell'articolo 42, paragrafo 3, i profili DNA pertinenti;

y) i dati dattiloscopici;

z) una copia, possibilmente a colori, dei documenti di identificazione.

4. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui ai paragrafi 2 e 3 del presente articolo e le norme comuni di cui al paragrafo 5 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

5. Le norme tecniche sono simili per le interrogazioni nel CS-SIS, nelle copie nazionali o condivise e nelle copie tecniche di cui all'articolo 56, paragrafo 2. Tali norme tecniche sono basate su norme comuni.

Articolo 21

Proporzionalità

1. Prima di inserire 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 la segnalazione nel SIS.

2. Ove si ricerchi una persona o un oggetto nell'ambito di una segnalazione connessa a un reato di terrorismo, il caso è ritenuto adeguato, pertinente e sufficientemente importante da giustificare l'esistenza della segnalazione nel SIS. Per motivi di sicurezza pubblica o nazionale, gli Stati membri possono eccezionalmente astenersi dall'inserire una segnalazione, quando la stessa rischi di ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari.

Articolo 22

Requisito per l'inserimento di una segnalazione

1. L'insieme minimo di dati necessari per l'inserimento di una segnalazione nel SIS sono i dati di cui all'articolo 20, paragrafo 3, lettere a), g), k) e n), tranne nelle situazioni di cui all'articolo 40. Gli altri dati di cui allo stesso paragrafo sono anch'essi inseriti nel SIS, se disponibili.

2. I dati di cui all'articolo 20, paragrafo 3, lettera e), del presente regolamento sono inseriti solo qualora ciò sia strettamente necessario ai fini dell'identificazione della persona interessata. Quando tali dati sono inseriti, gli Stati membri assicurano che l'articolo 10 del regolamento (UE) 2016/680 sia rispettato.

Articolo 23

Compatibilità delle segnalazioni

1. Prima di inserire una segnalazione, uno Stato membro verifica se la persona o l'oggetto in questione siano già stati segnalati nel SIS. Per verificare se una persona sia già oggetto di una segnalazione, è effettuata anche una verifica con i dati dattiloscopici, se tali dati sono disponibili.

2. Per una stessa persona o per uno stesso oggetto è inserita nel SIS una sola segnalazione per Stato membro. Se necessario, possono essere inserite nuove segnalazioni sulla stessa persona o sullo stesso oggetto da altri Stati membri, conformemente al paragrafo 3.

3. Qualora una persona o un oggetto siano già stati segnalati nel SIS, uno Stato membro che desideri inserire una nuova segnalazione verifica che non esista alcuna incompatibilità tra le segnalazioni. Se non vi è alcuna incompatibilità, lo Stato membro può inserire la nuova segnalazione. Se le segnalazioni sono incompatibili, gli uffici SIRENE degli Stati membri interessati si consultano tramite lo scambio di informazioni supplementari al fine di raggiungere un accordo. Le norme sulla compatibilità delle segnalazioni sono stabilite nel manuale SIRENE. Per motivi di interesse nazionale essenziale è possibile derogare alle norme sulla compatibilità previa consultazione tra gli Stati membri.

4. In caso di riscontri positivi (hit) su segnalazioni multiple di una stessa persona, lo Stato membro di esecuzione si conforma alle norme in materia di priorità delle segnalazioni previste nel manuale SIRENE.

Nel caso in cui una persona sia oggetto di segnalazioni multiple inserite da diversi Stati membri, le segnalazioni per l'arresto inserite conformemente all'articolo 26 sono eseguite in via prioritaria a norma dell'articolo 25.

Articolo 24

Disposizioni generali relative agli indicatori di validità

1. Qualora uno Stato membro reputi che dare applicazione a una segnalazione inserita a norma degli articoli 26, 32 o 36 non sia compatibile con il proprio diritto nazionale, con i propri obblighi internazionali o con interessi nazionali essenziali, può chiedere che alla segnalazione sia apposto un indicatore di validità affinché non sia eseguita sul proprio territorio l'azione richiesta sulla base della segnalazione. L'indicatore di validità è apposto dall'ufficio SIRENE dello Stato membro segnalante.

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

3. Se in casi 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 chiesto l'apposizione. Se vi può acconsentire, lo Stato membro di esecuzione adotta le misure necessarie per far sì che l'azione da intraprendere 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, uno Stato membro richiede allo Stato membro segnalante di aggiungere l'indicatore di validità che impedisce l'arresto come seguito a una segnalazione per l'arresto a fini di consegna se l'autorità giudiziaria competente in virtù del diritto 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 chiesta.

Uno Stato membro può altresì chiedere l'apposizione di un indicatore di validità alla segnalazione se la sua autorità giudiziaria competente rilascia la persona oggetto della segnalazione durante la procedura di consegna.

2. Tuttavia, su richiesta di un'autorità giudiziaria competente in virtù del diritto nazionale, in base a un'istruzione generale o in un caso specifico, uno Stato membro può altresì chiedere allo Stato membro segnalante di apporre un indicatore di validità su una segnalazione per l'arresto a fini di consegna 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 per l'inserimento delle segnalazioni

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

2. Le segnalazioni per l'arresto a fini di consegna sono altresì inserite sulla scorta di mandati d'arresto emessi in conformità degli accordi conclusi tra l'Unione e paesi terzi in virtù dei trattati 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 e paesi terzi in virtù dei trattati ai fini della consegna di persone sulla base di un mandato d'arresto, che prevedono la trasmissione del mandato d'arresto tramite il SIS.

4. In caso di operazione in corso, lo Stato membro segnalante può rendere temporaneamente una segnalazione per l'arresto inserita a norma del presente articolo non consultabile dagli utenti finali negli Stati membri coinvolti nell'operazione. In tali casi la segnalazione è accessibile solo agli uffici SIRENE. Gli Stati membri rendono la segnalazione non consultabile unicamente se:

a) l'obiettivo dell'operazione non può essere raggiunto con altre misure;

b) un'autorizzazione preventiva è stata concessa dall'autorità giudiziaria competente dello Stato membro segnalante; e

c) tutti gli Stati membri coinvolti nell'operazione sono stati informati tramite lo scambio di informazioni supplementari.

La funzionalità di cui al primo comma è attivata esclusivamente per un periodo non superiore a 48 ore. Tuttavia, se necessario a fini operativi, l'attivazione può essere prolungata di ulteriori periodi di 48 ore. Gli Stati membri redigono statistiche sul numero di segnalazioni in cui è stata utilizzata tale funzionalità.

5. Qualora esistano indizi concreti che gli oggetti di cui all'articolo 38, paragrafo 2, lettere a), b), c), e), g), h), j) e k) siano collegati a una persona oggetto di segnalazione a norma dei paragrafi 1 e 2 del presente articolo, possono essere inserite segnalazioni di tali oggetti per localizzare la persona. In tali casi, la segnalazione della persona e la segnalazione dell'oggetto sono connesse in conformità dell'articolo 63.

6. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al paragrafo 5 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

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.

Uno Stato membro può inserire la copia di più mandati di arresto europei in una segnalazione per l'arresto a fini di consegna.

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.

Articolo 28

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

Lo Stato membro che ha inserito una 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 lo 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 una segnalazione a fini di estradizione comunica a tutti gli altri Stati membri i dati seguenti tramite scambio di informazioni supplementari:

a) l'autorità da cui proviene la richiesta di arresto;

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

c) la natura e la qualificazione giuridica del reato;

d) la 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; e

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

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

Articolo 30

Conversione di un'azione da intraprendere relativa a segnalazioni 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 all'articolo 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 cui à stato richiesto di procedere all'arresto dà seguito alla segnalazione comunicando il luogo di soggiorno della persona interessata.

Articolo 31

Esecuzione di un'azione richiesta nella segnalazione per l'arresto a fini di consegna o estradizione

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

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 o persone vulnerabili a cui deve essere impedito di viaggiare

Articolo 32

Obiettivi e condizioni per l'inserimento delle segnalazioni

1. Su richiesta dell'autorità competente dello Stato membro segnalante, sono inserite nel SIS segnalazioni sulle seguenti categorie di persone:

a) persone scomparse che devono essere poste sotto protezione:

   i) ai fini della loro tutela;

   ii) per prevenire una minaccia per l'ordine pubblico o la sicurezza pubblica;

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

c) minori a rischio di sottrazione da parte di un genitore, un familiare o un tutore a cui deve essere impedito di viaggiare;

d) minori a cui deve essere impedito di viaggiare a causa di un rischio concreto ed evidente che siano fatti uscire dal territorio di uno Stato membro o che lo lascino e che

   i) diventino vittime della tratta di esseri umani, di matrimonio forzato, di mutilazione genitale femminile o di altre forme di violenza di genere;

   ii) diventino vittime dei reati di terrorismo o vi siano coinvolti; oppure

   iii) siano reclutati o arruolati in gruppi armati, ovvero costretti a partecipare attivamente ad ostilità;

e) persone vulnerabili maggiorenni e a cui deve essere impedito di viaggiare ai fini della loro tutela, a causa di un rischio concreto ed evidente che siano fatti uscire dal territorio di uno Stato membro o che lo lascino e che diventino vittime della tratta di esseri umani o di violenza di genere.

2. Il paragrafo 1, lettera a), si applica specialmente ai minori e a persone che devono essere istituzionalizzate per decisione di un'autorità competente.

3. La segnalazione di un minore di cui al paragrafo 1, lettera c), è inserita in seguito a una decisione delle autorità competenti, incluse le autorità giudiziarie degli Stati membri competenti in materia di responsabilità genitoriale, in caso di rischio concreto ed evidente che il minore possa essere fatto uscire in modo illecito e imminente dallo Stato membro in cui hanno sede le autorità competenti.

4. Le segnalazioni relative alle persone di cui al paragrafo 1, lettere d) ed e), sono inserite in seguito a una decisione delle autorità competenti, incluse le autorità giudiziarie.

5. Lo Stato membro segnalante riesamina periodicamente la necessità di mantenere le segnalazioni di cui al paragrafo 1, lettere c), d) ed e), del presente articolo in conformità dell'articolo 53, paragrafo 4.

6. Lo Stato membro segnalante assicura che:

a) i dati che esso inserisce nel SIS indichino in quale delle categorie di cui al paragrafo 1 rientra la persona interessata dalla segnalazione;

b) i dati che esso inserisce nel SIS indichino il tipo di caso interessato, qualora sia noto; e

c) per quanto riguarda le segnalazioni inserite a norma del paragrafo 1, lettere c), d) ed e), il proprio ufficio SIRENE abbia tutte le informazioni pertinenti a sua disposizione al momento della creazione della segnalazione.

7. Quattro mesi prima che il minore oggetto di segnalazione ai sensi del presente articolo raggiunga la maggiore età conformemente al diritto nazionale dello Stato membro segnalante, 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.

8. Qualora esistano indizi concreti che gli oggetti di cui all'articolo 38, paragrafo 2, lettere a), b), c), e), g), h) e k) siano collegati a una persona oggetto di segnalazione a norma del paragrafo 1 del presente articolo, possono essere inserite segnalazioni di tali oggetti per localizzare la persona. In tali casi la segnalazione della persona e la segnalazione dell'oggetto sono connesse in conformità dell'articolo 63.

9. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme relative alla categorizzazione dei tipi di casi e all'inserimento dei dati di cui al paragrafo 6. I tipi di casi di minori scomparsi includono, tra l'altro, i minori fuggiti da casa, i minori non accompagnati nel contesto della migrazione e i minori a rischio di sottrazione da parte di un genitore.

La Commissione adotta altresì atti di esecuzione al fine di stabilire e sviluppare le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al paragrafo 8.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

Articolo 33

Esecuzione dell'azione richiesta nella segnalazione

1. In caso di reperimento di una persona di cui all'articolo 32, le autorità competenti dello Stato membro di esecuzione comunicano, fatte salve le prescrizioni di cui al paragrafo 4, il suo luogo di soggiorno allo Stato membro segnalante.

2. In caso di persone che devono essere poste sotto protezione di cui all'articolo 32, paragrafo 1, lettere a), c), d) ed e), lo Stato membro di esecuzione consulta immediatamente le proprie autorità competenti e quelle dello Stato membro segnalante tramite lo scambio di informazioni supplementari per concordare senza indugio le misure da prendere. Le autorità competenti dello Stato membro di esecuzione possono, conformemente al diritto nazionale, porre tali persone sotto protezione per impedire loro di proseguire il loro viaggio.

3. Nel caso di minori, la decisione sulle misure da prendere o la decisione di porre il minore sotto protezione di cui al paragrafo 2 è adottata nel rispetto dell'interesse superiore del minore. Tali decisioni sono adottate immediatamente ed entro 12 ore dal reperimento del minore, eventualmente in consultazione con le pertinenti autorità per la tutela dei minori.

4. 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 di inserimento 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, segnalazioni 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 gli oggetti di cui all'articolo 38, paragrafo 2, lettere a), b), c), e), g), h) e k) siano collegati a una persona oggetto di segnalazione a norma del paragrafo 1 del presente articolo, possono essere inserite segnalazioni di tali oggetti per localizzare la persona. In tal caso la segnalazione della persona e la segnalazione dell'oggetto sono connesse in conformità dell'articolo 63.

3. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al paragrafo 2 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

Articolo 35

Esecuzione dell'azione richiesta nella segnalazione

Le informazioni richieste sono comunicate allo Stato membro segnalante 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 di inserimento delle segnalazioni

1. Le segnalazioni su persone, su oggetti di cui all'articolo 38, paragrafo 2, lettere a), b), c), e), g), h), j), k) e l), e su mezzi di pagamento diversi dai contanti sono inseriti, nel rispetto del diritto nazionale dello Stato membro segnalante, ai fini di controlli discreti, controlli di indagine o controlli specifici a norma dell'articolo 37, paragrafi 3, 4 e 5.

2. Nell'inserire le segnalazioni ai fini di controlli discreti, controlli di indagine o controlli specifici e qualora le informazioni richieste dallo Stato membro segnalante siano complementari rispetto a quelle previste dall'articolo 37, paragrafo 1, lettere da a) a h), lo Stato membro segnalante aggiunge alla segnalazione tutte le informazioni richieste. Se tali informazioni riguardano le categorie particolari di dati personali di cui all'articolo 10 della direttiva (UE) 2016/680, tali informazioni possono essere richieste solo se sono strettamente necessarie per conseguire la finalità specifica della segnalazione e per il reato in relazione al quale è stata inserita la segnalazione.

3. Può essere effettuata una segnalazione di persone ai fini di controlli discreti, controlli di indagine o controlli specifici ai fini della prevenzione, dell'accertamento, dell'indagine o del perseguimento 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 uno dei reati di cui all'articolo 2, paragrafi 1 e 2, della decisione quadro 2002/584/GAI;

b) qualora le informazioni di cui all'articolo 37, paragrafo 1, siano necessarie all'esecuzione di una pena detentiva o una misura di sicurezza privativa della libertà nei confronti di una persona condannata per uno dei reati di cui all'articolo 2, paragrafi 1 e 2, della decisione quadro 2002/584/GAI;

c) qualora la valutazione globale della persona, in particolare sulla base dei suoi precedenti penali, faccia supporre che possa commettere in avvenire uno dei reati di cui all'articolo 2, paragrafi 1 e 2, della decisione quadro 2002/584/GAI.

4. Inoltre, una segnalazione di persone ai fini di controlli discreti, controlli di indagine o controlli specifici può essere inserita conformemente al diritto 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 inserisce la segnalazione a norma del presente paragrafo informa gli altri Stati membri di tale segnalazione. Ciascuno Stato membro stabilisce a quali autorità sono trasmesse tali informazioni. Le informazioni sono trasmesse tramite gli uffici SIRENE.

5. Qualora esistano indizi concreti che gli oggetti di cui all'articolo 38, paragrafo 2, lettere a), b), c), e), g), h), j), k), l), o i mezzi di pagamento diversi dai contanti siano collegati ai reati gravi di cui al paragrafo 3 del presente articolo o alle gravi minacce di cui al paragrafo 4 del presente articolo, possono essere inserite segnalazioni di tali oggetti e può essere creata una connessione tra tali segnalazioni e quelle inserite ai sensi dei paragrafi 3 e 4 del presente articolo.

6. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al paragrafo 5 del presente articolo nonché le informazioni complementari di cui al paragrafo 2 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

Articolo 37

Esecuzione dell'azione richiesta nella segnalazione

1. Nell'ambito dei controlli discreti, dei controlli di indagine o dei controlli specifici, lo Stato membro di esecuzione raccoglie e trasmette allo Stato membro segnalante, totalmente o in parte le informazioni seguenti:

a) il fatto che sia stata localizzata la persona oggetto di una segnalazione o che siano stati localizzati gli oggetti di cui all'articolo 38, paragrafo 2, lettere a), b), c), e), g), h), j), k), l), o i mezzi di pagamento diversi dai contanti oggetto di una segnalazione;

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 in bianco o del documento di identità rilasciato, di cui si può ragionevolmente presumere che siano associati alla persona interessata;

e) qualsiasi identità rivelata e qualsiasi descrizione personale della persona che usa il documento in bianco o il documento di identità rilasciato oggetto della segnalazione;

f) gli oggetti di cui all'articolo 38, paragrafo 2, lettere a), b), c), e), g), h), j), k) e l), o i mezzi di pagamento diversi dai contanti usati;

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

h) le circostanze in cui sono stati localizzati la persona o gli oggetti di cui all'articolo 38, paragrafo 2, lettere a), b), c), e), g), h), j), k) e l), o i mezzi di pagamento diversi dai contanti;

i) qualsiasi altra informazione richiesta dallo Stato membro segnalante in conformità dell'articolo 36, paragrafo 2.

Se riguardano le categorie particolari di dati personali di cui all'articolo 10 della direttiva (UE) 2016/680, le informazioni di cui al primo comma, lettera i), del presente paragrafo sono trattate conformemente alle condizioni previste da detto articolo e solo se integrano altri dati personali trattati per la stessa finalità.

2. Lo Stato membro di esecuzione comunica le informazioni di cui al paragrafo 1 tramite lo scambio di informazioni supplementari.

3. Il controllo discreto comprende la raccolta discreta del maggior numero possibile di informazioni descritte al paragrafo 1 durante le attività abituali svolte dalle autorità nazionali competenti dello Stato membro di esecuzione. La raccolta di tali informazioni non compromette la natura discreta dei controlli e la persona oggetto della segnalazione non viene in alcun modo informata dell'esistenza della segnalazione.

4. Il controllo di indagine consiste nell'interrogatorio della persona, anche sulla base delle informazioni o delle domande specifiche aggiunte alla segnalazione dallo Stato membro segnalante ai sensi dell'articolo 36, paragrafo 2. L'interrogatorio è effettuato conformemente al diritto interno dello Stato membro di esecuzione.

5. Nell'ambito dei controlli specifici, le persone, i veicoli, i natanti, gli aeromobili, i container e gli oggetti trasportati possono essere perquisiti ai fini di cui all'articolo 36. Le perquisizioni sono svolte conformemente al diritto nazionale dello Stato membro di esecuzione.

6. Se il diritto nazionale dello Stato membro di esecuzione non lo autorizza, il controllo specifico è convertito, per lo Stato membro in questione, in controllo di indagine. Se il diritto nazionale dello Stato membro di esecuzione non lo autorizza, il controllo di indagine è convertito, per lo Stato membro in questione, in controllo discreto. Qualora si applichi la direttiva 2013/48/UE, gli Stati membri provvedono a che il diritto di indagati e imputati di avvalersi di un difensore sia rispettato alle condizioni previste da detta direttiva.

7. Il paragrafo 6 lascia impregiudicato l'obbligo degli Stati membri di mettere a disposizione degli utenti finali le informazioni richieste ai sensi dell'articolo 36, paragrafo 2.

CAPO X

Segnalazione di oggetti a fini di sequestro o di prova in un procedimento penale

Articolo 38

Obiettivi e condizioni di inserimento delle segnalazioni

1. Gli Stati membri segnalanti inseriscono nel SIS le segnalazioni relative agli oggetti ricercati a fini di sequestro o di prova in un procedimento penale.

2. Le segnalazioni sono inserite relativamente alle categorie di oggetti agevolmente identificabili indicate di seguito:

a) veicoli a motore 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) motori per aeromobili;

j) armi da fuoco;

k) documenti ufficiali in bianco rubati, altrimenti sottratti, smarriti o pretesi tali ma falsi;

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

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

n) banconote (banconote registrate) e banconote false;

o) prodotti informatici;

p) componenti identificabili di veicoli a motore;

q) componenti identificabili di macchinari industriali;

r) altri oggetti di elevato valore identificabili definiti conformemente al paragrafo 3.

Per quanto riguarda i documenti di cui alle lettere k), l) e m), lo Stato membro segnalante può specificare se tali documenti siano rubati, altrimenti sottratti, smarriti, non validi o falsi.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 75 per modificare il presente regolamento definendo le nuove sottocategorie di oggetti di cui al paragrafo 2, lettere o), p), q) e r) del presente articolo.

4. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme tecniche necessarie per l'inserimento, l'aggiornamento, la cancellazione e la consultazione dei dati di cui al paragrafo 2 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, 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 competente sequestra l'oggetto conformemente al diritto nazionale e si mette in contatto con l'autorità dello Stato membro 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 lo scambio di informazioni supplementari.

3. Lo Stato membro di esecuzione adotta le misure richieste conformemente al diritto nazionale.

CAPO XI

Segnalazione di ignoti ricercati a fini di identificazione in conformità del diritto nazionale

Articolo 40

Segnalazione di ignoti ricercati a fini di identificazione in conformità del diritto nazionale

Gli Stati membri possono inserire nel SIS segnalazioni su ignoti ricercati contenenti solamente dati dattiloscopici. Tali dati dattiloscopici sono serie complete o incomplete di impronte digitali o impronte palmari rinvenute sul luogo di un reato di terrorismo o di un altro reato grave oggetto di indagine. Sono inseriti nel SIS solo qualora si possa stabilire con un grado molto elevato di probabilità che appartengono a un autore del reato.

Se l'autorità competente dello Stato membro segnalante non può stabilire l'identità del sospettato sulla base di dati di altre pertinenti banche dati nazionali, dell'Unione o internazionali, i dati dattiloscopici di cui al primo comma possono essere inseriti nella categoria di segnalazioni di cui trattasi con la dicitura «ignoto ricercato» solo allo scopo di identificare tale persona.

Articolo 41

Esecuzione dell'azione richiesta nella segnalazione

In caso di riscontro positivo (hit) con i dati inseriti a norma dell'articolo 40, l'identità della persona è stabilita conformemente al diritto nazionale, contestualmente alla verifica da parte di esperti che i dati dattiloscopici nel SIS appartengano a tale persona. Gli Stati membri di esecuzione comunicano le informazioni sull'identità e il luogo di soggiorno della persona allo Stato membro segnalante tramite lo scambio di informazioni supplementari per agevolare una tempestiva indagine del caso.

CAPO XII

Norme specifiche per i dati biometrici

Articolo 42

Norme specifiche per l'inserimento di fotografie, immagini del volto, dati dattiloscopici e profili DNA

1. Sono inseriti nel SIS unicamente le fotografie, le immagini del volto e i dati dattiloscopici di cui all'articolo 20, paragrafo 3, lettere w) e y) che soddisfano norme minime di qualità dei dati e specifiche tecniche. Tali dati sono inseriti solo previo controllo di qualità volto ad accertare che siano state soddisfatte le norme minime di qualità dei dati e le specifiche tecniche.

2. I dati dattiloscopici inseriti nel SIS possono essere costituiti da una a dieci impronte digitali piane e da una a dieci impronte digitali rollate. Possono inoltre includere due impronte palmari.

3. Un profilo DNA può essere aggiunto alle segnalazioni solo nelle situazioni di cui all'articolo 32, paragrafo 1, lettera a), e previo controllo di qualità volto ad accertare il rispetto delle norme minime di qualità dei dati e delle specifiche tecniche e unicamente se non sono disponibili, o non sono sufficienti per l'identificazione, fotografie, immagini del volto 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 di tali persone. In caso di aggiunta di un profilo DNA ad una segnalazione, tale profilo contiene le informazioni minime strettamente necessarie per l'identificazione della persona scomparsa.

4. Per l'archiviazione dei dati biometrici di cui ai paragrafi 1 e 3 del presente articolo sono stabilite norme di qualità minima dei dati e specifiche tecniche in conformità del paragrafo 5 del presente articolo. Tali norme minime di qualità dei dati e specifiche tecniche stabiliscono il livello di qualità richiesto per l'uso dei dati ai fini della verifica dell'identità di una persona in conformità dell'articolo 43, paragrafo 1, e per l'uso dei dati ai fini dell'identificazione di una persona in conformità dell'articolo 43, paragrafi 2, 3 e 4.

5. La Commissione adotta atti di esecuzione al fine di stabilire norme minime di qualità dei dati e specifiche tecniche di cui ai paragrafi 1, 3 e 4 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

Articolo 43

Norme specifiche per la verifica o l'interrogazione tramite fotografie, immagini del volto, dati dattiloscopici e profili DNA

1. Qualora siano disponibili fotografie, immagini del volto, dati dattiloscopici e profili DNA in una segnalazione nel SIS, tali fotografie, immagini del volto, dati dattiloscopici e profili DNA sono usati per confermare l'identità di una persona reperita grazie all'interrogazione del SIS con dati alfanumerici.

2. I dati dattiloscopici possono essere consultati in tutti i casi per identificare una persona. Tuttavia, i dati dattiloscopici devono essere consultati per identificare una persona quando l'identità della persona non può essere accertata con altri mezzi. A tal fine il SIS centrale contiene un sistema automatico per il riconoscimento delle impronte digitali (AFIS).

3. I dati dattiloscopici nel SIS in relazione a segnalazioni inserite a norma degli articoli 26, 32, 36 e 40 possono essere consultati anche usando serie complete o incomplete di impronte digitali o palmari rinvenute sul luogo di un reato grave o di un reato di terrorismo oggetto di indagine, qualora si possa stabilire con un elevato grado di probabilità che tali serie di impronte appartengono a un autore del reato, purché l'interrogazione sia effettuata simultaneamente nelle pertinenti banche dati nazionali di impronte digitali dello Stato membro.

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 del volto per identificare una persona presso valichi di frontiera regolari.

Prima che questa funzionalità sia attuata nel SIS, la Commissione presenta una relazione sulla disponibilità, sullo stato di preparazione e sull'affidabilità della tecnologia necessaria. Il Parlamento europeo è consultato in merito alla relazione.

Dopo l'inizio dell'uso della funzionalità ai valichi di frontiera regolari, alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 75 per integrare il presente regolamento riguardo alla determinazione degli altri casi in cui è possibile ricorrere a fotografie e immagini del volto per identificare le persone.

CAPO XIII

Diritto di accesso e riesame delle segnalazioni

Articolo 44

Autorità nazionali competenti con diritto di accesso ai dati nel SIS

1. Le autorità nazionali competenti hanno accesso ai dati inseriti nel SIS e il diritto di consultarli direttamente o su una copia di dati del SIS ai fini:

a) dei controlli di frontiera, a norma del regolamento (UE) 2016/399;

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

c) della prevenzione, dell'accertamento, dell'indagine **o** del perseguimento di reati di terrorismo o di altri reati gravi o dell'esecuzione di sanzioni penali, nello Stato membro interessato, purché si applichi la direttiva (UE) 2016/680;

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, compreso sui permessi di soggiorno e sui visti per soggiorni di lunga durata, e in materia di rimpatrio di cittadini di paesi terzi, nonché delle verifiche sui cittadini di paesi terzi che entrano o soggiornano illegalmente nel territorio degli Stati membri;

e) dei controlli di sicurezza sui cittadini di paesi terzi che chiedono la protezione internazionale, nella misura in cui tali autorità che eseguono i controlli non si configurino come «autorità accertanti» ai sensi dell'articolo 2, lettera f), della direttiva 2013/32/UE del Parlamento europeo e del Consiglio ([1]) e, se del caso, della consulenza fornita in conformità del regolamento (CE) n. 377/2004 del Consiglio ([2]);

2. Il diritto di accesso ai dati nel SIS e il diritto di consultarli direttamente possono essere esercitati dalle autorità nazionali competenti che sono responsabili della naturalizzazione, come previsto nel diritto interno, ai fini dell'esame della domanda di naturalizzazione.

3. 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 di un'imputazione, nell'assolvimento delle loro funzioni, come previsto nel diritto nazionale, e dalle relative autorità di coordinamento.

4. Le autorità competenti di cui al presente articolo sono inserite nell'elenco di cui all'articolo 56, paragrafo 7.

Articolo 45

Servizi competenti per l'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 ([3]) hanno accesso ai dati inseriti nel SIS a norma dell'articolo 38, paragrafo 2, lettere a), b), c), m) e p) del presente regolamento, al solo scopo di verificare che i veicoli e le relative carte di circolazione e targhe di cui è richiesta l'immatricolazione non siano stati rubati, altrimenti sottratti o smarriti o siano falsi o non siano ricercati a fini di prova in un procedimento penale.

L'accesso ai dati da parte dei servizi di cui al primo comma, è disciplinato dal diritto nazionale ed 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 nel SIS.

([1]) Direttiva 2013/32/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, recante procedure comuni ai fini del riconoscimento e della revoca dello status di protezione internazionale (GU L 180 del 29.6.2013, pag. 60).

([2]) Regolamento (CE) n. 377/2004 del Consiglio, del 19 febbraio 2004, relativo alla creazione di una rete di funzionari di collegamento incaricati dell'immigrazione (GU L 64 del 2.3.2004, pag. 1).

([3]) 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).

3. I servizi di cui al paragrafo 1 del presente articolo che non sono servizi pubblici accedono ai dati nel SIS soltanto per il tramite di un'autorità di cui all'articolo 44. 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 non si applica all'accesso al SIS ottenuto a norma del presente articolo. La comunicazione alle autorità giudiziarie o di polizia, ad opera dei servizi di cui al paragrafo 1 del presente articolo, di informazioni ottenute mediante la consultazione del SIS è disciplinata dal diritto nazionale.

Articolo 46

Servizi competenti per l'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, compresi i relativi motori, 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, e gli aeromobili, compresi i relativi motori, di cui è richiesta l'immatricolazione o che 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;

d) dati relativi a motori per aeromobili.

L'accesso ai dati da parte dei servizi di cui al primo comma è disciplinato dal diritto nazionale ed 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 nel SIS.

3. I servizi di cui al paragrafo 1 del presente articolo che non sono servizi pubblici accedono ai dati nel SIS soltanto per il tramite di un'autorità di cui all'articolo 44. 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 non si applica all'accesso al SIS ottenuto a norma del presente articolo. La comunicazione alle autorità giudiziarie o di polizia, ad opera dei servizi di cui al paragrafo 1 del presente articolo di informazioni ottenute mediante la consultazione del SIS, è disciplinata dal diritto nazionale.

Articolo 47

Servizi competenti per la registrazione di armi da fuoco

1. I servizi competenti negli Stati membri per il rilascio dei certificati di registrazione per le armi da fuoco hanno accesso ai dati relativi alle persone inseriti nel SIS a norma degli articoli 26 e 36 e ai dati relativi alle armi da fuoco inseriti nel SIS a norma dell'articolo 38, paragrafo 2. L'accesso è esercitato per verificare se la persona che chiede la registrazione sia ricercata per l'arresto a fini di consegna o di estradizione o ai fini di un controllo discreto, di indagine o specifico, o se le armi da fuoco di cui è richiesta la registrazione siano ricercate a fini di sequestro o di prova in un procedimento penale.

2. L'accesso ai dati da parte dei servizi di cui al paragrafo 1 è disciplinato dal diritto nazionale ed è limitato alle specifiche competenze dei servizi interessati.

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

4. I servizi di cui al paragrafo 1 che non sono servizi governativi hanno accesso ai dati nel SIS solo per il tramite di un'autorità di cui all'articolo 44. Tale autorità ha il diritto di accedere direttamente ai dati e informa il servizio interessato se l'arma da fuoco può essere registrata o meno. 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.

5. L'articolo 39 non si applica all'accesso al SIS ottenuto a norma del presente articolo. La comunicazione alle autorità giudiziarie o di polizia, ad opera dei servizi di cui al paragrafo 1 del presente articolo, di informazioni ottenute mediante la consultazione del SIS è disciplinata dal diritto nazionale.

Articolo 48

Accesso di Europol ai dati SIS

1. L'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), istituita dal regolamento (UE) 2016/794, ove necessario all'adempimento del suo mandato, ha il diritto di accedere ai dati nel SIS e di consultarli. Europol può anche scambiare e richiedere ulteriori informazioni supplementari in conformità delle disposizioni del manuale SIRENE.

2. Qualora un'interrogazione effettuata da Europol riveli la presenza di una segnalazione nel SIS, Europol ne informa lo Stato membro segnalante tramite lo scambio di informazioni supplementari a mezzo dell'infrastruttura di comunicazione e conformemente alle disposizioni del manuale SIRENE. Finché non è in grado di utilizzare le funzionalità previste per lo scambio di informazioni supplementari, Europol informa lo Stato membro segnalante tramite i canali definiti dal regolamento (UE) 2016/794.

3. Europol può trattare le informazioni supplementari fornitele dagli Stati membri a fini di raffronto con le proprie banche dati e i progetti di analisi operativa, allo scopo di identificare collegamenti o altri nessi pertinenti e per le analisi strategiche, tematiche od operative di cui all'articolo 18, paragrafo 2, lettere a), b) e c), del regolamento (UE) 2016/794. Qualsiasi trattamento di informazioni supplementari da parte di Europol ai fini del presente articolo è effettuato in conformità di tale regolamento.

4. L'uso da parte di Europol delle informazioni ottenute tramite un'interrogazione del SIS o tramite il trattamento di informazioni supplementari è soggetto al consenso dello Stato membro segnalante. 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 segnalante e in modo pienamente conforme alla normativa dell'Unione in materia di protezione dei dati.

5. Europol:

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

b) in deroga all'articolo 31, paragrafo 1, del regolamento (UE) 2016/794, cancella le informazioni supplementari contenenti dati personali entro un anno dalla cancellazione della relativa segnalazione. A titolo di deroga, se Europol dispone di informazioni nelle proprie banche dati o nei progetti di analisi operativa su un caso cui si riferiscono le informazioni supplementari, Europol può, in via eccezionale, continuare a conservare le informazioni supplementari per svolgere i suoi compiti, ove necessario. Europol informa lo Stato membro segnalante e quello di esecuzione dell'ulteriore conservazione di tali informazioni supplementari e ne fornisce una giustificazione;

c) limita l'accesso ai dati nel SIS, comprese le informazioni supplementari, al proprio personale specificamente autorizzato che necessita dell'accesso a tali dati per l'assolvimento dei propri compiti;

d) adotta e applica misure per garantire la sicurezza, la riservatezza e l'autocontrollo a norma degli articoli 10, 11 e 13;

e) provvede affinché il proprio personale autorizzato a trattare i dati del SIS riceva una formazione e informazioni adeguate a norma dell'articolo 14, paragrafo 1; e

f) fatto salvo il regolamento (UE) 2016/794, consente al Garante europeo della protezione dei dati di sorvegliare ed esaminare le attività da essa svolte nell'esercizio del suo diritto di accesso ai dati nel SIS e di consultazione degli stessi e nello scambio e nel trattamento di informazioni supplementari.

6. Europol duplica dal SIS i dati contenuti soltanto per fini tecnici, sempreché tale duplicazione sia necessaria per la consultazione diretta da parte di personale debitamente autorizzato di Europol. Il presente regolamento si applica a tali copie. La copia tecnica è usata solamente 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 i dati di una segnalazione né i dati complementari trasmessi dagli Stati membri o dal CS-SIS.

7. Per verificare la liceità del trattamento dei dati, per l'autocontrollo e per garantire un'adeguata sicurezza e integrità dei dati, Europol conserva registri di tutti gli accessi al SIS e le interrogazioni del SIS a norma dell'articolo 12. Tali registri e tale documentazione non sono considerati scaricamenti o duplicazioni illeciti di parti del SIS.

8. Gli Stati membri informano Europol, tramite lo scambio di informazioni supplementari, in merito a qualsiasi riscontro positivo (hit) su segnalazioni relative a reati di terrorismo. Gli Stati membri possono eccezionalmente non informare Europol, se ciò comprometterebbe le indagini in corso, la sicurezza di una persona, o sarebbe in contrasto con gli interessi essenziali della sicurezza dello Stato membro segnalante.

9. Il paragrafo 8 si applica a decorrere dalla data in cui Europol è in grado di ricevere informazioni supplementari in conformità del paragrafo 1.

Articolo 49

Accesso di Eurojust ai dati SIS

1. Solo i membri nazionali di Eurojust e i loro assistenti, ove necessario all'adempimento del loro mandato, hanno il diritto di accedere ai dati 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, quel membro nazionale informa al riguardo lo Stato membro segnalante. Eurojust comunica solamente le informazioni ottenute a seguito di detta interrogazione a paesi terzi e organismi terzi con il consenso dello Stato membro segnalante e nel pieno rispetto del diritto dell'Unione in materia di protezione dei dati.

3. Il presente articolo non pregiudica le disposizioni del regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio ([1]) e del regolamento (UE) 2018/1725 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 del Garante europeo della protezione dei dati a norma di detti regolamenti.

4. Per verificare la liceità del trattamento dei dati, per l'autocontrollo e per garantire un'adeguata sicurezza e integrità dei dati, Eurojust conserva registri di tutti gli accessi al SIS e tutte le interrogazioni del SIS effettuati da un membro nazionale di Eurojust o da un suo assistente conformemente alle disposizioni dell'articolo 12.

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

6. Eurojust adotta e applica misure per garantire la sicurezza, la riservatezza e l'autocontrollo a norma degli articoli 10, 11 e 13.

Articolo 50

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. A norma dell'articolo 40, paragrafo 8, del regolamento (UE) 2016/1624, i membri delle squadre ai sensi dell'articolo 2, punti 8) e 9), di tale regolamento hanno, nell'ambito dei rispettivi mandati e a condizione che siano autorizzati a effettuare controlli a norma dell'articolo 44, paragrafo 1, del presente regolamento e abbiano ricevuto la formazione necessaria a norma dell'articolo 14, paragrafo 1, del presente regolamento il diritto di accedere ai dati nel SIS e di consultarli, nella misura in cui ciò sia necessario per l'assolvimento dei loro compiti e sia richiesto dal piano operativo per un'operazione specifica. L'accesso ai dati nel SIS non è esteso ad altri membri delle squadre.

2. I membri delle squadre di cui al paragrafo 1 esercitano il diritto di accedere ai dati nel SIS e di consultarli in conformità del paragrafo 1 tramite un'interfaccia tecnica. L'interfaccia tecnica è istituita e gestita dall'Agenzia europea della guardia di frontiera e costiera e permette un collegamento diretto con il SIS centrale.

3. Qualora un'interrogazione effettuata da un membro delle squadre di cui al paragrafo 1 del presente articolo 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 intervengono 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. Per verificare la liceità del trattamento dei dati, per l'autocontrollo e per garantire un'adeguata sicurezza e integrità dei dati, l'Agenzia europea della guardia di frontiera e costiera conserva registri di tutti gli accessi al SIS e le interrogazioni del SIS in conformità dell'articolo 12.

5. L'Agenzia europea della guardia di frontiera e costiera adotta e applica misure per garantire la sicurezza, la riservatezza e l'autocontrollo a norma degli articoli 10, 11 e 13 e provvede affinché le squadre di cui al paragrafo 1 del presente articolo applichino tali misure.

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

([1]) Regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio, del 14 novembre 2018, sull'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) e che sostituisce e abroga la decisione 2002/187/GAI del Consiglio (GU L 295 del 21.11.2018, pag. 138).

7. Fatto salvo il paragrafo 2, nessuna parte del SIS è collegata a un sistema di raccolta e trattamento di dati gestito dalle squadre di cui al paragrafo1 o dall'Agenzia europea della guardia di frontiera e costiera, e nessun dato nel SIS a cui hanno accesso tali squadre è trasferito a tale sistema. Nessuna parte del SIS può essere scaricata o copiata. La registrazione degli accessi e delle interrogazioni non è considerata scaricamento o duplicazione illecita di dati nel SIS.

8. L'Agenzia europea della guardia di frontiera e costiera consente al Garante europeo della protezione dei dati di sorvegliare ed esaminare le attività svolte dalle squadre di cui al presente articolo nell'esercizio del loro diritto di accesso ai dati nel SIS e di consultazione degli stessi. Ciò non pregiudica le ulteriori disposizioni del regolamento (UE) 2018/1725.

Articolo 51

Valutazione dell'uso del SIS da parte di Europol, di Eurojust e dell'Agenzia europea della guardia di frontiera e costiera

1. La Commissione effettua almeno ogni cinque anni una valutazione dell'esercizio e dell'uso del SIS da parte di Europol, dei membri nazionali di Eurojust e dei loro assistenti nonché delle squadre di cui all'articolo 50, paragrafo 1.

2. Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera garantiscono un seguito adeguato alle conclusioni e alle raccomandazioni risultanti da tale valutazione.

3. Una relazione sui risultati della valutazione e sul relativo seguito è trasmessa al Parlamento europeo e al Consiglio.

Articolo 52

Ambito dell'accesso

Gli utenti finali, compresi Europol, i membri nazionali di Eurojust e i loro assistenti nonché i membri delle squadre ai sensi dell'articolo 2, punti 8) e 9), del regolamento (UE) 2016/1624, accedono solo ai dati necessari per l'assolvimento dei loro compiti.

Articolo 53

Periodo di riesame delle segnalazioni di persone

1. Le segnalazioni di persone sono conservate esclusivamente per il periodo necessario a realizzare le finalità per le quali sono state inserite.

2. Uno Stato membro può segnalare una persona ai fini di cui all'articolo 26 e all'articolo 32, paragrafo 1, lettere a) e b), per un periodo di cinque anni. Lo Stato membro segnalante riesamina la necessità di mantenere la segnalazione entro tale periodo di cinque anni.

3. Uno Stato membro può segnalare una persona ai fini di cui agli articoli 34 e 40 per un periodo di tre anni. Lo Stato membro segnalante riesamina la necessità di mantenere la segnalazione entro tale periodo di tre anni.

4. Uno Stato membro può segnalare una persona ai fini di cui all'articolo 32, paragrafo 1, lettere c), d) ed e), e all'articolo 36 per un periodo di un anno. Lo Stato membro segnalante riesamina la necessità di mantenere la segnalazione entro tale periodo di un anno.

5. Ciascuno Stato membro fissa, se del caso, tempi di riesame più brevi conformemente al diritto nazionale.

6. Nel periodo di riesame di cui ai paragrafi 2, 3 e 4, lo Stato membro segnalante può decidere, a seguito di una valutazione individuale globale che è registrata, di mantenere la segnalazione di una persona per un periodo più a lungo del periodo di riesame, ove ciò sia necessario e proporzionato alle finalità per le quali la segnalazione stessa era stata inserita. In tali casi, i paragrafi 2, 3 o 4 si applicano anche a tale proroga. Ogni proroga è comunicata al CS-SIS.

7. Le segnalazioni di persone sono cancellate automaticamente allo scadere del periodo di riesame di cui ai paragrafi 2, 3 e 4, salvo qualora lo Stato membro segnalante abbia informato il CS-SIS della proroga a norma del paragrafo 6. Il CS-SIS segnala automaticamente allo Stato membro segnalante, con quattro mesi d'anticipo, la prevista cancellazione di dati.

8. Gli Stati membri redigono statistiche sul numero di segnalazioni di persone il cui periodo di conservazione è stato prorogato a norma del paragrafo 6 del presente articolo e le trasmettono, su richiesta, alle autorità di controllo di cui all'articolo 69.

9. Non appena risulti chiaro all'ufficio SIRENE che una segnalazione di una persona ha conseguito il suo obiettivo e deve pertanto essere cancellata, esso ne informa immediatamente l'autorità autrice della segnalazione. L'autorità dispone di 15 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 ricezione di una risposta alla scadenza del periodo di 15 giorni, l'ufficio SIRENE provvede affinché la segnalazione sia cancellata. Laddove consentito dal diritto nazionale, la segnalazione è cancellata dall'ufficio SIRENE. Gli uffici SIRENE segnalano alla rispettiva autorità di controllo i problemi ricorrenti incontrati nell'attività svolta ai sensi del presente paragrafo.

Articolo 54

Periodo di riesame delle segnalazioni di oggetti

1. Le segnalazioni di oggetti sono conservate esclusivamente per il periodo necessario a realizzare le finalità per le quali sono state inserite.

2. Uno Stato membro può segnalare oggetti ai fini di cui agli articoli 36 e 38 per un periodo di dieci anni. Lo Stato membro segnalante riesamina la necessità di mantenere la segnalazione entro tale periodo di dieci anni.

3. Le segnalazioni di oggetti inserite a norma degli articoli 26, 32, 34 e 36 sono riesaminate a norma dell'articolo 53, se collegate alla segnalazione di una persona. Tali segnalazioni sono conservate solo finché è conservata la segnalazione della persona.

4. Nel periodo di riesame di cui ai paragrafi 2 e 3, lo Stato membro segnalante può decidere di mantenere la segnalazione di un oggetto per un periodo più lungo del periodo di riesame, ove ciò sia necessario alle finalità per le quali la segnalazione stessa era stata inserita. In tali casi si applica il paragrafo 2 o, se opportuno, il paragrafo 3.

5. La Commissione può adottare atti di esecuzione per stabilire tempi di riesame più brevi per talune categorie di segnalazioni di oggetti. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

6. Gli Stati membri redigono statistiche sul numero di segnalazioni di oggetti il cui periodo di conservazione è stato prorogato a norma del paragrafo 4.

CAPO XIV

Cancellazione delle segnalazioni

Articolo 55

Cancellazione delle segnalazioni

1. Le segnalazioni per l'arresto a fini di consegna o estradizione ai sensi dell'articolo 26 sono cancellate allorché la persona è stata consegnata o estradata alle autorità competenti dello Stato membro segnalante. Sono altresì cancellate allorché la decisione giudiziaria su cui le segnalazioni si basavano è stata revocata dall'autorità giudiziaria competente in conformità del diritto nazionale. Le segnalazioni sono cancellate alla loro scadenza ai sensi dell'articolo 53.

2. Le segnalazioni di persone scomparse o di persone vulnerabili a cui deve essere impedito di viaggiare a norma dell'articolo 32 sono cancellate secondo le norme seguenti:

a) per quanto riguarda i minori scomparsi e i minori a rischio di sottrazione, la segnalazione è cancellata:

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

   ii) allo scadere del termine di validità della segnalazione conformemente all'articolo 53; o

   iii) su decisione dell'autorità competente dello Stato membro segnalante;

b) per quanto riguarda gli adulti scomparsi per i quali non siano richieste misure di protezione, la segnalazione è cancellata:

   i) una volta eseguita l'azione richiesta quando il luogo di soggiorno è stato individuato da parte dello Stato membro di esecuzione;

   ii) allo scadere del termine di validità della segnalazione conformemente all'articolo 53; o

   iii) su decisione dell'autorità competente dello Stato membro segnalante;

c) per quanto riguarda gli adulti scomparsi per i quali siano richieste misure di protezione, la segnalazione è cancellata:

   i) una volta eseguita l'azione richiesta quando la persona è posta sotto protezione;

ii) allo scadere del termine di validità della segnalazione conformemente all'articolo 53; o

iii) su decisione dell'autorità competente dello Stato membro segnalante;

d) per quanto riguarda le persone vulnerabili maggiorenni a cui, ai fini della loro tutela, deve essere impedito di viaggiare e i minori a cui deve essere impedito di viaggiare, la segnalazione è cancellata:

i) una volta eseguita l'azione richiesta, ad esempio ponendo la persona sotto protezione;

ii) allo scadere del termine di validità della segnalazione conformemente all'articolo 53; o

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

Fatto salvo il diritto nazionale, qualora una persona sia stata istituzionalizzata su decisione dell'autorità competente, la segnalazione può essere mantenuta fino al suo rimpatrio.

3. Le segnalazioni riguardanti persone ricercate nell'ambito di un procedimento giudiziario ai sensi dell'articolo 34, sono cancellate:

a) all'atto della comunicazione del luogo di soggiorno della persona all'autorità competente dello Stato membro segnalante;

b) allo scadere del termine di validità della segnalazione conformemente all'articolo 53; o

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

Se non è possibile dare seguito alle informazioni trasmesse di cui alla lettera a), l'ufficio SIRENE dello Stato membro segnalante ne informa l'ufficio SIRENE dello Stato membro di esecuzione affinché sia risolto il problema

Nel caso sia ottenuto un riscontro positivo (hit) in cui i dati riguardanti l'indirizzo erano stati trasmessi allo Stato membro segnalante e successivamente sia ottenuto, nello stesso Stato membro di esecuzione, un riscontro positivo (hit) che rivela gli stessi dati riguardanti l'indirizzo, tale riscontro positivo (hit) 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 (hit) ripetuto lo Stato membro segnalante, il quale svolge una valutazione individuale globale della necessità di mantenere la segnalazione.

4. Le segnalazioni ai fini di un controllo discreto, di indagine o specifico ai sensi dell'articolo 36, sono cancellate:

a) allo scadere del termine di validità della segnalazione conformemente all'articolo 53; o

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

5. Le segnalazioni di oggetti a fini di sequestro o di prova ai sensi dell'articolo 38, sono cancellate:

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 i competenti uffici SIRENE o che l'oggetto sia sottoposto ad altra procedura giudiziaria o amministrativa;

b) allo scadere del termine di validità della segnalazione conformemente all'articolo 53; o

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

6. Le segnalazioni di ignoti ricercati di cui all'articolo 40 sono cancellate:

a) quando è identificata la persona;

b) allo scadere del termine di validità della segnalazione conformemente all'articolo 53; o

c) su decisione di cancellare la segnalazione dell'autorità competente dello Stato membro segnalante.

7. Le segnalazioni di oggetti inserite a norma degli articoli 26, 32, 34 e 36, se collegate alla segnalazione di una persona, sono cancellate se la segnalazione di una persona è cancellata a norma del presente articolo.

CAPO XV

Regole generali sul trattamento dei dati

Articolo 56

Trattamento dei dati SIS

1. Gli Stati membri trattano 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 sono duplicati soltanto per fini tecnici, qualora tale duplicazione sia necessaria per la consultazione diretta da parte delle autorità competenti di cui all'articolo 44. Il presente regolamento si applica a tali copie. Gli Stati membri non copiano i dati di una segnalazione o i dati complementari inseriti da un altro Stato membro dal proprio N.SIS o dal CS-SIS in un altro sistema di dati nazionale.

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.

Gli Stati membri tengono un inventario aggiornato di tali copie, lo rendono accessibile alle rispettive autorità di controllo e assicurano che il presente regolamento, in particolare l'articolo 10, si applichi a tali copie.

4. L'accesso ai dati del SIS da parte delle autorità nazionali competenti di cui all'articolo 44 è autorizzato esclusivamente nei limiti delle loro competenze e riservato solamente al personale debitamente autorizzato.

5. Per quanto riguarda le segnalazioni di cui agli articoli 26, 32, 34, 36, 38 e 40 del presente regolamento, ogni trattamento delle informazioni nel SIS per finalità diverse da quelle per le quali sono state inserite nel SIS deve essere connesso a un caso specifico e giustificato dalla necessità di prevenire una minaccia grave ed 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 necessario ottenere l'autorizzazione preventiva dello Stato membro segnalante.

6. Qualsiasi uso dei dati del SIS non conforme ai paragrafi da 1 a 5 del presente articolo è considerato un abuso ai sensi del diritto interno di ciascuno Stato membro ed è soggetto a sanzioni in conformità dell'articolo 73.

7. Ciascuno Stato membro invia all'eu-LISA l'elenco delle proprie autorità competenti autorizzate a consultare direttamente i dati 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 per quali finalità. L'eu-LISA provvede affinché l'elenco sia pubblicato annualmente nella *Gazzetta ufficiale dell'Unione europea*. L'eu-LISA mantiene sul proprio sito web un elenco sempre aggiornato contenente le modifiche trasmesse dagli Stati membri tra una pubblicazione annuale e l'altra.

8. Sempreché il diritto dell'Unione non preveda specifiche disposizioni, la legislazione di ciascuno Stato membro si applica ai dati del rispettivo N.SIS.

Articolo 57

Dati SIS e archivi nazionali

1. L'articolo 56, 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 eseguita 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 56, paragrafo 2, non pregiudica il diritto di uno Stato membro di conservare nel proprio archivio nazionale i dati contenuti in una segnalazione particolare inserita nel SIS da quello stesso Stato membro.

Articolo 58

Informazione nel caso di mancata esecuzione di una segnalazione

Se l'azione richiesta non può essere eseguita, lo Stato membro la cui azione è richiesta ne informa senza indugio lo Stato membro segnalante tramite lo scambio di informazioni supplementari.

Articolo 59

Qualità dei dati nel SIS

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

2. Qualora uno Stato membro segnalante riceva pertinenti dati complementari o modificati di cui all'articolo 20, paragrafo 3, esso completa o modifica senza indugio la segnalazione.

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

4. Qualora uno Stato membro diverso dallo Stato membro segnalante disponga di pertinenti dati complementari o modificati di cui all'articolo 20, paragrafo 3, esso li trasmette senza indugio, tramite lo scambio di informazioni supplementari, allo Stato membro segnalante per consentirgli di completare o modificare la segnalazione. Se i dati complementari o modificati riguardano le persone, essi sono trasmessi solo se l'identità della persona è accertata.

5. Se uno Stato membro diverso dallo Stato membro segnalante è in possesso di elementi che dimostrano che detti dati contengono errori di fatto o sono stati archiviati illecitamente, ne informa al più presto, tramite lo scambio di informazioni supplementari ed entro due giorni lavorativi dacché è in possesso di detti elementi, lo Stato membro segnalante. Lo Stato membro segnalante verifica l'informazione e, se necessario, rettifica o cancella senza indugio i dati in questione.

6. Se, entro due mesi dal momento in cui sono emersi gli elementi ai sensi del paragrafo 5 del presente articolo, gli Stati membri non giungono a un accordo, lo Stato membro che non ha inserito la segnalazione sottopone la questione alle autorità nazionali di controllo interessate e al Garante europeo della protezione dei dati affinché prendano una decisione mediante cooperazione in conformità dell'articolo 71.

7. Gli Stati membri si scambiano informazioni supplementari nei casi in cui una persona presenta un reclamo nel quale fa valere di non essere la persona oggetto della segnalazione. Se dalla verifica risulta che la persona oggetto della segnalazione non è il reclamante, il reclamante è informato delle disposizioni dell'articolo 62 e del suo diritto di ricorso di cui all'articolo 68, paragrafo 1.

Articolo 60

Incidenti di sicurezza

1. È considerato incidente di sicurezza qualunque evento che ha o possa avere ripercussioni sulla sicurezza del SIS o possa causare danni o perdite ai dati SIS o alle informazioni supplementari, in particolare quando possano essere stati consultati dati illecitamente o quando sono state o possano 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. Fatte salve la notifica e la comunicazione di una violazione dei dati personali a norma dell'articolo 33 del regolamento (UE) 2016/679 o dell'articolo 30 della direttiva (UE) 2016/680, gli Stati membri, Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera comunicano senza indugio gli incidenti di sicurezza alla Commissione, all'eu-LISA, all'autorità di controllo competente e al Garante europeo della protezione dei dati. L'eu-LISA comunica senza indugio qualsiasi incidente di sicurezza relativo al CS-SIS alla Commissione e al Garante europeo della protezione dei dati.

4. Le informazioni su un incidente di sicurezza che ha o possa avere ripercussioni sul funzionamento del SIS in uno Stato membro o nell'eu-LISA, o sulla disponibilità, integrità e riservatezza dei dati inseriti o inviati da altri Stati membri o sulle informazioni supplementari scambiate, sono trasmesse senza indugio a tutti gli Stati membri e registrate secondo il piano di gestione degli incidenti stabilito dall'eu-LISA.

5. Gli Stati membri e l'eu-LISA collaborano qualora si verifichino incidenti di sicurezza.

6. La Commissione segnala immediatamente al Parlamento europeo e al Consiglio gli incidenti gravi. Tali segnalazioni sono classificate EU RESTRICTED/RESTREINT UE conformemente alle norme vigenti in materia di sicurezza.

7. Qualora un incidente di sicurezza sia causato da un uso improprio dei dati, gli Stati membri, Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera garantiscono l'imposizione di sanzioni in conformità dell'articolo 73.

Articolo 61

Distinzione tra persone con caratteristiche simili

1. Quando, inserendo una nuova segnalazione, risulta evidente che nel SIS è già presente una segnalazione relativa a una persona che possiede la stessa descrizione dell'identità, l'ufficio SIRENE si mette in contatto entro dodici ore con lo Stato membro segnalante, tramite lo scambio di informazioni supplementari, allo scopo di verificare se la segnalazione riguardi o meno la stessa persona.

2. Se da tale controllo incrociato risulta che la persona oggetto di una nuova segnalazione e quella oggetto di una segnalazione già inserita nel SIS sono effettivamente la stessa persona, l'ufficio SIRENE applica la procedura per l'inserimento di segnalazioni multiple di cui all'articolo 23.

3. Qualora la verifica del controllo incrociato stabilisca che si tratta di due persone diverse, l'ufficio SIRENE convalida la richiesta di inserimento della seconda segnalazione aggiungendo i dati necessari per evitare errori di identificazione.

Articolo 62

Dati complementari per trattare i casi di usurpazione di identità

1. Quando sono possibili confusioni fra la persona 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 la cui identità è stata usurpata, dati che la riguardano per evitare le conseguenze negative di un errore di identificazione. La persona la cui identità sia stata usurpata ha il diritto di revocare il proprio consenso al trattamento dei dati aggiunti.

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; e

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, e previo consenso esplicito della persona la cui identità è stata usurpata per ogni categoria di dati, possono essere inseriti e successivamente trattati nel SIS soltanto i seguenti dati della persona la cui identità è stata usurpata:

a) cognomi;

b) nomi;

c) nomi e cognomi alla nascita;

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

e) segni fisici particolari, oggettivi e inalterabili;

f) il luogo di nascita;

g) la data di nascita;

h) il genere;

i) le fotografie e immagini del volto;

j) le impronte digitali, impronte palmari o entrambe;

k) tutte le cittadinanze possedute;

l) la categoria dei documenti di identificazione;

m) il paese di rilascio dei documenti di identificazione;

n) il numero dei documenti di identificazione;

o) la data di rilascio dei documenti di identificazione;

p) l'indirizzo della persona;

q) il nome del padre della persona;

r) il nome della madre della persona.

4. La Commissione adotta atti di esecuzione al fine di stabilire e sviluppare le norme tecniche necessarie per l'inserimento e il successivo trattamento dei dati di cui al paragrafo 3 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, 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 63

Connessioni fra segnalazioni

1. Uno Stato membro può creare una connessione tra segnalazioni che introduce nel SIS. Effetto della connessione è instaurare 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 periodo di riesame.

3. La creazione di una connessione non incide sui diritti di accesso previsti dal 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. Qualora uno Stato membro ritenga che la creazione di una connessione tra segnalazioni da parte di un altro Stato membro sia incompatibile con il suo diritto 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. La Commissione adotta atti di esecuzione per stabilire e sviluppare le norme tecniche necessarie per la connessione tra segnalazioni. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

Articolo 64

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 le finalità per le quali sono stati forniti. Essi sono in ogni caso cancellati entro un anno dalla cancellazione della relativa segnalazione dal SIS.

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 inserita o a una segnalazione in collegamento con la quale è stata eseguita un'azione nel suo territorio. Il periodo per cui tali dati possono essere conservati in tali archivi è disciplinato dal diritto nazionale.

Articolo 65

Trasferimento di dati personali a terzi

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

CAPO XVI

Protezione dei dati

Articolo 66

Legislazione applicabile

1. Il regolamento (UE) 2018/1725 si applica al trattamento dei dati personali da parte dell' eu-LISA, dell'Agenzia europea della guardia di frontiera e costiera e di Eurojust in conformità del presente regolamento. Il regolamento (UE) 2016/794 si applica al trattamento dei dati personali da parte di Europol in conformità del presente regolamento.

2. La direttiva (UE) 2016/680 si applica al trattamento dei dati personali in conformità del presente regolamento da parte delle autorità nazionali competenti e dei servizi ai fini di prevenzione, accertamento, indagine o perseguimento di reati o esecuzione di sanzioni penali, comprese la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

3. Il regolamento (UE) 2016/679 si applica al trattamento dei dati personali in conformità del presente regolamento da parte delle autorità nazionali competenti e dei servizi, a eccezione del trattamento a fini di prevenzione, accertamento, indagine o perseguimento di reati o esecuzione di sanzioni penali, comprese la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Articolo 67

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

1. Gli interessati possono esercitare i diritti di cui agli articoli 15, 16 e 17 del regolamento (UE) 2016/679 e agli articoli 14 e 16, paragrafi 1 e 2, della direttiva (UE) 2016/680.

2. Uno Stato membro diverso dallo Stato membro segnalante può fornire a un interessato informazioni sui dati trattati, e che sono dati personali dell'interessato, soltanto se dà prima la possibilità allo Stato membro segnalante di prendere posizione. Alla comunicazione tra tali Stati membri si provvede tramite scambio di informazioni supplementari.

3. Gli Stati membri possono decidere di non fornire informazioni all'interessato, in tutto o in parte, in conformità del diritto 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 dell'interessato al fine di:

a) non ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari;

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

c) proteggere la sicurezza pubblica;

d) proteggere la sicurezza nazionale; oppure

e) proteggere i diritti e le libertà altrui.

Nei casi di cui al primo comma, lo Stato membro informa l'interessato, senza ingiustificato ritardo e per iscritto, di ogni rifiuto o limitazione dell'accesso e dei motivi del rifiuto o della limitazione. Dette informazioni possono essere omesse qualora la loro comunicazione rischi di compromettere una delle finalità di cui al primo comma, lettere da a) a e). Lo Stato membro informa l'interessato della possibilità di proporre un reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale.

Lo Stato membro fornisce i motivi di fatto o di diritto su cui si basa la decisione di non fornire le informazioni all'interessato. Tali informazioni sono rese disponibili alle autorità di controllo.

In tali casi, l'interessato deve poter esercitare i propri diritti anche tramite le autorità di controllo competenti.

4. In seguito a una richiesta di accesso, rettifica o cancellazione, lo Stato membro informa l'interessato non appena possibile e comunque entro i termini di cui all'articolo 12, paragrafo 3, del regolamento (UE) 2016/679 del seguito dato all'esercizio dei diritti di cui al presente articolo.

Articolo 68

Mezzi di impugnazione

1. Fatte salve le disposizioni sui mezzi di impugnazione di cui al regolamento (UE) 2016/679 e alla direttiva (UE) 2016/680, chiunque può adire qualsiasi autorità competente, tra cui l'autorità giudiziaria, in base al diritto di qualsiasi Stato membro, per accedere, rettificare, cancellare, 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 dalle autorità giudiziarie o dalle autorità di cui al paragrafo 1 del presente articolo, fatto salvo l'articolo 72.

3. Gli Stati membri presentano relazioni annuali al comitato europeo per la protezione dei dati su:

a) il numero di richieste di accesso presentate 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 all'autorità 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 di cancellazione dei dati archiviati illecitamente che sono state 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 che sono state presentate all'autorità di controllo;

e) il numero di procedimenti giudiziari avviati;

f) il numero di cause in cui l'autorità giudiziaria ha statuito a favore del ricorrente;

g) eventuali osservazioni sui casi di riconoscimento reciproco delle decisioni definitive emesse dalle autorità giudiziarie o dalle autorità di altri Stati membri in merito a segnalazioni inserite dallo Stato membro segnalante.

Un modello per le relazioni di cui al presente paragrafo è elaborato dalla Commissione.

4. Le relazioni degli Stati membri sono incluse nella relazione congiunta di cui all'articolo 71, paragrafo 4.

Articolo 69

Controllo dell'N.SIS

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

2. Le autorità di controllo provvedono 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 è svolto dalle autorità di controllo oppure da queste commissionato direttamente a un revisore per la protezione di dati indipendente. Le autorità di controllo mantengono in qualsiasi momento il controllo sul revisore indipendente e la responsabilità del suo operato.

3. Gli Stati membri provvedono affinché le rispettive autorità di controllo dispongano delle risorse sufficienti per assolvere i compiti ad esse assegnati a norma del presente regolamento e possano avvalersi della consulenza di persone in possesso di adeguate conoscenze in materia di dati biometrici.

Articolo 70

Controllo dell'eu-LISA

1. Il Garante europeo della protezione dei dati ha il compito di sorvegliare le attività di trattamento dei dati personali da parte dell'eu-LISA e di assicurare che tali attività siano effettuate in conformità del presente regolamento. Si applicano di conseguenza i compiti e le competenze di cui agli articoli 57 e 58 del regolamento (UE) 2018/1725.

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

Articolo 71

Cooperazione tra le autorità di controllo e il Garante europeo della protezione dei dati

1. Le autorità 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 le autorità di controllo e il garante europeo della protezione dei dati, ciascuno nell'ambito delle proprie competenze, 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 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. I costi di tali riunioni e la gestione delle stesse sono a carico del comitato europeo per la protezione dei dati. Nella prima riunione è adottato un regolamento interno. Ulteriori metodi di lavoro sono elaborati congiuntamente, se necessario.

4. Ogni anno il comitato europeo per la protezione dei dati trasmette al Parlamento europeo, al Consiglio e alla Commissione una relazione congiunta sulle attività inerenti al controllo coordinato.

CAPO XVII

Responsabilità e sanzioni

Articolo 72

Responsabilità

1. Fatti salvi il diritto al risarcimento e la responsabilità ai sensi del regolamento (UE) 2016/679, della direttiva (UE) 2016/680 e del regolamento (UE) 2018/1725.

a) ogni persona o Stato membro che abbia subito danni materiali o immateriali, in conseguenza di un trattamento illecito di dati personali in seguito all'uso dell'N.SIS o di qualsiasi altro atto incompatibile con il presente regolamento compiuti da uno Stato membro, ha diritto al risarcimento da parte di quest'ultimo; e

b) ogni persona o Stato membro che abbia subito danni materiali o immateriali in conseguenza di qualsiasi atto incompatibile con il presente regolamento compiuto dall'eu-LISA ha diritto al risarcimento da parte della stessa.

Uno Stato membro o l'eu-LISA sono esonerati in tutto o in parte dalla responsabilità di cui al primo comma se provano che l'evento che ha dato luogo al danno non è loro imputabile.

2. Uno Stato membro è ritenuto responsabile di ogni eventuale danno arrecato al SIS conseguente all'inosservanza degli obblighi del presente regolamento, fatto salvo il caso e nella misura in cui l'eu-LISA o un altro Stato membro che partecipa al SIS abbiano omesso di adottare provvedimenti ragionevolmente idonei a prevenire il danno o ridurne al minimo l'impatto.

3. Le azioni proposte contro uno Stato membro per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono disciplinate dal diritto nazionale di tale Stato membro. Le azioni proposte contro l'eu-LISA per il risarcimento dei danni di cui ai paragrafi 1 e 2 sono soggette alle condizioni previste dai trattati.

Articolo 73

Sanzioni

Gli Stati membri provvedono affinché l'eventuale uso improprio o trattamento dei dati conservati nel SIS o qualsiasi scambio di informazioni supplementari in contrasto con il presente regolamento sia punibile ai sensi del diritto nazionale.

Le sanzioni previste sono effettive, proporzionate e dissuasive.

CAPO XVIII

Disposizioni finali

Articolo 74

Controllo e statistiche

1. L'eu-LISA provvede affinché siano attivate procedure atte a controllare il funzionamento del SIS in rapporto agli obiettivi prefissati in termini di risultato, di rapporto costi/benefici, di sicurezza e di qualità del servizio.

2. Ai fini della manutenzione tecnica, delle relazioni, delle relazioni sulla qualità dei dati, e delle statistiche, l'eu-LISA ha accesso alle informazioni necessarie riguardanti le operazioni di trattamento effettuate nel SIS centrale.

3. L'eu-LISA pubblica statistiche giornaliere, mensili e annuali relative al numero di registrazioni per categoria di segnalazione, sia per ciascuno Stato membro sia su base aggregata. L'eu-LISA pubblica inoltre relazioni annuali relative al numero di riscontri positivi (hit) 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, sia per ciascuno Stato membro sia su base aggregata. Le statistiche prodotte non contengono dati personali. La relazione statistica annuale è pubblicata.

4. Gli Stati membri, Europol, Eurojust e l'Agenzia europea della guardia di frontiera e costiera forniscono all'eu-LISA e alla Commissione le informazioni necessarie per redigere le relazioni di cui ai paragrafi 3, 6, 8 e 9.

5. 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 dei servizi competenti negli Stati membri per il rilascio di certificati di immatricolazione o per la gestione del traffico di natanti, compresi i relativi motori, di aeromobili, compresi i relativi motori, e di armi da fuoco. Le statistiche riportano anche il numero di riscontri positivi (hit) per categoria di segnalazione.

6. L'eu-LISA trasmette al Parlamento europeo, al Consiglio, agli Stati membri, alla Commissione, a Europol, a Eurojust e all'Agenzia europea della guardia di frontiera e costiera nonché al Garante europeo della protezione dei dati tutte le relazioni statistiche che produce.

Per controllare l'attuazione degli atti giuridici dell'Unione, anche ai fini del regolamento (UE) n. 1053/2013, la Commissione può chiedere all'eu-LISA di fornire specifiche relazioni statistiche aggiuntive, periodicamente o ad hoc, sulle prestazioni del SIS, sull'uso del SIS e sullo scambio di informazioni supplementari.

L'Agenzia europea della guardia di frontiera e costiera può chiedere all'eu-LISA di fornire specifiche relazioni statistiche aggiuntive, periodicamente o ad hoc, ai fini dello svolgimento di analisi di rischio e valutazioni della vulnerabilità di cui agli articoli 11 e 13 del regolamento (UE) 2016/1624.

7. Ai fini dell'articolo 15, paragrafo 4, e dei paragrafi 3, 4 e 6 del presente articolo l'eu-LISA istituisce, attua e ospita un archivio centrale nei suoi siti tecnici contenente i dati di cui all'articolo 15, paragrafo 4, e al paragrafo 3 del presente articolo che non consentono l'identificazione delle persone fisiche e che permettono alla Commissione e alle agenzie di cui paragrafo 6 del presente articolo di ottenere relazioni e statistiche personalizzate. Su richiesta, l'eu-LISA concede agli Stati membri e alla Commissione, nonché a Europol, a Eurojust e all'Agenzia europea della guardia di frontiera e costiera, nella misura necessaria all'assolvimento dei loro compiti, l'accesso all'archivio centrale mediante un accesso protetto tramite l'infrastruttura di comunicazione. L'eu-LISA attua controlli dell'accesso e specifici profili di utente allo scopo di assicurare che all'archivio centrale si abbia accesso unicamente ai fini dell'elaborazione di relazioni e statistiche.

8. Due anni dopo la data di applicazione del presente regolamento a norma dell'articolo 79, paragrafo 5, primo comma, e successivamente ogni due anni, l'eu-LISA presenta al Parlamento europeo e al Consiglio una relazione sul funzionamento tecnico del SIS centrale e dell'infrastruttura di comunicazione, che comprenda la loro sicurezza, sull'AFIS e sullo scambio bilaterale e multilaterale di informazioni supplementari fra Stati membri. Una volta la tecnologia in uso, la relazione contiene altresì una valutazione del ricorso alle immagini del volto per accertare l'identità delle persone.

9. Tre anni dopo la data di applicazione del presente regolamento a norma dell' articolo 79, paragrafo 5, primo comma, e successivamente ogni quattro anni, la Commissione svolge 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 il perdurare della 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 relazione di valutazione comprende altresì una valutazione dell'AFIS e delle campagne d'informazione sul SIS svolte dalla Commissione a norma dell'articolo 19.

La Commissione trasmette la relazione di valutazione al Parlamento europeo e al Consiglio.

10. La Commissione adotta atti di esecuzione per stabilire le modalità dettagliate del funzionamento dell'archivio centrale di cui al paragrafo 7 del presente articolo e le norme sulla protezione dei dati e sulla sicurezza applicabili a tale archivio. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 76, paragrafo 2.

Articolo 75

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 38, paragrafo 3, e all'articolo 43, paragrafo 4, è conferito alla Commissione per un periodo indeterminato a decorrere dal 27 dicembre 2018.

3. La delega di potere di cui all'articolo 38, paragrafo 3, e all'articolo 43, paragrafo 4, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere specificata nella decisione. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale del 13 aprile 2016 «Legiferare meglio».

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 38, paragrafo 3, o dell'articolo 43, paragrafo 4, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 76

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è 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 77

Modifiche alla decisione 2007/533/GAI

La decisione 2007/533/GAI è così modificata:

1) l'articolo 6 è sostituito dal seguente:

«*Articolo 6*

Sistemi nazionali

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

2. Ciascuno Stato membro è responsabile di garantire la disponibilità ininterrotta dei dati SIS II agli utenti finali.»;

2) l'articolo 11 è sostituito dal seguente:

«*Articolo 11*

Riservatezza - Stati membri

1. 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 II e con le informazioni supplementari, conformemente alla propria legislazione nazionale. Tale obbligo vincola tali soggetti e organismi anche dopo che avranno rispettivamente lasciato l'incarico o cessato di lavorare, ovvero portato a termine le proprie attività.

2. Se collabora con contraenti esterni per un qualsiasi compito relativo al SIS II, lo Stato membro monitora da vicino le attività del contraente per garantire il rispetto di tutte le disposizioni della presente decisione, in particolare sulla sicurezza, la riservatezza e la protezione dei dati.

3. La gestione operativa dell'N.SIS II o delle copie tecniche non può essere affidata a imprese o organizzazioni private.»;

3) l'articolo 15 è così modificato:

a) è inserito il paragrafo seguente:

«3 bis. L'organo di gestione sviluppa e gestisce un meccanismo e procedure per lo svolgimento dei controlli di qualità sui dati contenuti nel CS-SIS.

Esso riferisce periodicamente agli Stati membri a tale riguardo. L'organo di gestione riferisce periodicamente alla Commissione in merito ai problemi incontrati, dandone comunicazione anche agli Stati membri interessati.

La Commissione riferisce periodicamente al Parlamento europeo e al Consiglio in merito ai problemi di qualità dei dati incontrati.»;

b) il paragrafo 8 è sostituito dal seguente:

«8. La gestione operativa del SIS II centrale consiste nell'insieme dei compiti necessari al funzionamento del SIS II centrale 24 ore su 24 e 7 giorni su 7, ai sensi della presente decisione, e comprende in particolare le attività di manutenzione e gli adattamenti tecnici necessari per il buon funzionamento del sistema. Tali compiti comprendono anche il coordinamento, la gestione e il sostegno delle attività di collaudo per il SIS II centrale e i N.SIS II che garantiscono che il SIS II centrale e i N.SIS II operino secondo i requisiti per la conformità tecnica di cui all'articolo 9.»;

4) all'articolo 17 sono aggiunti i paragrafi seguenti:

«3. Se collabora con contraenti esterni per un qualsiasi compito relativo al SIS II, l'organo di gestione monitora da vicino le attività del contraente per garantire il rispetto di tutte le disposizioni della presente decisione, in particolare sulla sicurezza, la riservatezza e la protezione dei dati.

4. La gestione operativa del CS-SIS non può essere affidata a imprese o organizzazioni private.»;

5) all'articolo 21, è aggiunto il comma seguente:

«Allorché si ricerchi una persona o un oggetto nell'ambito di una segnalazione connessa a un reato di terrorismo, il caso è ritenuto adeguato, pertinente e sufficientemente importante da giustificare l'esistenza della segnalazione nel SIS II. Per motivi di sicurezza pubblica o nazionale, gli Stati membri possono eccezionalmente astenersi dall'inserire una segnalazione, quando la stessa rischi di ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari.»;

6) l'articolo 22 è sostituito dal seguente:

«*Articolo 22*

Norme specifiche per l'inserimento, la verifica o l'interrogazione tramite fotografie e impronte digitali

1. Fotografie e impronte digitali possono essere inserite solo previo controllo speciale di qualità per accertare che soddisfino gli standard minimi di qualità dei dati. Le specifiche sul controllo speciale di qualità sono stabilite secondo la procedura di cui all'articolo 67.

2. Qualora siano disponibili dati relativi alle fotografie e alle impronte digitali in una segnalazione nel SIS II, tali fotografie e impronte digitali sono usati per confermare l'identità di una persona reperita grazie all'interrogazione del SIS II con dati alfanumerici.

3. I dati relativi alle impronte digitali possono essere consultati in tutti i casi per identificare una persona. Tuttavia, i dati relativi alle impronte digitali devono essere consultati a fini di identificazione se l'identità della persona non può essere accertata con altri mezzi. A tal fine il SIS II centrale contiene un sistema automatico per il riconoscimento delle impronte digitali (AFIS).

4. I dati relativi alle impronte digitali nel SIS II in relazione a segnalazioni inserite a norma degli articoli 26, 32 e 36 possono essere consultati anche usando serie complete o incomplete di impronte digitali rinvenute sul luogo di un reato grave o di un reato di terrorismo oggetto di indagine, qualora si possa stabilire con un elevato grado di probabilità che quelle serie di impronte appartengono a un autore del reato, e purché l'interrogazione sia effettuata simultaneamente nelle pertinenti banche dati nazionali di impronte digitali dello Stato membro.»;

7) l'articolo 41 è sostituito dal seguente:

«*Articolo 41*

Accesso di Europol ai dati nel SIS II

1. L'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), istituita dal regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio (*) ove necessario all'adempimento del suo mandato, ha il diritto di accedere ai dati nel SIS II e di consultarli. Europol può altresì scambiare e richiedere ulteriori informazioni supplementari in conformità delle disposizioni del manuale SIRENE.

2. Qualora un'interrogazione effettuata da Europol riveli la presenza di una segnalazione nel SIS II, Europol ne informa lo Stato membro segnalante tramite lo scambio di informazioni supplementari a mezzo dell'infrastruttura di comunicazione e conformemente alle disposizioni del manuale SIRENE. Finché non è in grado di utilizzare le funzionalità previste per lo scambio di informazioni supplementari, Europol informa lo Stato membro segnalante tramite i canali definiti dal regolamento (UE) 2016/794.

3. Europol può trattare le informazioni supplementari fornitele dagli Stati membri al fine di raffrontarle con le proprie banche dati e i progetti di analisi operativa, allo scopo di identificare collegamenti o altri nessi pertinenti e per analisi strategiche, tematiche od operative di cui all'articolo 18, paragrafo 2, lettere a), b) e c), del regolamento (UE) 2016/794. Qualsiasi trattamento di informazioni supplementari da parte di Europol ai fini del presente articolo è effettuato in conformità a tale regolamento.

4. L'uso da parte di Europol delle informazioni ottenute tramite un'interrogazione del SIS II o tramite il trattamento di informazioni supplementari è soggetto al consenso dello Stato membro segnalante. 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 segnalante e nel pieno rispetto della normativa dell'Unione in materia di protezione dei dati.

5. Europol:

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

b) in deroga all'articolo 31, paragrafo 1, del regolamento (UE) 2016/794, cancella le informazioni supplementari contenenti dati personali entro un anno dalla cancellazione della relativa segnalazione. A titolo di deroga, se Europol dispone di informazioni nelle proprie banche dati o nei progetti di analisi operativa su un caso cui si riferiscono le informazioni supplementari, Europol può, in via eccezionale, continuare a conservare le informazioni supplementari per svolgere i suoi compiti, ove necessario. Europol informa lo Stato membro segnalante e quello di esecuzione dell'ulteriore conservazione di tali informazioni supplementari e fornisce una giustificazione;

c) limita l'accesso ai dati nel SIS II, comprese le informazioni supplementari, al proprio personale specificamente autorizzato che necessita dell'accesso a tali dati ai fini dell'assolvimento dei propri compiti;

d) adotta e applica misure per garantire la sicurezza, la riservatezza e l'autocontrollo a norma degli articoli 10, 11 e 13;

e) provvede affinché il proprio personale autorizzato a trattare i dati SIS II riceva una formazione e informazioni adeguate a norma dell'articolo 14;

f) fatto salvo il regolamento (UE) 2016/794, consente al Garante europeo della protezione dei dati di sorvegliare ed esaminare le attività da essa svolte nell'esercizio del suo diritto di accesso ai dati nel SIS II e di consultazione degli stessi e nello scambio e nel trattamento di informazioni supplementari.

6. Europol può duplicare i dati dal SIS II soltanto per fini tecnici, sempreché tale duplicazione sia necessaria per la consultazione diretta da parte del personale debitamente autorizzato di Europol. La presente decisione si applica a tali copie. La copia tecnica è usata al fine di conservare i dati SIS II 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 II. Europol si astiene dal copiare in altri sistemi di Europol i dati di una segnalazione o i dati complementari trasmessi dagli Stati membri o dal CS-SIS II.

7. Per verificare la liceità del trattamento dei dati, per l'autocontrollo e per garantire un'adeguata sicurezza e integrità dei dati, Europol conserva registri di tutti gli accessi al SIS II e le interrogazioni del SIS II in conformità delle disposizioni dell'articolo 12. Tali registri e tale documentazione non sono considerati scaricamenti o duplicazioni illeciti di parti del SIS II.

8. Gli Stati membri informano Europol, tramite lo scambio di informazioni supplementari, in merito a qualsiasi riscontro positivo (hit) su segnalazioni relative a reati di terrorismo. Gli Stati membri possono eccezionalmente non informare Europol, se ciò comprometterebbe le indagini in corso, la sicurezza di una persona, o sarebbe in contrasto con gli interessi essenziali della sicurezza dello Stato membro segnalante.

9. Il paragrafo 8 si applica a decorrere dalla data in cui Europol è in grado di ricevere informazioni supplementari in conformità del paragrafo 1.

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

8) è inserito l'articolo seguente:

«*Articolo 42 bis*

Accesso ai dati del SIS II 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. A norma dell'articolo 40, paragrafo 8, del regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio (*), i membri delle squadre di cui all'articolo 2, punti 8) e 9), di tale regolamento hanno, nell'ambito dei rispettivi mandati e a condizione che siano autorizzati a effettuare controlli a norma dell'articolo 40, paragrafo 1, della presente decisione e abbiano ricevuto la formazione necessaria a norma dell'articolo 14 della presente decisione, il diritto di accedere ai dati nel SIS II e di consultarli, nella misura in cui ciò sia necessario per l'assolvimento dei loro compiti e sia richiesto dal piano operativo per un'operazione specifica. L'accesso ai dati nel SIS II non è esteso ad altri membri delle squadre.

2. I membri delle squadre di cui al paragrafo 1 esercitano il diritto di accedere ai dati nel SIS II e di consultarli in conformità del paragrafo 1 tramite un'interfaccia tecnica. L'interfaccia tecnica è istituita e gestita dall'Agenzia europea della guardia di frontiera e costiera e permette un collegamento diretto con il SIS II centrale.

3. Qualora un'interrogazione effettuata da un membro delle squadre di cui al paragrafo 1 del presente articolo riveli l'esistenza di una segnalazione nel SIS II, lo Stato membro segnalante ne è informato. In conformità dell'articolo 40 del regolamento (UE) 2016/1624, i membri delle squadre intervengono esclusivamente in risposta a una segnalazione nel SIS II 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. Per verificare la liceità del trattamento dei dati, per l'autocontrollo e per garantire un'adeguata sicurezza e integrità dei dati, l'Agenzia europea della guardia di frontiera e costiera conserva registri di tutti gli accessi al SIS II e le interrogazioni del SIS II in conformità delle disposizioni dell'articolo 12.

5. L'Agenzia europea della guardia di frontiera e costiera adotta e applica misure per garantire la sicurezza, la riservatezza e l'autocontrollo a norma degli articoli 10, 11 e 13 e provvede affinché le squadre di cui al paragrafo 1 del presente articolo applichino tali misure.

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

7. Fatto salvo il paragrafo 2, nessuna parte del SIS II è collegata a un sistema informatico di raccolta e trattamento di dati gestito dalle squadre di cui al paragrafo 1 o dall'Agenzia europea della guardia di frontiera e costiera, e nessun dato nel SIS II a cui hanno accesso tali squadre è trasferito a tale sistema. Nessuna parte del SIS II può essere scaricata o copiata. La registrazione degli accessi e delle interrogazioni non è considerata come scaricamento o duplicazione illecita di dati nel SIS II.

8. L'Agenzia europea della guardia di frontiera e costiera consente al Garante europeo della protezione dei dati di sorvegliare ed esaminare le attività svolte dalle squadre di cui al presente articolo nell'esercizio del loro diritto di accesso ai dati nel SIS II e di consultazione degli stessi. Ciò non pregiudica le ulteriori disposizioni del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio (**).

(*) Regolamento (UE) 2016/1624 del Parlamento europeo e del Consiglio, del 14 settembre 2016, relativo alla guardia di frontiera e costiera europea 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).

(**) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).».

Articolo 78

Abrogazione

Il regolamento (CE) n. 1986/2006 e le decisioni 2007/533/GAI e 2010/261/UE sono abrogati a decorrere dalla data di applicazione del presente regolamento di cui all'articolo 79, paragrafo 5, primo comma.

I riferimenti al regolamento (CE) n. 1986/2006 e alla decisione 2007/533/GAI abrogati si intendono fatti al presente regolamento e vanno letti secondo la tavola di concordanza di cui all'allegato.

Articolo 79

Entrata in vigore, inizio delle attività e applicazione

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

2. Entro il 28 dicembre 2021 la Commissione adotta una decisione che stabilisce la data a decorrere dalla quale le attività del SIS hanno inizio a norma del presente regolamento, dopo aver verificato che sono soddisfatte le condizioni seguenti:

a) che siano stati adottati gli atti di esecuzione necessari per l'applicazione del presente regolamento;

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

c) che l'eu-LISA abbia comunicato alla Commissione il positivo completamento di tutte le attività di collaudo relative al CS-SIS e all'interazione tra CS-SIS e N.SIS.

3. La Commissione controlla attentamente il processo del graduale rispetto delle condizioni di cui al paragrafo 2 e informa il Parlamento europeo e il Consiglio in merito all'esito della verifica di cui a tale paragrafo.

4. Entro il 28 dicembre 2019 e successivamente ogni anno fino all'adozione della decisione della Commissione di cui al paragrafo 2, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sullo stato di avanzamento dei preparativi per la piena attuazione del presente regolamento. Tale relazione contiene anche informazioni particolareggiate sulle spese sostenute e sugli eventuali rischi che possono incidere sui costi complessivi.

5. Il presente regolamento si applica a decorrere dalla data stabilita in conformità del paragrafo 2.

In deroga al primo comma:

a) l'articolo 4, paragrafo 4, l'articolo 5, l'articolo 8, paragrafo 4, l'articolo 9, paragrafi 1 e 5, l'articolo 12, paragrafo 8, l'articolo 15, paragrafo 7, l'articolo 19, l'articolo 20, paragrafi 4 e 5, l'articolo 26, paragrafo 6, l'articolo 32, paragrafo 9, l'articolo 34, paragrafo 3, l'articolo 36, paragrafo 6, l'articolo 38, paragrafi 3 e 4, l'articolo 42, paragrafo 5, l'articolo 43, paragrafo 4, l'articolo 54, paragrafo 5, l'articolo 62, paragrafo 4, l'articolo 63, paragrafo 6, l'articolo 74, paragrafi 7 e 10, gli articoli 75 e 76, l'articolo 77, punti da 1) a 5), e i paragrafi 3 e 4 del presente articolo si applicano a decorrere dalla data di entrata in vigore del presente regolamento;

b) l'articolo 77, punti 7) e 8), si applica a decorrere dal 28 dicembre 2019;

c) l'articolo 77, punto 6), si applica a decorrere dal 28 dicembre 2020.

6. La decisione della Commissione di cui al paragrafo 2 è pubblicata nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri conformemente ai trattati.

Fatto a Bruxelles, il 28 novembre 2018

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*La presidente*
A. TAJANI	K. EDTSTADLER

ALLEGATO

TAVOLA DI CONCORDANZA

Decisione 2007/533/GAI	Il presente regolamento
Articolo 1	Articolo 1
Articolo 2	Articolo 2
Articolo 3	Articolo 3
Articolo 4	Articolo 4
Articolo 5	Articolo 5
Articolo 6	Articolo 6
Articolo 7	Articolo 7
Articolo 8	Articolo 8
Articolo 9	Articolo 9
Articolo 10	Articolo 10
Articolo 11	Articolo 11
Articolo 12	Articolo 12
Articolo 13	Articolo 13
Articolo 14	Articolo 14
Articolo 15	Articolo 15
Articolo 16	Articolo 16
Articolo 17	Articolo 17
Articolo 18	Articolo 18
Articolo 19	Articolo 19
Articolo 20	Articolo 20
Articolo 21	Articolo 21
Articolo 22	Articoli 42 e 43
Articolo 23	Articolo 22
—	Articolo 23
Articolo 24	Articolo 24
Articolo 25	Articolo 25
Articolo 26	Articolo 26
Articolo 27	Articolo 27
Articolo 28	Articolo 28
Articolo 29	Articolo 29
Articolo 30	Articolo 30
Articolo 31	Articolo 31
Articolo 32	Articolo 32
Articolo 33	Articolo 33
Articolo 34	Articolo 34
Articolo 35	Articolo 35
Articolo 36	Articolo 36
Articolo 37	Articolo 37
Articolo 38	Articolo 38
Articolo 39	Articolo 39
—	Articolo 40
—	Articolo 41

Decisione 2007/533/GAI	Il presente regolamento
Articolo 40	Articolo 44
—	Articolo 45
—	Articolo 46
—	Articolo 47
Articolo 41	Articolo 48
Articolo 42	Articolo 49
—	Articolo 51
Articolo 42a	Articolo 50
Articolo 43	Articolo 52
Articolo 44	Articolo 53
Articolo 45	Articolo 54
—	Articolo 55
Articolo 46	Articolo 56
Articolo 47	Articolo 57
Articolo 48	Articolo 58
Articolo 49	Articolo 59
—	Articolo 60
Articolo 50	Articolo 61
Articolo 51	Articolo 62
Articolo 52	Articolo 63
Articolo 53	Articolo 64
Articolo 54	Articolo 65
Articolo 55	—
Articolo 56	—
Articolo 57	Articolo 66
Articolo 58	Articolo 67
Articolo 59	Articolo 68
Articolo 60	Articolo 69
Articolo 61	Articolo 70
Articolo 62	Articolo 71
Articolo 63	—
Articolo 64	Articolo 72
Articolo 65	Articolo 73
Articolo 66	Articolo 74
—	Articolo 75
Articolo 67	Articolo 76
Articolo 68	—
—	Articolo 77
Articolo 69	—
—	Articolo 78
Articolo 70	—
Articolo 71	Articolo 79

Regolamento (CE) n. 1986/2006	Il presente regolamento
Articoli 1, 2 e 3	Articolo 45