Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Mai 2022

Rapporto esplicativo concernente la revisione della legge federale del 25 settembre 2015 sulle attività informative

per l'avvio della procedura di consultazione

Rapporto esplicativo

1 Situazione iniziale

1.1 Necessità di agire e obiettivi

La legge sulle attività informative del 25 settembre 2015[1] (LAIn) è entrata in vigore il 1 settembre 2017. Già nel corso dei dibattiti parlamentari sono stati proposti la futura integrazione e l'esame di singoli disciplinamenti.

Per questo motivo, con decisione del 16 agosto 2017 sull'entrata in vigore della LAIn e delle relative ordinanze, il Consiglio federale ha incaricato il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), nell'ambito di una futura revisione della LAIn, ma al più tardi entro la fine del 2021, di creare nella LAIn e nella legge sul Parlamento del 13 dicembre 2002[2] (LParl) una base legale per la presentazione autonoma del preventivo da parte dell'autorità di vigilanza indipendente al fine di aumentarne ulteriormente l'indipendenza. Il 20 febbraio 2019 il Consiglio federale ha quindi incaricato il DDPS di presentargli, entro la fine di giugno del 2020, un avamprogetto per una revisione della LAIn in grado di essere sottoposto a procedura di consultazione. In particolare, dovrebbero essere valutati la delega dei compiti dell'Autorità di controllo indipendente per l'esplorazione radio e l'esplorazione dei segnali via cavo (ACI) all'Autorità di vigilanza indipendente sulle attività informative (AVI-AIn), gli adeguamenti nel settore delle misure di acquisizione soggette ad autorizzazione e gli adeguamenti di natura formale.

Punti essenziali:

Con decisione del 26 agosto 2020, il Consiglio federale ha prorogato fino alla fine del 2021 il termine per la presentazione del disegno di revisione. Allo stesso tempo ha incaricato il DDPS di ridefinire il disciplinamento dei sistemi di informazione e il diritto di ricevere informazioni ai sensi della legge riguardo ai dati del Servizio delle attività informative della Confederazione (SIC). Ciò si basava sulle proposte relative alla gestione dei dati informativi formulate dalla Delegazione della Commissione della gestione delle Camere federali (DelCG) nel suo rapporto annuale 2019[3]. Con l'entrata in vigore della versione riveduta della legge del 25 settembre 2020[4] sulla protezione dei dati (LPD*riv*) e nuovi sviluppi tecnologici nella gestione dei dati mutano ulteriori condizioni generali per il loro trattamento, inducendo il Consiglio federale a rivederne la conservazione da parte dei servizi informazioni (cfr. in merito il commento introduttivo prima dell'art. 44 segg.). A livello di volume, ciò rappresenta la parte principale dell'attuale progetto. A tale proposito il Consiglio federale ha prorogato il termine per la presentazione di un progetto di revisione pronto per la procedura di consultazione entro la fine del 2021.

Altri temi della presente revisione sono:

- misure supplementari per individuare tempestivamente e sventare l'estremismo violento, sulla base di diverse iniziative parlamentari successive a sviluppi negativi della situazione in materia di sicurezza (v. commento all'art. 27)
- un nuovo disciplinamento volto a chiarire il finanziamento di gravi minacce per la sicurezza del nostro Paese in risposta all'inasprimento della situazione in materia di sicurezza in vari settori della sicurezza interna ed esterna, quali il terrorismo, lo spionaggio e l'estremismo violento, disciplinamento che, a causa della portata dell'ingerenza nei diritti fondamentali, è impostato quale misura di acquisizione soggetta ad autorizzazione (v. commento all'art. 26)
- proposte di miglioramento per l'attuazione pratica della LAIn, formulate principalmente da organismi esterni sulla base delle prime esperienze fatte nell'esecuzione della LAIn
- adeguamenti linguistici per unificare la terminologia nelle tre lingue ufficiali.

1.2 Genesi del presente disegno di legge

Alla preparazione del progetto di revisione hanno partecipato rappresentanti dell'AVI-Ain e dell'ACI, del DDPS (Segreteria generale, Ufficio federale della protezione della popolazione UFPP, Servizio informazioni militare SIM, Centro operazioni elettroniche COE), del Dipartimento federale degli affari esteri (DFAE: Segreteria generale), del Dipartimento federale di giustizia e polizia (DFGP: Segreteria generale, Ufficio federale di giustizia UFG, Ufficio federale di polizia fedpol e Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni SCPT), del Ministero pubblico della Confederazione (MPC), della Cancelleria federale (CaF e Incaricato federale della protezione dei dati e della trasparenza IFPDT) nonché della Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP) e della Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS).

I gruppi di lavoro interdipartimentali guidati dal SIC hanno elaborato un progetto tematico. Le proposte di revisione inerenti alla vigilanza (art. 77 − 78*d*) sono state elaborate da AVI-Ain e ACI in modo autonomo. Le loro bozze sono state poi inserite nel progetto. A causa della situazione di rischio e dei provvedimenti volti ad arginare la pandemia di coronavirus, la maggior parte dei lavori e delle consultazioni si è svolta per corrispondenza.

1 RS **121**
2 RS **171.10**
3 FF **2020** 2659 segg., 2740
4 FF **2020** 6695

Su sua propria richiesta, il Tribunale amministrativo federale (TAF) non ha partecipato ai gruppi di lavoro. Il SIC lo ha tuttavia informato costantemente sullo stato di avanzamento dei lavori ed esso ha così avuto l'opportunità di esprimersi per scritto nell'ambito di una consultazione preliminare. È stato inoltre consultato per scritto durante la consultazione degli Uffici.

2 Commento ai singoli articoli

Per una migliore leggibilità dei commenti, tutti gli adeguamenti linguistici che non comportano modifiche materiali e riguardanti una sola lingua sono elencati all'inizio:

Concerne soltanto il testo francese:

Articoli 15, 18 e 35

Oggi, nell'ambito delle attività informative, si parla di «source humaine». Per questo in tutta la legge il termine «informateur» viene sostituito da «source humaine».

Articolo 23 capoverso 2

Il termine «audition» è sostituito dal termine «interrogatoire», utilizzato anche nell'articolo 24.

Articoli 39, 41 e 42

Il termine «du réseau câblé» è stralciato. La precisazione in merito al tipo di esplorazione non è necessaria, bensì si evince dall'argomento trattato nella Sezione sette, ossia l'esplorazione dei segnali via cavo.

« Réseau filaire » viene sostituito da « réseau câblé »; così facendo la terminologia viene uniformata in tutto il testo di legge (art. 39 cpv. 1 e 41, cpv. 1, lett. d).

Concerne soltanto il testo tedesco:

Nell'intero atto normativo il termine «orientiert» è sostituito dal termine «informiert».

Articoli 19 capoverso 3 e 20 capoverso 2

Il presente adeguamento si prefigge l'utilizzo uniforme in tutta la legge della formulazione « geheim halten ».

Articolo 32

Rubrica

Con l'integrazione della rubrica si evince immediatamente che si intende la fine della misura di acquisizione.

Capoverso 1 lettera c

Si tratta di un mero adeguamento linguistico della denominazione abituale « Vorsteherin oder Vorsteher des VBS » di cui all'articolo 37 della legge del 21 marzo 1997[5] sull'organizzazione del Governo e dell'Amministrazione (LOGA).

Concerne soltanto il testo italiano:

Articolo 39 capoverso 4 lettera c

Il termine «dei segnali via cavo» è stralciato. La precisazione in merito al tipo di esplorazione non è necessaria, bensì si evince dall'argomento trattato nella Sezione sette, ossia l'esplorazione dei segnali via cavo.

Seguono i commenti relativi alle modifiche materiali:

Articolo 1

Lettera a

L'attuale formulazione della LAIn sembra indicare che il SIC svolge i suoi compiti esclusivamente in virtù di quest'ultima, ma non è così. Come qualsiasi altro servizio, esso adempie anche compiti prettamente amministrativi in applicazione della LOGA. Partecipa ad esempio alle consultazioni degli uffici nell'ambito dell'elaborazione dei testi legislativi, oppure al trattamento di interventi parlamentari o ancora risponde alle richieste dei media. Inoltreil SIC assume, dirige e assiste il proprio personale, gestisce l'infrastruttura informatica, acquista beni amministrativi secondo il diritto in materia di acquisti pubblici e gestisce le proprie finanze. La menzione esplicita

5 RS **172.010**

delle attività informative nell'articolo 1 LAIn mette in chiaro che le altre attività amministrative del SIC non sono disciplinate in quest'ultima, ma si rifanno alle disposizioni generalmente applicabili per l'Amministrazione federale.

Lettera d

Poiché la LAIn disciplina anche la distinzione tra i dati informativi e quelli amministrativi e contiene taluni principi per il trattamento di questi ultimi, nell'articolo 1 si menziona ora anche il trattamento dei dati da parte del SIC quale oggetto di disciplinamento della LAIn.

Articolo 5

Anche se vi si cita soltanto il SIC, il presente articolo si applica anche alle autorità d'esecuzione cantonali. Ciò vale peraltro per tutte le norme di principio del presente disegno. Le suddette autorità sono menzionate esplicitamente unicamente quando una norma riguarda nello specifico solo loro o se è necessario evidenziarne i diritti e obblighi, perché altrimenti non sarebbe chiaro se l'autorità d'esecuzione cantonale è autorizzata a compiere un determinato atto.

Capoverso 5

I limiti posti sinora al trattamento dei dati informativi a favore dell'attività politica e dell'esercizio della libertà di opinione, di riunione o di associazione devono continuare a rimanere intatti. Tuttavia, il capoverso 6 descrive in modo più preciso di quanto fatto finora le eccezioni necessarie. La modifica è intesa a chiarire che i dati trattati dal SIC per adempiere i propri compiti amministrativi non rientrano nei suddetti limiti. Se, ad esempio, nell'adempiere i propri compiti amministrativi tratta affari del Parlamento che sono stati assegnati al SIC stesso, questi riguardano l'attività politica. Ne risultano anche dati personali non rilevanti ai fini dell'adempimento dei compiti informativi. I nomi degli autori e dei cofirmatari di interventi parlamentari riguardanti la sicurezza interna ed esterna sono quindi reperibili presso il SIC e sono parte integrante del titolo dell'oggetto. Anche nel trattamento delle richieste di informazioni in materia di diritto sulla protezione dei dati, risultano dati personali dalla relativa procedura. La loro conservazione presso il SIC serve a verificare la correttezza della fornitura delle informazioni e nel caso si adisca l'IFPDT. Il SIC è tenuto a memorizzare tali dati per un certo periodo di tempo, anche se non sono necessari per adempiere i compiti informativi.

Capoverso 6

Lettera a

Può succedere che al momento di ricevere i dati, in base alla fonte, al contenuto o al contesto, il nesso con i compiti da svolgere sembri assolutamente probabile, ma non sia ancora sicuro. Per decidere in merito sono necessari e possibili ulteriori chiarimenti. Così, ad esempio, un servizio partner può far pervenire al SIC una richiesta di informazioni inerente a una persona che nel suo Paese diffonde idee di estrema destra, il che già motiva una competenza dell'autorità estera. Poiché detta persona si è recata nel nostro Paese per un incontro, il servizio partner desidera ora sapere se il SIC dispone di informazioni al riguardo. In seguito, il SIC conferisce all'autorità d'esecuzione [cantonale] del Cantone in cui ha soggiornato la persona in questione un mandato affinché indaghi su quest'ultima. Soltanto il risultato del mandato dimostrerà se si tratta di un incontro tra estremisti violenti, in modo da poter stabilire se sussiste il nesso con i compiti e se è quindi ammesso un ulteriore trattamento dei dati. Ovviamente ciò può verificarsi anche per i dati che pervengono alle autorità d'esecuzione cantonali. Per ragioni di trasparenza, la procedura da seguire per il necessario chiarimento del presunto nesso è ora sancita in modo esplicito (cfr. in merito anche il commento all'art. 46 cpv. 2).

Lettera b

Il campo d'applicazione delle eccezioni disciplinate nel capoverso 6 era finora limitato al terrorismo, allo spionaggio e all'estremismo violento. Ciò era riconducibile alla legge federale del 21 marzo 1997[6] sulle misure per la salvaguardia della sicurezza interna (LMSI) che ancora non trattava il tema ciber e che presumeva non si sarebbe proceduto ad attività di proliferazione in violazione dei suddetti diritti fondamentali. Tuttavia, non vi è alcun motivo per cui nel settore della non proliferazione e nelle attività nel ciberspazio, significative in materia di politica di sicurezza, andrebbe tutelata la violazione dei diritti fondamentali menzionati nell'articolo 5 capoverso 5. Il campo d'applicazione di tale disposizione è pertanto esteso a tutte le attività di cui all'articolo 6 capoverso 1 lettera a. Si chiarisce così che il SIC può occuparsi, ad esempio, di dichiarazioni d'intenti su ciberattacchi o di informazioni su incontri preparatori. Nel settore della proliferazione, tuttavia, neanche con la nuova normativa i gruppi parlamentari di amicizia con Paesi rilevanti diventano oggetto di osservazione da parte del SIC. I gruppi sono sufficientemente sensibili per non farsi sfruttare a fini di attività di proliferazione.

Lettera c

Dal punto di vista dei servizi informazioni è importante sapere contro chi incombe la minaccia. Soltanto così il SIC può riferire con cognizione di causa e le autorità competenti possono adottare misure adeguate per avvisare e proteggere le persone e le organizzazioni minacciate. Non è un problema se esse non si avvalgono dei diritti fondamentali elencati nell'articolo 5 capoverso 5. Se, ad esempio, il SIC viene a conoscenza che è in progetto un attentato contro la sede centrale di un grande gruppo, può informarne quest'ultimo e la polizia cantonale competente e trattare dati in tal senso. In rari casi può però succedere che debbano essere tutelate anche persone o organizzazioni che si avvalgono dei loro diritti fondamentali particolarmente protetti. Se, ad esempio, il SIC viene informato che un politico sarà aggredito fisicamente durante un'apparizione pubblica, per proteggerlo deve essere autorizzato, eccezionalmente, a trattare dati inerenti alle sue pubbliche relazioni in ambito politico. Altri esempi sono gli attacchi di ciberspionaggio portati direttamente contro parlamentari o danneggiamenti di matrice estremista violenta contro un membro del governo responsabile della sanità pubblica. Ovviamente il trattamento dei dati in via eccezionale entra però in linea di conto in primo luogo soltanto per proteggere interessi importanti (ad es. vita e integrità della persona). L'ammissibilità in via eccezionale del trattamento dei dati da parte dei servizi informazioni sarà

6 RS **120**

ora estesa esplicitamente anche a persone e organizzazioni che potrebbero essere minacciate dalle attività menzionate nell'articolo 6 capoverso 1 lettere a. Così, ad esempio, associazioni con una quota elevata di stranieri sono finite ripetutamente nel mirino di autorità estere, con conseguenti possibili ciberattacchi, spionaggio con motivazione politica o anche aggressioni fisiche.

Lettera d

Ai fini della valutazione di un'informazione (ad es. per verificarne la correttezza) è altresì importante conoscerne la provenienza. Soltanto se il SIC sa da chi proviene l'informazione può valutarla correttamente e giudicare se è affidabile. È differente, ad esempio, se un giornalista scandalistico esprime sui media la propria opinione sulla lotta al terrorismo o se a farlo è invece un esperto comprovato. Il SIC non è affatto interessato né alla persona del giornalista né a quella dell'esperto, ma soltanto all'informazione. Per valutarla è però importante sapere da chi proviene. Da queste fonti accessibili al pubblico provengono molte informazioni di base importanti per l'attività informativa.

La situazione nella gestione delle fonti umane è analoga: la fonte stessa non è l'obiettivo, ma soltanto il mezzo dell'attività informativa del SIC. Tuttavia, quest'ultimo deve conoscere l'identità della fonte e, in tal senso, trattare dati su di essa, anche nei casi piuttosto rari in cui l'attività della fonte è legata alla sua attività politica o all'esercizio della sua libertà di opinione, di riunione o di associazione.

Lettera e

Il SIC ha il compito di informare costantemente servizi di Confederazione e Cantoni in merito a eventuali minacce e, se necessario, di allertarli (cfr. art. 6 cpv. 3 LAIn). Esso ha anche il compito di informare servizi della Confederazione e dei Cantoni su fatti e riscontri che possono incidere sui compiti legali di tali servizi in materia di salvaguardia della sicurezza interna o esterna (cfr. art. 6 cpv. 3 LAIn). Il SIC lo fa nell'ambito della cosiddetta rete informativa integrata, nella quale autorità di Confederazione e Cantoni che si occupano di questioni concernenti la sicurezza rendono reciprocamente accessibili informazioni rilevanti per la situazione in materia di salvaguardia della sicurezza interna o esterna. Coinvolgendo tutti i partner, il SIC allestisce un quadro globale della situazione e lo attualizza costantemente (cfr. rapporto del Consiglio federale sulla politica di sicurezza della Svizzera, FF 2016, pag. 7093, nota a piè di pagina 80, nonché messaggio concernente la LAIn, commento all'art. 6 LAIn, FF 2014, pag. 1922 seg.).

Nel suo rapporto annuale 2019 la DelCG è giunta alla conclusione che tali valutazioni dei rischi da parte dei servizi informazioni per pianificare misure in materia di polizia di sicurezza si basano, tra l'altro, su dati che rientrano nelle limitazioni dell'articolo 5 capoverso 5. Essa ha ritenuto che ciò è ammissibile se a tale scopo si trattano dati per un periodo inferiore a un anno. Tale precisazione viene attuata con la nuova lettera e. Essa si applica ai dati trattati dal SIC per gestire la rete informativa integrata secondo l'articolo 54 capoverso 1 e che gli sono necessari per allestire la presentazione elettronica della situazione. Così, ad esempio, se si esorta a perturbare l'assemblea annuale di un partito occorre citarlo affinché le autorità competenti possano proteggere l'evento. Le misure di polizia di sicurezza non vengono adottate dal SIC stesso, bensì dalle autorità competenti della Confederazione e dei Cantoni. Peraltro, si tratta anche di dati su persone che sono all'origine dell'importanza dell'evento a livello di politica di sicurezza, pur se la minaccia non è rivolta direttamente contro di loro (ad es. appello a protestare violentemente contro un discorso pubblico di un politico o la visita di un capo di Stato estero).

Capoverso 7

I termini «dati registrati con riferimento alle persone» e «registrazione di dati» vengono sostituiti da «dati personali». Poiché nel capoverso 6 sono ora disciplinati anche il nesso con i compiti e le minacce, il tenore della disposizione è riformulato. Non vi sono però modifiche a livello materiale.

Capoverso 8

In passato il termine «esponenti» ha dato luogo a varie discussioni, non essendo definito da nessuna parte. Qui si chiarisce che si tratta di persone che partecipano a un'organizzazione o a un gruppo di questo tipo, mettono a sua disposizione risorse umane o materiale, organizzano azioni propagandistiche a sostegno dei suoi obiettivi, reclutano adepti o promuovono in altro modo le sue attività secondo l'articolo 6 capoverso 1 lettera a. Il contenuto normativo non ne viene però modificato.

Articolo 6

Capoverso 1 lettera b

I termini «attacco a un'infrastruttura critica» o «attacchi a infrastrutture critiche» utilizzati sinora nella LAIn si sono rivelati troppo limitati per considerare tutte le circostanze nel ciberspazio importanti ai fini della politica di sicurezza. Inoltre, da alcuni anni i ciberattacchi hanno spesso una rilevanza in tal senso. Essi non sono perpetrati soltanto da singoli pirati informatici (*hacker*) o da gruppi criminali, ma sempre più spesso da attori statali (o comunque sostenuti da Stati), Forze armate e servizi informazioni. L'individuazione tempestiva e la prevenzione informative devono poter tener conto di questo nuovo aspetto della minaccia per la sicurezza interna ed esterna del nostro Paese. Con l'esplorazione informativa il SIC consente di stimare correttamente, sotto il profilo della politica di sicurezza, tali ciberattacchi e pone le basi per valutare l'opportunità di adottare contromisure nell'ambito della politica (estera). Già oggi spetta al SIC illustrare la situazione generale delle ciberminacce all'attenzione del Comitato ristretto Ciber (art. 8 cpv. 6 dell'ordinanza sui ciber-rischi del 27 maggio 2020[7]), senza che il SIC stesso possa limitarsi ai ciberaspettidei suoi settori di compiti classici. I ciberattacchi contro organizzazioni o ONG internazionali con sede in Svizzera e l'uso improprio di infrastrutture TIC nel nostro Paese per ciberattacchi possono essere di notevole importanza anche in materia di politica di sicurezza in particolare quando provengono direttamente o indirettamente da organi servizi statali esteri. Il SIC deve essere in grado di identificare, impedire e analizzare sotto il profilo informativo anche tali ciberincidenti.

7 RS **120.73**

Ciò giustifica l'estensione del mandato del SIC sull'intero ciberspazio. È importante, tuttavia, che rimanga centrale il criterio dell'importanza nell'ottica della politica di sicurezza. In questo modo si evita che il SIC diventi l'autorità responsabile della cibersicurezza per chiunque. La nozione «fatti rilevanti sotto il profilo della politica di sicurezza» si riferisce pertanto a eventi e sviluppi verificatisi nel ciberspazio atti a minacciare l'autodeterminazione informativa della Svizzera e il nostro Paese in quanto piazza economica e sede di istituti di ricerca e di organizzazioni internazionali, ad arrecare alla Svizzera gravi danni dal punto di vista della politica di sicurezza o a compromettere la capacità di azione delle sue autorità e delle sue infrastrutture critiche. In questo caso il SIC fornisce principalmente prestazioni per proteggere il nostro Paese dai ciber-rischi, come sancito nelle pertinenti strategie della Confederazione.

Capoverso 2bis

La rete informativa integrata è una forma organizzativa particolare per la condivisione di informazioni che incidono sulla situazione in materia di sicurezza, fornite al SIC da vari partner che fanno parte dell'Analisi integrata della situazione Svizzera o da servizi partner esteri. Possono essere, ad esempio, indicazioni in merito a spostamenti di persone potenzialmente violente, a incitazioni alla violenza o a dati concernenti minacce. La presentazione elettronica della situazione (cfr. al riguardo l'art. 54 cpv. 1 e il relativo commento) deve contenere tutte le informazioni di cui necessitano le competenti autorità svizzere per adottare misure di sicurezza. Vi rientrano anche dati che il SIC non tratterebbe nell'adempimento dei suoi compiti di cui al capoverso 1. Tuttavia, il trattamento nella presentazione elettronica della situazione si limita a tale strumento e allo scopo qui menzionato (cfr. al riguardo l'art. 5 cpv. 6 lettera e e il relativo commento).

Capoverso 5

Al fine di garantire il servizio di preallerta informativa per la protezione di infrastrutture critiche, il SIC deve poter stabilire e mantenere contatti con i loro gestori. La tenuta e l'aggiornamento dell'inventario degli oggetti delle infrastrutture è di competenza dell'UFPP. Per questo motivo è necessaria un'intesa stretta e regolare tra quest'ultimo e il SIC per avviare e impostare i contatti con suddetti gestori, intesa che sarà disciplinata nel dettaglio nell'ordinanza del 16 agosto 2017[8] sulle attività informative (OAIn). Con l'integrazione del presente capoverso si risponde a un'esigenza dei gestori. Ciò è parimenti conforme alla Strategia nazionale del Consiglio federale dell'8 dicembre 2017[9] per la protezione delle infrastrutture critiche 2018−2022.

Articolo 7

Capoverso 1 lettere e e f ed 1bis

Un sospetto iniziale del SIC in merito alla presenza di una minaccia acuta per la sicurezza o di violazioni delle prescrizioni di servizio può sorgere in vari modi e giungere su svariati canali. Ad esempio, un collaboratore del SIC, ma anche un servizio partner, può presentare una comunicazione di sicurezza che dà luogo a un accertamento dei fatti. È altresì possibile che un conflitto tra lavoratori comporti rischi per la sicurezza che vengono segnalati. Possono dare adito a un sospetto iniziale determinati indizi, quali l'introduzione di telefoni cellulari privati o di altri apparecchi di registrazione in aree sensibili del luogo di lavoro o contatti problematici in ambito privato o di servizio.

Ad esempio, può esserci un sospetto che alcuni collaboratori del SIC operino pervun servizio informazioni di un altro Stato o siano da esso reclutati. In un tal caso, il SIC deve essere in grado di verificare tale sospetto iniziale senza informare immediatamente i collaboratori interessati degli accertamenti necessari. Altrimenti vi sarebbe il rischio che vengano eliminati indizi o modificati comportamenti. In ogni caso, un'analisi riferita a persone è possibile soltanto se è autorizzata dal detentore dei dati interessato a livello di direzione del SIC.

La valutazione riferita a persone di accessi a dati del SIC presuppone l'approvazione scritta di un membro della direzione nonché del detentore dei dati in questione e in parte può essere realizzata soltanto con la partecipazione di settori tecnici del SIC. Così è garantito in ogni caso almeno il principio del doppio controllo. A seconda della gravità del sospetto, diventa necessaria la designazione della Sicurezza SIC da parte del direttore del SIC, ad esempio per l'avvio e l'esecuzione di un procedimento disciplinare. Se il SIC constata un presunto comportamento punibile, sporge denuncia alle competenti autorità preposte al perseguimento penale.

Anche per collaboratori già assunti che dispongono di un controllo di sicurezza relativo alle persone valido (CSP) secondo la legge del 18 dicembre 2020 sulla sicurezza delle informazioni[10] (LSIn), il SIC può effettuare accertamenti qualora si verifichi un evento che solleva questioni legate alla sicurezza. A seconda dell'esito, successivamente predispone una ripetizione del CSP. Diversamente dalle misure secondo la lettera e, gli accertamenti secondo la lettera f necessitano del consenso della persona interessata. Ciò permette di evitare che i collaboratori del SIC debbano aspettarsi di essere sottoposti a tali controlli relativi alla loro persona in qualsiasi momento.

Capoverso 1 lettere g e h

Il SIC deve accertarsi che persone che rientrano nella rosa più ristretta di selezione per un impiego presso il SIC, nonché persone e imprese che si candidano per mandati del SIC o li eseguono, non rappresentino alcun rischio per la sicurezza dei suoi collaboratori, delle sue installazioni e dei dati che esso tratta. A tal fine, i collaboratori ai quali sono affidate le misure di protezione e di sicurezza devono avere la possibilità di eseguire accertamenti su tali persone e imprese. Analogamente a quanto avviene con il CSP, gli accertamenti si eseguono con il consenso della persona o dell'impresa interessata. A seconda della data di entrata in vigore della LSIn (presumibilmente nel 2023), sarà necessario un coordinamento con la revisione della LAIn.

Gli accertamenti consistono nella consultazione dei dati interni ed esterni di cui dispone il SIC, nella richiesta di informazioni orali e scritte, in particolare anche presso le persone e le imprese interessate, e nella consultazione di fonti di informazione accessibili al pubblico. Si tratta di dati esistenti. Gli accertamenti di cui al presente articolo non danno adito a competenze per acquisire nuovi dati.

8 RS **121.1**
9 FF **2018** 455
10 RS… (FF **2020** 8755)

Tali accertamenti eseguiti tempestivamente non sostituiscono i controlli di sicurezza relativi alle persone e la procedura di sicurezza relativa alle aziende secondo la LSIn. Non sempre, però, possono avere luogo prima dell'assunzione. Il SIC li avvia secondo l'articolo 33 LSIn prima che la persona inizi la sua funzione. Per ragioni organizzative, tuttavia, in rari casi il servizio specializzato CSP riesce a concluderli prima che la persona assuma la funzione. Già prima del risultato del CSP le persone assunte hanno accesso ai locali del SIC e a documenti riservati. Un impiego pratico e razionale del lavoro è possibile soltanto se le persone hanno accesso in misura sufficiente ai dati informativi generali del SIC. Quest'ultimo ottiene dalla persona da assumere il consenso scritto per il controllo e ne richiama l'attenzione sugli obblighi in materia di segreto d'ufficio e di protezione dei dati.

Se il SIC vuole assumere una persona in qualità di fonte umana, effettua in precedenza determinate verifiche per garantire l'affidabilità della potenziale fonte. Le persone interessate non ne sono informate.

Capoverso 2

Dato che nella LAIn non vi sono più normative riguardanti singoli sistemi di informazione, il termine «sistemi di informazione» è sostituito da «dati». Ciò non comporta modifiche materiali.

Capoverso 3

Per proteggere i propri collaboratori dai servizi informazioni esteri, il SIC tiene un elenco di Paesi nei quali viaggiare comporta rischi elevati. Taluni di essi cercano di sorvegliare i collaboratori di servizi informazioni esteri quando vi si recano. Ciò può iniziare alla frontiera con controlli più approfonditi. Questi Paesi cercano di individuare con chi hanno contatti i collaboratori dei servizi informazioni. È altresì nota la sorveglianza del telefono cellulare, che trasmette lo scambio di dati nonché i movimenti nel Paese di destinazione o si introduce a tal punto nell'apparecchio che le attività saranno monitorate anche al ritorno in Svizzera. Per tali sorveglianze non si distingue se il viaggio ha finalità private o di servizio.

Se nel tempo libero i collaboratori del SIC desiderano viaggiare in detti Paesi, devono ora richiedere un'autorizzazione al servizio del SIC competente per le misure di protezione e di sicurezza. Nel gruppo internazionale informale dei servizi informazioni occidentali si sta discutendo se tali misure debbano essere la norma per continuare a cooperare a livello internazionale. L'obbligo di autorizzazione per viaggi privati costituisce una certa ingerenza nei diritti fondamentali dei collaboratori e richiede pertanto una base legale.

Articolo 8 capoverso 1

Ai fini di una terminologia uniforme, il termine «pericolo» è sostituito da «minaccia».

Articolo 9 capoverso 3

Le autorità d'esecuzione cantonali hanno l'obbligo di verificare e accertare tutti gli indizi di attività di cui all'articolo 6 capoverso 1 lettera a. È possibile che dagli accertamenti risulti che non si tratti di un'attività coperta dal settore di compiti della LAIn, così che non è dato il nesso con i compiti (ad es. un insegnante preoccupato si rivolge alle autorità d'esecuzione cantonali perché uno dei suoi alunni, di fede islamica, si comporta in modo singolare e l'insegnante teme una radicalizzazione; gli accertamenti delle autorità d'esecuzione cantonali non sono tuttavia in grado di confermare tale sospetto). In tal caso, le autorità d'esecuzione cantonali sono autorizzate a conservare i dati trattati per cinque anni ai fini della verifica (cfr. art. 46 cpv. 4), ma non presentano alcun rapporto al SIC. Se tuttavia si conferma una minaccia per la sicurezza interna o esterna ai sensi della LAIn, presentano immediatamente rapporto al SIC. Poiché l'attuale articolo 85 capoverso 2 ha lo stesso contenuto normativo, può essere abrogato (cfr. al riguardo il commento a questo articolo).

Capoverso 4

Si chiarisce ora che il SIC è il titolare del trattamento dei dati delle autorità d'esecuzione cantonali ai sensi dell'articolo 5 lettera j LPD*riv*, sempreché il trattamento dei dati si basi sulla LAIn. In tale contesto, è irrilevante se le autorità d'esecuzione cantonali si sono attivate senza essere state sollecitate o sulla base di un mandato specifico del SIC. Ciò non genera però nuovi rischi per il SIC, che si assume già oggi tale responsabilità e, nell'ambito dell'autocontrollo (cfr. art. 75 LAIn), riduce al minimo i rischi che ne risultano. Le richieste di informazioni che le autorità d'esecuzione cantonali ricevono vengono trattate fondandosi sull'articolo 63 e seguenti.

Articolo 14 capoverso 3

Secondo l'attuale diritto, il SIC può osservare fatti e installazioni in luoghi pubblici e liberamente accessibili ed effettuarvi registrazioni su supporto audiovisivo. Ciò comprende anche l'osservazione concomitante, ossia seguire e osservare, di norma, una persona o un veicolo per un certo periodo da parte di una squadra di osservazione.

I collaboratori incaricati di tali osservazioni sono vincolati all'ordinamento giuridico in vigore. A volte è quindi tanto più facile per una persona scelta come obiettivo sottrarsi a un'osservazione e quanto più difficile per l'osservatore non perdere inavvertitamente il contatto con l'oggetto dell'osservazione. Così, ad esempio, ignorare un semaforo rosso, superare la velocità massima consentita, ma anche svoltare nel fitto traffico urbano, possono essere sufficienti per far perdere il contatto alla squadra di osservazione. Le leggi cantonali in materia di polizia (per es. FR, GE, GR, NE, SZ, TG, TI, ZH) sono pertanto sempre più integrate da disposizioni che consentono l'uso di apparecchi di localizzazione (trasmettitori GPS) durante tali osservazioni, al fine di individuare rapidamente i soggetti o gli oggetti scelti come obiettivo qualora si perda il contatto visivo.

Nell'aprile del 2020, su denuncia di varie organizzazioni, il Tribunale federale (TF) ha esaminato una nuova base legale nella legge in materia di polizia del Cantone di Berna relativa all'utilizzo di apparecchi di localizzazione[11]. Il TF ha ritenuto la sorveglianza «(in tempo reale) mediante un apparecchio di localizzazione GPS montato su un veicolo» un'«ingerenza non lieve nella sfera privata» della

[11] Decisione 1C 181/2019; DTF 147 I 103

persona interessata e ha abrogato la relativa disposizione dell'articolo 118 capoverso 2 della legge bernese in materia di polizia. Nella motivazione della sentenza, il TF ha sottolineato, tra l'altro, che la disposizione bernese non conteneva alcuna restrizione ai casi concreti o urgenti di sospetto di reato e nessuna limitazione temporale. Benché la normativa bernese figurasse sotto il titolo «Observation», era formulata in modo talmente esplicito («Può utilizzare apparecchi di sorveglianza per verificare l'ubicazione di persone o cose») che non era chiaro se si trattasse di una forma di osservazione autonoma nello spazio pubblico o di una misura di supporto all'osservazione concomitanteda parte di un'unità di osservazione. Il TF federale l'ha quindi giudicata una misura a sé stante e l'ha confrontata con le pertinenti disposizioni del Codice di procedura penale[12] (CPP , art. 280 segg.) e della LAIn (art. 26 cpv. 1. lett. b.), giungendo alla conclusione che un tale impiego non è ammesso senza presupposti restrittivi e senza l'autorizzazione del giudice e, in determinati casi, senza avviso a posteriori.

Il Consiglio federale ritiene che la sentenza lasci quindi aperta la possibilità di disciplinare l'impiego di apparecchi di localizzazione quale misura di supporto a osservazioni lecite in condizioni restrittive, se in tal modo non ne risulta un'ingerenza ben maggiore nella sfera privata che non mediante l'osservazione stessa.

L'impiego dell'apparecchio di localizzazione qui proposto si limita perciò a trasmettere le coordinate attuali dell'oggetto dell'osservazione durante l'osservazione in corso e con l'unico scopo di garantirne il mantenimento. Se il contatto con l'oggetto osservato è stato perso di continuo, si deve interrompere la trasmissione dei dati di localizzazione. Tale durata deve essere breve, cioè adattata alla situazione, ma rimanere di sicuro al di sotto dell'ora. L'impiego di un apparecchio di localizzazione durante l'osservazione è così unicamente un ausilio. I dati non possono essere memorizzati per una successiva analisi o per altri scopi. Se la memorizzazione dei dati è irrinunciabile per ragioni tecniche, per far sì che l'apparecchio di localizzazione funzioni, devono essere immediatamente distrutti al termine dell'osservazione. Se l'oggetto dell'osservazione si reca in un luogo non pubblico e di pubblico accesso, occorre interrompere la trasmissione di dati dell'apparecchio di localizzazione. Lo stesso vale se la squadra di osservazione termina l'osservazione. Se desidera continuarla in un secondo momento, deve trovare l'oggetto di osservazione con i mezzi abituali. La trasmissione dei dati di localizzazione può essere riattivata soltanto quando l'oggetto è nuovamente visibile alla squadra. Tuttavia, norme talmente dettagliate vanno disciplinate nelle relative ordinanze, che saranno in seguito oggetto di revisione.

L'impiego di un apparecchio di localizzazione previsto nel presente articolo deve pertanto essere chiaramente distinto da quello di cui all'articolo 280 lettera c CPP e all'articolo 26 capoverso 1 lettera b LAIn. Questi due articoli si prefiggono in primo luogo di determinare in modo permanente la posizione e di rilevare i movimenti sull'arco di un periodo definito. Sono vincolati a severi presupposti, a un impiego duraturo e rappresentano l'ingerenza non lieve nella vita privata constatata dal Tribunale federale.

L'obiettivo dell'impiego di un apparecchio di localizzazione, disciplinato nel presente articolo, è invece semplicemente di facilitare e garantire un'osservazione. Così si possono ad esempio evitare manovre di sorpasso pericolose nel traffico stradale fitto, in quanto la squadra di osservazione è in grado di ritrovare l'oggetto di osservazione grazie all'apparecchio di localizzazione se esso scompare dal campo visivo per un breve periodo. È inoltre più facile per gli osservatori rimanere anonimi se riescono a mantenere distanze variabili rispetto alla persona scelta come obiettivo. L'ingerenza nella vita privata non è quindi più grave che nel caso dell'osservazione stessa, che non solo determina la posizione dell'oggetto scelto come obiettivo, ma anche il suo comportamento, gli eventuali contatti ecc. Il supporto all'osservazione concomitante mediante l'impiego di apparecchi di localizzazione senza autorizzazione del giudice appare quindi proporzionato alla luce della giurisprudenza del TF. In ogni caso, il SIC rimane vincolato ai principi dell'acquisizione dei dati, che prescrive la proporzionalità nella scelta della misura di acquisizione (art. 5 cpv. 3).

L'impiego di un apparecchio di localizzazione secondo il presente articolo non sostituirà la sorveglianza continua con apparecchi di localizzazione di cui all'articolo 26 capoverso 1 lettera b LAIn in caso di gravi minacce per la sicurezza della Svizzera. Occorre inoltre sottolineare che impiegare un apparecchio di localizzazione basandosi sul presente articolo necessita sempre di un'osservazione continua da parte di collaboratori. Al contrario, un impiego di un apparecchio di cui all'articolo 26 capoverso 1 lettera b LAIn ha luogo senza osservazione e i dati acquisiti vengono rilevati e valutati di continuo o a posteriori.

Articolo 18

Se nell'acquisizione di informazioni il SIC collabora con servizi svizzeri, può essere necessario proteggere anche i loro collaboratori esattamente come quelli del SIC o delle autorità d'esecuzione cantonali. In primo piano vi sono i servizi del DDPS (*Computer Network Operations* (CNO) del Centro per le operazioni elettroniche della Base d'aiuto alla condotta (BAC) dell'esercito, in futuro probabilmente Comando Ciber) incaricati dal SIC delle acquisizioni nel ciberspazio. L'articolo 18 capoverso 1 è pertanto completato da una lettera b^{bis}.

La LAIn utilizza il termine «autorità d'esecuzione cantonali», il che è reso uniforme nel capoverso 2 lettera a.

Articolo 19

Capoverso 2 lettera f

In linea con la nuova formulazione nell'articolo 6 capoverso 1 lettera b, in caso di minacce concrete anche il catalogo delle possibili fonti di minaccia in relazione con il diritto d'accesso è integrato dalle attività nel ciberspazio significative per la politica di sicurezza.

Articolo 20

Capoverso 1 lettera b

12 RS **312.0**

La presente modifica si rende necessaria in ragione della nuova denominazione a seguito della riorganizzazione degli organi delle guardie di confine e delle dogane e non contiene alcuna modifica di ordine materiale. Poiché attualmente anche la nuova legge sui compiti d'esecuzione dell'Ufficio federale della dogana e della sicurezza dei confini[13] (UDSC) si trova allo stadio legislativo, la modifica qui proposta decadrà a seconda della data di entrata in vigore di detta legge.

Capoverso 1 lettera i

Le autorità competenti per l'esercizio di sistemi informatici o che vi coadiuvano devono fornire al SIC informazioni riguardo a ciberattacchi rilevanti sul piano della politica di sicurezza affinché esso possa procedere a una presentazione della situazione completa nel ciberspazio e, se del caso, adottare misure per individuare e sventare ciberattacchi. La presente disposizione non sostituisce in alcun caso le prescrizioni legali quanto alla protezione del segreto delle telecomunicazioni, che devono essere sempre rispettate in caso di misure di sorveglianza specifiche.

Un'analoga proposta di regolamento si trova anche nel disegno della legge sulla sicurezza delle informazioni, che era in consultazione dal 12 gennaio fino al 14 aprile 2022[14]. Se l'articolo 73c capoverso 1 ivi previsto dovesse entrare in vigore prima, l'aggiunta "o che sostengono la protezione di sistemi informatici" riguardante il centro nazionale per la cibersicurezza diventerebbe superflua.

Capoverso 1 lettera j

In linea con le direttive tecniche, qui si inserisce unicamente l'abbreviazione della legge del 10 ottobre 1997 sul riciclaggio di denaro[15] (LRD).

Articolo 25

Capoverso 1 lettera a

L'obbligo di informazione dei privati è esteso ai gestori di aziende alberghiere che operano a titolo professionale. Come le imprese di trasporto, finora soggette a tale obbligo, essi dispongono spesso di informazioni che sono necessarie per individuare tempestivamente e sventare minacce per la sicurezza interna o esterna. Il SIC potrebbe così determinare i luoghi di permanenza temporanea di persone oggetto di osservazione e, a seconda della situazione, anche gli interlocutori di una di esse se, ad esempio, la persona in questione paga varie camere d'albergo o se la sua camera è pagata da terzi. Si potrebbe anche individuare quale organizzazione affitta locali per tenervi riunioni. Le normative di base in materia di memorizzazione dei dati o di obblighi di comunicazione delle aziende alberghiere continuano a essere determinate dal diritto cantonale. La LAIn non introduce nuovi obblighi né in materia di raccolta dei dati, né di conservazione dei dati, ma soltanto riguardo all'accesso ai dati esistenti su richiesta del SIC o dell'autorità d'esecuzione cantonale. Come avveniva finora, le informazioni vengono richieste soltanto in singoli casi.

Il termine «azienda alberghiera» comprende tutti i gestori che (perlopiù dietro retribuzione) mettono a disposizione di persone una possibilità di pernottamento. Vi rientrano anche i dati relativi allo scambio di appartamenti o case organizzato in modo professionale.

Capoverso 3

Come le autorità di cui agli articoli 19 e 20, ora anche i privati sono tenuti a mantenere segreta nei confronti di terzi un'eventuale richiesta di informazioni del SIC. Ciò è conforme al principio dell'irriconoscibilitàdell'acquisizione di informazioni di cui all'articolo 5 capoverso 4.

Sezione 4: Misure di acquisizione soggette ad autorizzazione

Le attuali disposizioni riguardanti le misure di acquisizione soggette ad autorizzazione vanno adeguate alla luce delle prime esperienze maturate con la loro applicazione e della necessità di intervenire riconosciuta in occasione delle varie iniziative parlamentari[16]. Da un lato, una nuova misura di acquisizione soggetta ad autorizzazione è intesa a colmare una lacuna nell'acquisizione dei dati. Attualmente il SIC non ha alcuna possibilità di ottenere informazioni da intermediari finanziari in merito al finanziamento di persone o gruppi rilevanti ai fini della sicurezza. In quanto consente di controllare i rapporti finanziari tra determinate persone espletati attraverso banche e istituzioni analoghe, questa nuova misura di acquisizione soggetta ad autorizzazione colma una lacuna nell'acquisizione dei dati (v. commento all'art. 26 cpv. 1 lett. f e g).

Inoltre, il campo di applicazione delle misure di acquisizione soggette ad autorizzazione deve essere esteso all'estremismo violento (v. commento all'art. 27 cpv. 1 lett. a). Come avveniva finora, anche nell'impiego della nuova informazione finanziaria o nell'impiego per svolgere accertamenti sull'estremismo violento devono essere rispettati i rigidi presupposti di cui all'articolo 27.

L'attuale articolo 29 viene ora suddiviso in diversi articoli. Questa nuova struttura del disciplinamento della procedura di autorizzazione porta a una migliore separazione dei contenuti.

Articolo 26

Capoverso 1

Lettera b

13 FF **2020** 6514
14 Consultabile su: www.fedlex.admin.ch >Procedure di consultazione >Concluse >2022 >DFF >Obbligo di notifica di ciberattacchi per i gestori di infrastrutture critiche
15 RS **955.0**
16 ad es.: Po 17.3831 e Mo 20.4568.

Qui va inserita l'indicazione che gli apparecchi di localizzazione possono essere utilizzati senza autorizzazione nell'ambito di misure di osservazione in corso («osservazione»). Si può rinviare al precedente commento all'articolo 14 capoverso 3.

Lettere f e g

Queste nuove misure di acquisizione soggette ad autorizzazione sono conformi agli articoli 284 e 285 CPP, che controllano i rapporti tra una persona oggetto di osservazione del SIC e istituzioni sottoposte alla legge sul riciclaggio di denaro. Con il rinvio all'articolo 2 LRD, la cerchia delle persone e delle istituzioni interessate, che ai sensi della nuova misura di acquisizione soggetta ad autorizzazione è ora tenuta a informare, coincide con quella del campo di applicazione della LRD.

Specialmente per il finanziamento del terrorismo si utilizzeranno non soltanto le grandi banche istituzionalizzate, ma anche servizi di piccole imprese che offrono prestazioni di servizi nel trasferimento di denaro internazionale, o anche di persone che scambiano denaro contante. Per tale motivo la LAIn riprende dalla LRD la definizione della cerchia delle persone potenzialmente interessate, presso la quale è possibile ottenere informazioni su transazioni e relazioni d'affari. La trasparenza su tali flussi finanziari, resa possibile grazie alla sorveglianza delle relazioni, serve al SIC per adempiere i compiti di cui all'articolo 6 LAIn.

Interessanti per il SIC sono i retroscena del finanziamento di organizzazioni e gruppi che sono già finiti nel suo mirino a causa di altre informazioni. Una sorveglianza mirata consente di valutare meglio la minaccia per la sicurezza interna o esterna della Svizzera da parte di un'organizzazione o di un gruppo. Si pensi, ad esempio, a imprese commerciali, a organizzazioni che perseguono scopi meramente ideali o a enti religiosi in merito ai quali esistono fondati indizi di partecipazione ad attività terroristiche, informative o di estremismo violento (v. commento all'art. 27 cpv. 1. lett. a), soprattutto al loro finanziamento. Informazioni sull'origine del finanziamento possono fornire al SIC ulteriori elementi conclusivi per poter riconoscere tempestivamente e sventare una minaccia per la sicurezza interna ed esterna della Svizzera.

Oggi il SIC ha soltanto possibilità assai limitate di ottenere informazioni riguardo al finanziamento di un ente. A determinate condizioni, ad esempio, nel singolo caso può ottenere informazioni dall'Ufficio di comunicazione in materia di riciclaggio di denaro (MROS) (art. 29 cpv. 2^{bis}–2^{ter} in combinato disposto con l'art. 30 seg. LRD nonché art. 20 cpv. 1. lett. j LAIn).

In quanto «Financial Intelligence Unit» (FIU) svizzera il MROS è il Servizio centrale nazionale che secondo la LRD riceve comunicazioni di sospetto concernenti riciclaggio di denaro, finanziamento del terrorismo, fondi da atti preparatori del riciclaggio di denaro od organizzazioni criminali degli istituti sottoposti alla LRD, le analizza (art. 23 cpv. 2 LRD), scambia informazioni a livello nazionale e internazionale (art. 29 e 30 LRD) e, nel caso di un sospetto fondato, denuncia il fatto alla competente autorità di perseguimento penale (art. 23 cpv. 4 LRD).

A prima vista, l'elenco dei compiti del MROS può indurre a concludere che l'attuale scambio di informazioni tra quest'ultimo e il SIC soddisfi già l'obiettivo della nuova normativa. Tuttavia, non è così: le comunicazioni degli intermediari finanziari al MROS presuppongono il sospetto fondato, ad esempio, del finanziamento del terrorismo (art. 9 LRD). Il semplice fatto che un'organizzazione che persegue scopi meramente ideali inciti i propri membri alla violenza non autorizza però ancora gli intermediari finanziari a rivolgersi al MROS. Inoltre, un intermediario dà comunicazione a quest'ultimo soltanto se riconosce le finalità del finanziamento. Infine, anche nel caso gli vengano rese note informazioni, il MROS deve salvaguardare il principio di specificità che si applica alle FIU a livello internazionale e che va rispettato rigorosamente. Secondo questo importante principio di cooperazione internazionale, le informazioni scambiate tra le FIU possono essere utilizzate soltanto per gli scopi per i quali sono state richieste e fornite (n. 3 della nota interpretativa alla raccomandazione 40 *«Groupe d'action financière»*; principio di specialità). Quale autorità che riceve le informazioni, il MROS deve rispettare le condizioni dell'autorità dalla quale provengono le informazioni stesse. Ciò vale anche qualora le informazioni ricevute da un ufficio estero siano trasmesse, con il suo [esplicito] consenso, a un'autorità nazionale (cfr. al riguardo l'art. 29 cpv. 2^{ter} LRD).

Il compito del SIC è diverso da quello del MROS: opera nell'ambito preventivo dell'acquisizione di informazioni e gli compete direttamente l'acquisizione di informazioni allo scopo di salvaguardare la sicurezza interna ed esterna. Se ha indizi concreti che, ad esempio, un ente religioso recluta persone per minacciare gravemente la sicurezza interna ed esterna della Svizzera, deve avere la possibilità di chiedere informazioni sul finanziamento e quindi anche sulla rete di contatti di detto ente al fine di completare la sua valutazione della minaccia. Nel singolo caso, queste informazioni possono fornire una base importante per adottare ulteriori misure, come ad esempio il divieto di determinate attività di cui all'articolo 73 LAIn. La nuova normativa mira pertanto a colmare un'importante lacuna negli strumenti utilizzati dal SIC per l'acquisizione di dati.

La misura va formata quale misura di acquisizione soggetta ad autorizzazione secondo la LAIn, in quanto costituisce un'ingerenza soprattutto nella libertà economica e nella libertà personale. Le misure di acquisizione soggette ad autorizzazione sono vincolate a requisiti molto rigorosi e necessitano sia di un'autorizzazione da parte del TAF, sia di un nullaosta da parte del capo del DDPS.

Questa nuova misura dell'acquisizione di dati è quindi complementare allo scambio di informazioni già esistente tra il SIC e il MROS (cfr. art. 29 cpv. 2^{bis}–2^{ter} in combinato disposto con l'art. 30 segg. LRD nonché art. 20 cpv. 1. lett. j LAIn). È importante che questa nuova misura non violi il divieto d'informazione di cui all'articolo 10*a* LRD. Esso attua il divieto di comunicazione di dati alla persona interessata secondo gli standard del *«Groupe d'action financière»*. Il cliente dell'istituto finanziario non deve accorgersi che nei propri confronti c'è una comunicazione di sospetto. Ciò potrebbe pregiudicare il perseguimento penale e in particolare l'assunzione delle prove.

Il SIC necessita di questa misura supplementare di acquisizione soggetta ad autorizzazione non soltanto per adempiere i compiti nell'ambito del terrorismo. Le risultanze dei dati finanziari possono essere importanti anche per riconoscere tempestivamente e sventare minacce per la sicurezza interna ed esterna derivanti dallo spionaggio. Possono ad esempio essere assai interessanti le informazioni sul finanziamento di infrastrutture, quali alloggi, che fungono da copertura o di abbonamenti a collegamenti di telecomunicazione, che servono per tenere i contatti con le fonti. È possibile anche scoprire o confermare l'esistenza di una società fittizia se ne utilizzano i conti unicamente persone che il SIC è in grado di identificare quali agenti sotto copertura. A seconda della situazione è quindi possibile identificare persone che operano in Svizzera per un altro Stato.

Nell'ambito dell'estremismo violento (v. commento all'art. 27 cpv. 1. lett. a), le informazioni sulle transazioni finanziarie possono fornire informazioni riguardo agli immobili che sono stati acquistati da persone identificate come estremisti violenti, ai beni che tali persone acquistano, alle persone e alle organizzazioni che sostengono finanziariamente o in altro modo. Le informazioni sul finanziamento di grandi eventi di gruppi estremisti violenti possono fornire le risultanze necessarie per l'esplorazione della rete.

Articolo 27

Capoverso 1 lettera a

Ai fini di una migliore leggibilità la presente lettera viene rinumerata.

Numero 1

Dall'entrata in vigore della LAIn, le reazioni violente degli estremisti di destra e degli estremisti di sinistra si sono intensificate. Aumentano l'aggressività nei confronti delle forze di sicurezza e il potenziale di violenza generale di questi gruppi. Pur se l'attuale ricorso alla violenza degli estremisti di destra è ancora relativamente basso, essi si allenano però negli sport di combattimento e si armano sempre di più. Gli estremisti di sinistra sono fortemente interconnessi a livello internazionale ed esercitano violenza contro le autorità con sempre maggiore intensità.

L'estremismo violento è opera di organizzazioni e persone che negano i fondamenti della democrazia e dello Stato di diritto e che commettono, incoraggiano o approvano atti violenti allo scopo di conseguire i propri obiettivi (cfr. art. 19 cpv. 2. lett. e). Se nell'emanare la legge sulle attività informative sono ancora state escluse misure di acquisizione soggette ad autorizzazione per svolgere accertamenti su attività di estremismo violento, eventi verificatisi all'estero hanno dimostrato che tali attività possono anche assumere dimensioni tali da minacciare gravemente la sicurezza interna o esterna. In parte si è trattato di casi di persone già note alle autorità come estremisti violenti, che hanno fatto ricorso ad azioni ritenute di portata terroristica (ad es. attentati di Christchurch/Nuova Zelanda o Halle/Germania). Dopo le recenti evoluzioni della situazione, anche in Svizzera sono nettamente in aumento la radicalizzazione e la violenza di parti di questi gruppi di persone. Indizi di acquisti di armi, munizioni e ordigni esplosivi e della formazione per utilizzarli non sono di per sé un motivo per ritenere che una persona estremista violenta oltrepasserà la soglia del terrorismo. Se si tratti nel singolo caso di un'attività di estremismo violento o terroristica dipende dall'obiettivo perseguito dall'azione, dalla sua intensità e dalla sua gravità. Spesso tutto ciò è individuabile soltanto dopo che l'atto è stato compiuto.

Senza l'impiego di misure di acquisizione soggette ad autorizzazione è difficile individuare evoluzioni analoghe. Gli ambienti in questione utilizzano sempre più spesso metodi operativi occulti sui quali il SIC, con le misure di acquisizione delle informazioni esenti da autorizzazione ammesse attualmente, non è in grado di svolgere accertamenti adeguati, motivo per cui, anche in caso di gravi forme di attività di estremismo violento con potenziali danni anche alla vita e all'integrità della persona, deve essere consentito l'impiego di misure di acquisizione soggette ad autorizzazione. Si considerino i casi in cui vi sono riscontri in base ai quali estremisti violenti si procurano armi, si formano all'uso delle stesse e nel contempo, da un lato, si isolano maggiormente dal mondo esterno e, dall'altro, sempre più − in particolare sui social media− si occupano di attentati legati all'estremismo violento o al terrorismo e si esprimono al riguardo. In tali casi per lo più non è stata ancora oltrepassata la soglia degli atti preparatori punibili e le persone in questione non hanno legami diretti con gruppi terroristici noti. Le informazioni disponibili possono tuttavia indicare una grave minaccia per la sicurezza, che dovrebbe essere chiarita in modo più approfondito (v. il rapporto del 13 gennaio 2021[17] del Consiglio federale in adempimento del postulato 17.3831 Glanzmann-Hunkeler: Strumenti incisivi contro gli estremisti violenti).

Se in Svizzera i mezzi preventivi sono lacunosi, è forte il pericolo che il nostro Paese diventi un luogo in cui trovano rifugio o si incontrano estremisti violenti stranieri (v. il parere del Consiglio federale del 13 maggio 2020[18] in merito al postulato 20.3100 Jositsch: Verifica dell'efficacia della nuova legge sulle attività informative). Perciò oggi, a livello sia cantonale che federale (cfr. ad es. il postulato 17.3831 Strumenti incisivi contro gli estremisti violenti) le misure di acquisizione soggette ad autorizzazione vengono richieste anche per individuare tempestivamente e sventare attività di estremismo violento che minacciano gravemente la sicurezza. Le esperienze maturate finora con suddette misure indicano che il loro impiego è adeguato per procedere ad accertamenti mirati e puntuali di singoli casi seri. Il SIC utilizza tali mezzi con cautela e soltanto per gravi minacce. Le misure devono inoltre essere esaminate dal TAF in base alla loro necessità e proporzionalità e approvate da quest'ultimo. Nel 2017 sono state applicate misure in quattro4 casi, nel 2018 in otto casi, nel 2019 in cinque casi e nel 2020 in quattro casi. Queste cifre indicano che il SIC si riserva di utilizzare tali mezzi in maniera moderata e solo nei casi di gravi minacce previsti dalla legge.

L'abolizione della limitazione alle lettere a−d dell'articolo 19 capoverso 2 LAIn delle misure di acquisizione soggette ad autorizzazione ne estende il campo di applicazione anche all'estremismo violento. I rigidi presupposti previsti per l'impiego di misure di acquisizione soggette ad autorizzazione di cui all'articolo 27 capoverso 1 rimangono però invariate e si applicano anche alle misure di acquisizione mirate all'estremismo violento; in particolare, la gravità della minaccia deve giustificare la misura di acquisizione.

Numero 2

L'applicazione pratica delle misure di acquisizione soggette ad autorizzazione per svolgere accertamenti su attività terroristiche ha evidenziato come il TAF non possa autorizzare misure nel settore delle telecomunicazioni, che in ragione di circostanze tecniche possono essere attuate esclusivamente in Svizzera, se per la stessa sicurezza di quest'ultima non sussiste una minaccia (incombente) concreta ai sensi dell'articolo 19 capoverso 2 LAIn. Ciò vale anche per casi in relazione con organizzazioni terroristiche bandite a

17 Consultabile su: www.parlamento.ch >17.3831> Rapporto in adempimento dell'intervento parlamentare.
18 Consultabile su: www.parlamento.ch > 20.3100.

livello sia nazionale, sia internazionale, quali Al-Qaida o lo «Stato islamico». I loro dirigenti all'estero utilizzano in parte servizi di telecomunicazione svizzeri sui quali si può fare luce soltanto mediante misure di acquisizione soggette ad autorizzazione in Svizzera. In passato lo stesso TAF ha dovuto respingere una richiesta del SIC perché la gravità della minaccia (incombente) alla sicurezza della Svizzera non era sufficientemente concreta. Il TAF ha rinviato al fatto che spetta al legislatore creare, per tali casi, una base legale per l'applicazione di misure di acquisizione soggette ad autorizzazione.

Ai sensi dell'articolo 2 lettera d LAIn, il Consiglio federale propone perciò di introdurre anche la grave minaccia a importanti interessi internazionali in materia di sicurezza quale criterio per ordinare misure di acquisizione soggette ad autorizzazione in Svizzera. Taluni accertamenti, specialmente su importanti processi di comunicazione tra persone che minacciano gravemente la sicurezza internazionale, per ragioni tecniche sono possibili soltanto in Svizzera. Se una detta persona, ad esempio un alto dirigente di un'organizzazione terroristica internazionale, utilizza un servizio di comunicazione gestito attraverso la Svizzera, oppure se attori stranieri portano gravi ciberattacchi contro altri Paesi per il tramite di infrastrutture svizzere, al SIC va data la possibilità di svolgere accertamenti anche nell'interesse della sicurezza internazionale e non soltanto nel caso di una minaccia incombente per la Svizzera. Come per la protezione di interessi svizzeri in materia di sicurezza, anche quelli internazionali vanno limitati agli ambiti tematici dell'articolo 6 capoverso 1 lettere a e b, ossia la difesa contro terrorismo, spionaggio, proliferazione, ciberattacchi ed estremismo violento. Nel caso opposto, tale capacità di cooperazione da parte della Svizzera può anche promuovere la disponibilità internazionale a cooperare a favore della sicurezza del nostro Paese.

Per l'impiego di queste nuove possibilità atte a individuare tempestivamente gravi minacce da parte dell'estremismo violento o interessi internazionali in materia di sicurezza, il Consiglio federale si dichiara favorevole a una prassi tanto restrittiva quanto lo era finora e non si aspetta un aumento sostanziale del numero di casi in cui saranno applicate tali misure. I requisiti di legge che ne disciplinano l'attuazione rimangono severi e sono soggetti a un controllo indipendente da parte del TAF. Il necessario nullaosta alle misure a livello politico consente una gestione attiva anche dal punto di vista della politica istituzionale. Nel complesso, se la situazione di minaccia rimane costante, dovrebbe trattarsi di circa 5−10 casi supplementari all'anno, per i quali in futuro si utilizzerebbero misure di acquisizione soggette ad autorizzazione per svolgere accertamenti su gravi minacce da parte dell'estremismo violento o minacce a importanti interessi internazionali in materia di sicurezza. Nella situazione attuale, i relativi compiti possono essere svolti con le risorse esistenti.

Articolo 28

L'articolo chiarisce che rientrano in questa categoria anche casi in cui una persona scelta come obiettivo, pur non avendo un proprio accesso all'infrastruttura da sorvegliare (telefono, veicolo, indirizzo postale ecc.) della terza persona, la utilizza però per trasmettere informazioni, in particolare anche a quest'ultima. Quale esempio concreto si può nominare un combattente jihadista svizzero che si trova all'estero del quale si sa che comunica periodicamente con una terza persona, ad esempio un familiare, in Svizzera. Sorvegliare il suo collegamento di telecomunicazione all'estero non è tecnicamente possibile, v mentre lo è di quello della terza persona in Svizzera. In tal modo si possono ottenere per la sicurezza della Svizzera importanti riscontri al fine di contrastare le minacce terroristiche. L'aggiunta «da o verso» è intesa a precisare che è possibile ordinare misure di acquisizione soggette ad autorizzazione nei confronti di una terza persona anche se questa è semplicemente colui che riceve informazioni della persona da sorvegliare. Anche in tali configurazioni si applicano i rigidi presupposti abituali riguardanti la gravità della minaccia e la proporzionalità della misura.

Il secondo capoverso dell'attuale articolo 28 è abrogato. Si può invece rinviare all'articolo 50 capoverso 2, che si applica anche nel caso in cui si ordini una misura di acquisizione soggetta ad autorizzazione nei confronti di una terza persona. Nella pratica si è constatato che qualcuno appartenente alla cerchia di persone soggette a segreto professionale (ad es. anche il personale ausiliario di medici) da privato può sottoscrivere numerosi abbonamenti di telefonia mobile e cederne il pieno utilizzo ad altre persone. La persona soggetta all'obbligo del segreto d'ufficio non utilizza mai tali connessioni, così che il segreto stesso di fatto non ne è interessato. Se dall'utente effettivo della connessione emergesse una corrispondente minaccia per la sicurezza della Svizzera, non è giustificato escludere la sorveglianza di tale connessione. Anche in questo caso la selezione sotto la vigilanza del TAF è la soluzione adeguata.

Articolo 29

Nel capoverso 1 la lettera c è stata integrata e inoltre si inserisce la lettera d. Il resto del capoverso 1 rimane invariato.

Capoverso 1 lettera c

Le misure di acquisizione soggette ad autorizzazione talvolta nella pratica non possono essere attuate senza ulteriori misure di accompagnamento. Se, ad esempio, un apparecchio di localizzazione deve essere montato su un veicolo e vi sono l'autorizzazione giudiziaria e il nullaosta politico per farlo, il veicolo può essere parcheggiato su suolo pubblico oppure privato liberamente accessibile, in un parcheggio sotterraneo privato con accesso limitato, in un garage singolo chiudibile o su un posteggio privato di una terza personaecc. Per il montaggio (e la successiva rimozione) dell'apparecchio di localizzazione è quindi necessario accedere ai relativi locali e luoghi, anche se la proprietà non è sempre chiaramente riconoscibile di primo acchito. Ai sensi dell'articolo 269ter capoverso 2 CPP, anche in seno al SIC occorre perciò prevedere la possibilità di conferire, assieme al permesso nel merito (ad es. montare un apparecchio di localizzazione), anche quello per attuare le necessarie misure di accompagnamento.

Le misure di accompagnamento legate all'impiego di una misura di acquisizione soggetta ad autorizzazione eventualmente necessarie dipendono dal singolo caso e non possono essere elencate in modo esaustivo nella legge. Il SIC deve pertanto descriverle in dettaglio nei documenti per la procedura di autorizzazione e quella di nullaosta. Per l'autorizzazione, nel valutare l'ammissibilità il TAF segue requisiti in materia di adeguatezza, necessità e sussidiarietà comparabili a quelli per la misura principale.

Capoverso 1 lettera d

A seguito dell'adeguamento dell'informazione riguardante le misure adottate dalle autorità di perseguimento penale o dal Servizio SCPT nell'articolo 29*a* capoverso 3 (v. sotto), ora le indicazioni su procedimenti penali diventano parte della domanda.

Articolo 29a

Capoverso 1

Il presente capoverso corrisponde all'attuale articolo 29 capoverso 2. A seguito dell'adeguamento nell'articolo 29 capoverso 1 lettera c, ai sensi dell'articolo 274 capoverso 4 CPP nel presente capoverso si sancisce esplicitamente che il TF nella sua decisione deve esprimersi in merito alle eventuali misure di accompagnamento.

Capoverso 2

Il presente capoverso corrisponde in gran parte all'attuale articolo 29 capoverso 3 prima frase. In conformità con l'attuale testo di legge il TAF nega l'autorizzazione a una domanda di misura di acquisizione soggetta ad autorizzazione qualora *tale* misura sia già stata autorizzata sulla base di un procedimento penale pendente contro la persona interessata. Non è però sufficientemente chiaro se per «*tale* misura» si intende una misura identica (ossia una sorveglianza del traffico delle telecomunicazioni) o semplicemente un'altra misura coercitiva (ad es. una sorveglianza tecnica di diritto processuale penale, mentre il SIC fa domanda di una sorveglianza delle telecomunicazioni). È perciò necessario precisare che cosa si intende per «*tale* misura».

La normativa vigente riguarda inoltre solo la data dell'autorizzazione e non prevede una regolamentazione esplicita nel caso in cui si ordini un'identica misura coercitiva di diritto processuale penale soltanto mentre sono in corso misure di acquisizione soggette ad autorizzazione. Un'attribuzione all'articolo 32 capoverso 1 lettera b (cessazione in caso vengano meno le condizioni) non è cogente, tanto più che i presupposti per ordinare una misura di acquisizione soggetta ad autorizzazione figurano all'articolo 27 capoverso 1, mentre la disposizione inerente alle identiche misure di diritto processuale penale si trova sotto il titolo «procedura di autorizzazione».

Come inteso finora, da un lato, devono essere possibili contemporaneamente varie misure delle autorità di perseguimento penale e del SIC e, dall'altro, escludersi a vicenda misure aventi il medesimo effetto. Nel tenore del testo di legge ciò si esplicita con il termine *identico*. Se quindi, ad esempio, sulla rete fissa è in corso una sorveglianza telefonica su ordine del MPC, in parallelo il SIC dovrebbe potersi introdurre in un telefono cellulare attribuibile alla persona scelta come obiettivo e svolgere accertamenti su questa comunicazione, in quanto trattasi di misure. se pur simili, non però identiche (che oltre a ciò hanno luogo per fini differenti). Non verrebbe invece autorizzata la vigilanza simultanea dello stesso numero di telefono fisso da parte di MPC e SIC, essendo le misure identiche.

Secondo il Consiglio federale, nell'ambito della procedura di autorizzazione è possibile tenere sufficientemente conto delle preoccupazioni espresse dal TAF riguardo al fatto che potrebbe venire a crearsi confusione tra la sorveglianza di diritto processuale penale e quella informativa se una misura di acquisizione soggetta ad autorizzazione deve essere esclusa soltanto in caso di misure coercitive di diritto processuale penale identiche, ma con finalità differenti e vincolate ad altre condizioni (prevenzione/repressione). Nelle sue domande il SIC deve indicare le misure coercitive di diritto processuale penale in essere e spiegare perché le misure di acquisizione soggette ad autorizzazione richieste non collidono con esse. In caso di trasmissione alle autorità di perseguimento penale di informazioni ottenute con misure di acquisizione soggette ad autorizzazione il SIC deve quindi indicare l'origine delle informazioni, così che le autorità di perseguimento penale possano fare attenzione che non vengano soppresse o eluse le garanzie di tutela di diritto processuale penale a favore dell'imputato.

Capoverso 3

Il presente capoverso corrisponde in gran parte all'attuale articolo 29 capoverso 3 seconda frase e viene allineato alla prassi attuale, ossia che prima di presentare la domanda al TAF si informa direttamente in merito a eventuali misure di autorità di perseguimento penale o dal Servizio SCPT e illustra il risultato nella domanda stessa.

Capoverso 4

Il presente capoverso corrisponde in gran parte all'attuale articolo 29 capoversi 4 e 5.

Il presente capoverso viene integrato dalla menzione delle misure di accompagnamento. La misura di acquisizione e le necessarie misure di accompagnamento sono così equiparate per l'autorizzazione.

Vi si menziona inoltre esplicitamente che il TAF può concedere l'autorizzazione sia a determinate condizioni, sia vincolandola a oneri. Ciò è in linea con l'attuale prassi giudiziaria. Viene così eliminata una differenza tra il testo francese e quelli in tedesco e in italiano.

Capoverso 5

A fini di chiarezza si precisa che il TAF può decidere soltanto in merito a misure che rientrano nel campo d'applicazione dell'ordinamento giuridico svizzero. Se una persona obiettivo di una misura in corso di esecuzione si reca all'estero, si applicano le disposizioni dell'articolo 36 e segg., in particolare dell'articolo 37, per l'intrusione nei sistemi informatici e nelle reti informatiche. Come menzionato sopra, per le misure all'estero non è possibile alcuna autorizzazione da parte del TAF. Previa consultazione del capo del DFAE e del capo del DFGP, il capo del DDPS decide in merito all'attuazione di misure all'estero (art. 37 cpv. 2).

Articolo 29b

Capoverso 1

In base al testo legislativo vigente, il termine di tre mesi per un'autorizzazione decorre dal momento in cui è stata concessa, indipendentemente dalla durata della successiva procedura di nullaosta a livello politico, o se il SIC è stato effettivamente in grado di attuare la misura di acquisizione che ha ottenuto l'autorizzazione e il nullaosta. Ciò può limitare la durata effettiva di una misura e ridurre il periodo fino alla presentazione di domande di proroga. Ora l'inizio della decorrenza massima di tre mesi del termine per una misura di acquisizione di informazioni speciale autorizzata dal TAF non deve automaticamente partire dalla data di autorizzazione del TAF, che deve invece poterlo fissare anche a una data successiva. Non si pensi soltanto al momento del nullaosta a livello politico, ma a una data

successiva per ragioni operative, come l'entrata di una determinata persona o il verificarsi di un evento come l'inizio di una manifestazione che minaccia la sicurezza. Le misure di acquisizione soggette ad autorizzazione devono poter essere gestite in modo più preciso a livello temporale, senza dover procedere a modifiche alla durata legale (tre mesi) o alla procedura conforme allo Stato di diritto.

Capoverso 2

In caso di ritardi nella procedura di autorizzazione e di nullaosta di una domanda di proroga delle misure di acquisizione soggette ad autorizzazione, di per sé presentata in tempo, vi è il rischio che il SIC debba sospendere la misura fino al nullaosta definitivo della proroga. Perciò è opportuno prevedere una nuova disposizione che consenta al termine della procedura di proroga di restare in vigore, consentendo alSIC di portare avanti la misura. In questo modo si evita che una misura di acquisizione venga interrotta a causa di un ritardo nella procedura. Ovviamente il SIC deve sospendere immediatamente una misura qualora il TAF non autorizzi la proroga. Una procedura di nullaosta non ha più luogo successivamente. La presentazione anticipata della domanda di proroga considera i cinque giorni lavorativi di cui all'articolo 29*a* capoverso 1 per la decisione del TAF e il numero medio di giorni della procedura di nullaosta, non vincolata ad alcun termine.

Capoverso 3

Come nella procedura in caso d'urgenza il SIC distrugge senza indugio i dati acquisiti se il TAF non concede l'autorizzazione o il capo del DDPS il nullaosta.

Articolo 29c

Il presente articolo corrisponde all'attuale articolo 29 capoverso 8.

Articolo 30

Capoversi 3 e 4

La mera proroga di una misura di acquisizione soggetta ad autorizzazione ha soltanto una componente temporale. La misura di acquisizione stessa rimane però identica. Viene così a cadere la decisione di principio politica sulla sua attuazione e il capo del DFAE e il capo del DFGP possono essere esonerati dalle consultazioni, che nell'attuale normativa costituiscono in parte considerevoli carichi di lavoro. Ora il capo del DDPS deve poter decidere sotto la propria responsabilità riguardo a semplici proroghe. In casi particolarmente significativi, rimane a sua discrezione la possibilità di consultare il capo del DFAE e il capo del DFGP, oppure può essere concordata tra loro.

Di norma, in caso di leggere estensioni di misure che hanno già ottenuto l'autorizzazione e il nullaosta, non si pongono più questioni di fondo. Ciò si verifica, ad esempio, quando una persona scelta come obiettivo acquista un telefono cellulare supplementare con un nuovo numero di telefono che deve essere incluso nella sorveglianza, già in essere, delle sue connessioni. Anche in tali casi si giustifica il fatto che, dopo l'autorizzazione del TAF, il capo del DDPS possa decidere direttamente in merito al nullaosta dell'estensione, mantenendo però la facoltà di consultare comunque i suoi omologhi del DFAE e del DFGP, se lo ritiene necessario visti i rischi politici connessi alla misura adottata. A loro volta, nel parere concernente l'ordine originale, qualora vi siano interessi particolari questi ultimi due possono chiedere di essere nuovamente consultati in caso di proroghe o di estensioni. Vige sempre la regola che il capo del DDPS informa il capo del DFAE e il capo del DFGP sulla decisione presa.

Articolo 33

Capoversi 1, 2bis, 3 e 4

Al fine di evitare confusioni nel calcolo del termine mensile, il termine per la comunicazione di misure di acquisizione soggette ad autorizzazione deve ora essere fissato uniformemente a 30 giorni.

Nell'applicare l'obbligo di comunicazione e le relative eccezioni, la prassi ha dimostrato che l'attuale normativa comporta in parte oneri sproporzionati rispetto alla tutela dei diritti delle persone interessate. Secondo il diritto vigente, il differimento di una comunicazione deve essere richiesto ogni tre mesi al TAF e successivamente ottenere il nullaosta del capo del DDPS dopo consultazione dei suoi omologhi del DFAE e del DFGP, poiché la procedura che si applica è uguale a quella per ordinare misure di acquisizione soggette ad autorizzazione. Per tale procedura la durata massima dell'autorizzazione è di tre mesi. I casi di differimento della comunicazione registrati sinora riguardavano principalmente persone contro le quali era pendente un procedimento penale connesso alla precedente sorveglianza informativa. Se per motivi legati alle indagini in corso la persona interessata non è ancora stata informata della procedura dalle autorità di perseguimento penale, una comunicazione della sorveglianza da parte del SIC può mettere a repentaglio il procedimento penale. Perciò ha sempre luogo un differimento della comunicazione o la sua proroga. La comunicazione avviene soltanto quando l'autorità di perseguimento penale ha informato la persona o ha sospeso il procedimento penale.

Un differimento non può pertanto più avvenire per soli tre mesi, ma deve poter durare fino a sei mesi o essere vincolato a un determinato evento (ad es. prosecuzione di un procedimento penale). Il SIC deve menzionare chiaramente nella sua domanda i motivi di un differimento e, se del caso, l'evento fino al quale si applicherà il differimento. Il TAF decide così con fondatezza quanto all'autorizzazione del differimento. Poiché il mero differimento della comunicazione non costituisce una misura definitiva, deve essere ora soggetto unicamente alla procedura di autorizzazione. È improbabile che un differimento giuridicamente doveroso non venga confermato per motivi politici. Un differimento della comunicazione in virtù delle relazioni della Svizzera con l'estero contempla invece una componente politica. Ecco perché esso dovrebbe passare anche attraverso la procedura di nullaosta.

La rinuncia definitiva alla comunicazione, invece, dovrebbe continuare a essere soggetta alla procedura di nullaosta a livello politico. Se il differimento della comunicazione è autorizzato dal TAF, può essere utile fornire informazioni ai dipartimenti coinvolti nella

procedura di nullaosta. Se necessario, ciò sarà disciplinato nel contesto dell'adeguamento delle relative ordinanze a seguito della revisione della legge.

L'obbligo di comunicazione continua ad applicarsi soltanto per le misure effettivamente attuate. Le misure che, pur avendo ottenuto l'autorizzazione e il nullaosta, non hanno potuto però essere attuate, ad esempio per motivi tecnici, non hanno interferito in alcun diritto fondamentale e perciò non sono soggette all'obbligo di comunicazione.

Articolo 37

Capoversi 3–6

L'articolo 37 non contiene attualmente alcun disciplinamento in caso d'urgenza come invece è il caso nell'articolo 31 per le misure di acquisizione soggette ad autorizzazione. L'intrusione nei sistemi informatici e nelle reti informatiche all'estero allo scopo di perturbarne, impedirne o rallentarne il funzionamento per difendersi dagli attacchi alle infrastrutture critiche è una misura, di norma, delicata e il cui effetto è immediatamente riconoscibile e deve continuare a essere adottata soltanto su decisione del Consiglio federale.

L'intrusione ai fini dell'acquisizione di informazioni avviene in maniera inosservata ein caso di urgenza deve potere avvenire immediatamente per ottenere informazioni importanti in tempo utile. Si giustifica pertanto l'aggiunta di un disciplinamento in caso d'urgenza analogo a quello per le misure di acquisizione soggette ad autorizzazione. Esso ha dimostrato la sua validità e prevede che il direttore del SIC può ordinare e far eseguire direttamente la misura e successivamente sottoporla ad autorizzazione e a nullaosta secondo la procedura ordinaria.

Se il capo del DDPS si rifiutasse, immediatamente o dopo aver consultato ilDFAE e il DFGP, di proseguire la misura, sarebbe inoltre tenuto a decidere in merito all'utilizzo dei dati eventualmente già acquisiti. È ipotizzabile che, pur se una misura non dev'essere proseguita per ragioni di ponderazione dei rischi a livello politico, il SIC possa però utilizzare informazioni già acquisite e rilevanti per la valutazione della situazione in materia di sicurezza.

Articolo 39

Capoverso 3

L'adeguamento nel capoverso 3 dovrebbe esprimere meglio il fatto che nell'esplorazione di segnali via cavo tutte le persone in Svizzera sono protette da un'esplorazione mirata con tale mezzo (cfr. art. 42 cpv. 2, che parla di persone *che si trovano in Svizzera*). Il SIC non può quindi svolgere accertamenti su persone straniere nel nostro Paese mediante l'esplorazione di segnali via cavo, il che corrisponde già all'attuale applicazione. Può per contro essere utile e necessario svolgere accertamenti su nostri concittadini all'estero mediante questo tipo di esplorazione, se è accertato che non si trovano in Svizzera. Ciò è conforme alla prassi corrente nell'esplorazione radio, ad esempio nel caso di svizzeri che si recano con finalità terroristiche nelle aree a presenza jihadista, oppure di filiali estere di ditte (per lo più anch'esse in mani straniere) che sono iscritte nel registro di commercio svizzero e hanno legami con presunte attività di proliferazione. Da un lato, è giustificato non fornire a tali persone all'estero una tutela maggiore rispetto agli stranieri all'estero e, dall'altro, in simili casi non è possibile attuare misure di acquisizione soggette ad autorizzazione in Svizzera in quanto mancano gli accessi tecnici o fisici idonei.

Le chiavi di ricerca continuano a essere una qualsiasi combinazione di caratteri, cifre e lettere o un loro *mix*, attraverso cui vengono filtrati dati per generare un risultato (ad es. nomi di persone fisiche o giuridiche, numeri di telefono, indirizzi IP, algoritmi, coordinate ecc.).

Articolo 41

Capoverso 1 lettera b

Secondo la prassi sviluppata dal Tribunale amministrativo federale per quanto riguarda le domande di autorizzazione, l'attuale termine «necessità» va sostituito dagli elementi idoneità, necessità e ragionevolezza; tutti e tre risultano determinanti per valutare la proporzionalità. L'elemento della necessità continua a essere presente.

Capoverso 1bis

Le domande di esplorazione di segnali via cavo sono per lo più complesse e non urgenti, motivo per cui si giustifica una proroga a 10 giorni lavorativi del termine decisionale.

Capoverso 2

Qui si è soltanto sostituita l'espressione «Il seguito della procedura» con «Per il resto, la procedura». Così si segnala in particolare che anche in questo caso la decisione è presa da un giudice unico.

Capoverso 3

Alla stregua di una misura di acquisizione soggetta ad autorizzazione, l'esplorazione di segnali via cavo necessita dell'autorizzazione giudiziaria da parte del TAF e, di seguito, del nullaosta politico da parte del capo del DDPS, previa consultazione dei suoi omologhi del DFAE e del DFGP. Secondo il diritto vigente, la prima autorizzazione è valida sei mesi al massimo e può essere prorogata di volta in volta di tre mesi al massimo, applicando la medesima procedura.

L'esplorazione di segnali via cavo è onerosa ed estremamente complessa. Per lo meno attualmente è idonea soltanto per un'acquisizione di informazioni di lunga durata su eventi all'estero importanti ai fini della politica di sicurezza. Poiché ha un orizzonte temporale lungo, i termini previsti dall'attuale legge si sono dimostrati nettamente troppo brevi: onde assicurare un esercizio senza interruzioni, già oggi, per ogni mandato di esplorazione di segnali via cavo, il SIC deve presentare dopo soli due mesi una domanda di proroga per la procedura di autorizzazione del TAF e per la procedura di nullaosta a livello politico. Occorre altresì notare che adattamenti dei sistemi o

altre misure (ad es. il potenziamento delle linee) spesso non producono subito risultati conformi, ma richiedono un periodo più lungo a tal fine. A ciò si aggiunge che l'esplorazione di segnali via cavo in Svizzera è ancora un terreno inesplorato e lo sviluppo delle conoscenze in corso ha bisogno di tempo.

Prorogando il termine per l'autorizzazione si tiene conto dell'orientamento prevalentemente strategico dell'esplorazione di segnali via cavo. Nell'ambito delle attività informative concernenti l'estero, le situazioni di minaccia e quindi le esigenze informative non mutano al ritmo di tre mesi e le capacità del SIC e del TAF possono dunque essere impiegate in modo più appropriato che non per procedure di autorizzazione che si susseguono rapidamente.

Per poter continuare a reagire in modo flessibile e tempestivo a mutamenti della situazione e necessità di esplorazione, anche con una durata più lunga delle autorizzazioni c'è la possibilità di adeguare il mandato. È il caso, ad esempio, quando per un mandato di esplorazione di segnali via cavo devono essere inclusi nuovi fornitori di servizi di telecomunicazione (FST), ubicazioni supplementari di un fornitore di servizi di telecomunicazioni esistente o nuove categorie di chiavi di ricerca. Il SIC deve chiedere anche tali adeguamenti secondo la procedura normale.

Articolo 42

Capoverso 3bis

Nell'emanare la LAIn si è partiti dal presupposto che, come previsto nell'articolo 43, i gestori di reti filari e i fornitori di servizi di telecomunicazione siano in grado di fornire informazioni sufficienti, in particolare sui flussi di dati internazionali che gestiscono. Nei primi casi di impiego dell'esplorazione di segnali via cavo si è evidenziato che ciò avviene in misura assai limitata. I gestori svizzeri spesso conoscono soltanto i punti di origine e di destinazione dei flussi di dati nei Paesi limitrofi e non i loro punti di provenienza o punti finali di più ampia portata. Le modalità di svolgimento di tali flussi di dati e il tipo di dati di comunicazione da trasportare sono soggetti a una rapida e continua evoluzione.

I flussi di dati internazionali sono condotti attraverso reti altamente dinamiche, i cui instradamenti cambiano rapidamente e non possono essere previsti sul lungo periodo. I fornitori di servizi di telecomunicazione ottimizzano costantemente i propri flussi di dati, sia per migliorare la qualità della trasmissione, sia per considerazioni di natura economica. Il servizio addetto all'esplorazione deve perciò poter eseguire un'analisi tecnica dei segnali e dei dati rilevati nell'ambito di mandati esistenti, al fine di fornire un quadro il più possibile aggiornato e vicino alla realtà dei flussi di dati trattati, dei segnali così trasportati e dell'origine e della destinazione dei dati di comunicazione. Si tratta altresì di determinare le caratteristiche tecniche dei segnali rilevati, in quanto ciò influisce direttamente sui mezzi tecnici che il servizio deve utilizzare per rilevare e trattare i segnali.

Questo tipo di analisi è di natura tecnica e non riguarda il contenuto informativo dei dati rilevati. Il servizio COE addetto all'esplorazione conserva tali informazioni tecniche quali basi per ulteriori mandati. Si tratta di individuare dove vengono trasportati quali tipi di flussi di dati e quali di essi possono contenere informazioni rilevanti sotto il profilo informativo. Il suddetto servizio può condividere i riscontri così acquisiti con il SIC per consentirgli di formulare in modo più mirato i mandati di esplorazione di segnali via cavo, vale a dire indicare i flussi di dati da sorvegliare in questi mandati.

Capitolo 4: Trattamento dei dati e controllo della qualità

Osservazioni generali

Nel suo rapporto annuale 2019 la DelCG proponeva di esaminare, nell'ambito della prossima revisione della LAIn, un'impostazione alternativa per il trattamento dei dati nella quale lo scopo dei sistemi d'informazione (art. 47−57 LAIn), le regole per il trasferimento di dati tra i sistemi (ar. 44 LAIn) e l'applicabilità dei limiti dell'articolo 5 LAIn sarebbero stati riequilibrati per singoli sistemi in relazione con periodi di cancellazione specifici. Si richiede una normativa decisamente meno complessa e più comprensibile. Lo scopo fondamentale dei suddetti limiti dell'articolo 5 LAIn non è tuttavia in discussione.

Il presente progetto di revisione tiene conto di tali raccomandazioni. La nuova impostazione di trattamento dei dati si caratterizza per la sua focalizzazione sui dati e sulla loro elaborazione. La verifica in entrata, la garanzia della qualità dei dati e la comunicazione dei dati sono disciplinate in modo uniforme. L'aspetto principale è la rinuncia a una differenziazione in diversi sistemi d'informazione e sistemi di memorizzazione (anche la LPD*riv* rinuncia al termine «sistema d'informazione»). Il disciplinamento è pertanto neutro dal punto di vista tecnologico, comprende tutti i dati del SIC e migliora notevolmente le possibilità di garanzia della qualità.

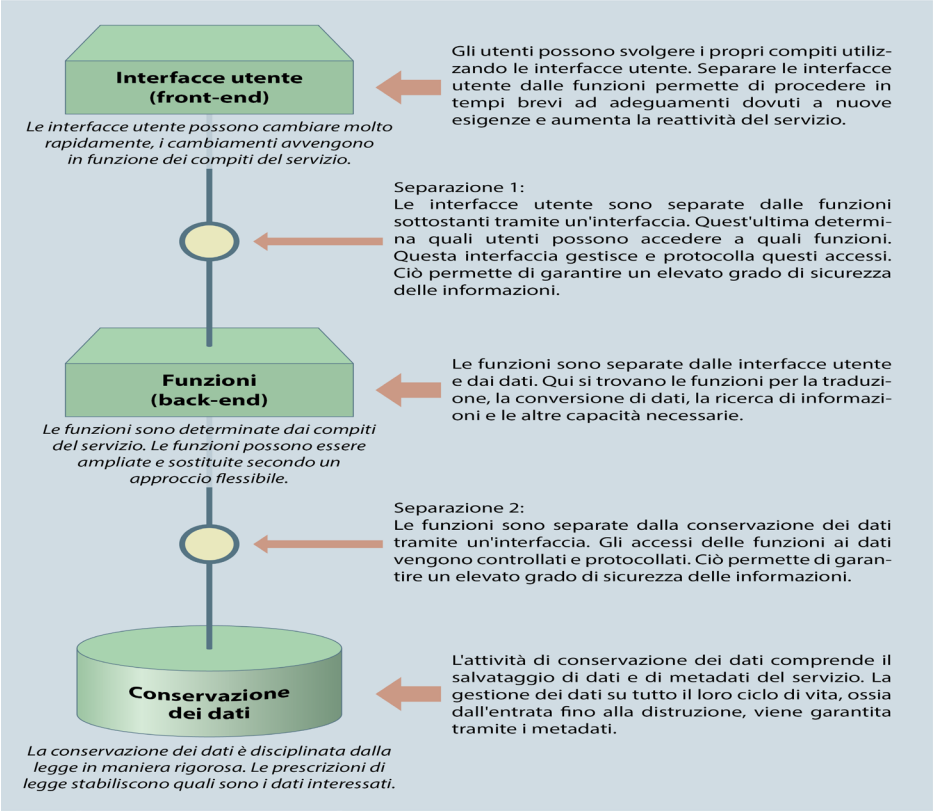
La nuova normativa non comporta un distacco sostanziale dai principi di quella attuale. Ciò vale, in particolare, anche quanto agli accessi selettivi ai dati. Si mantengono, ad esempio, le attuali categorie di dati. Per motivi di trasparenza sono indicate nuove sottocategorie, ma si tratta soltanto di contrassegni o metadati, non di categorie ai sensi della LPD*riv* quali i dati personali degni di particolare protezione ai sensi dell'articolo 5 lettera c LPD*riv*. Si mantengono anche le autorizzazioni d'accesso di altre autorità, con poche eccezioni che figurano nel commento alla sezione 5.

La rinuncia a menzionare sistemi d'informazione è anche in linea con moderni approcci di architettura informatica, che prevedono una separazione coerente tra sistemi d'informazione, logica di business e dati. Oggi risulta obsoleto il lavoro con sistemi d'informazione monolitici, con un'unità fisica di dati e software. Attualmente i dati vengono conservati in modo sicuro e ridondante in soluzioni di memorizzazione tecnicamente idonee. La memorizzazione su un layer di conservazione dei dati, abbinata al collegamento che avviene in modo del tutto logico con le soluzioni di software di accesso, permette di rinunciare alle memorizzazioni multiple di dati e una gestione dei dati che li comprenda tutti (verifica periodica, correzione, cancellazione, archiviazione) sull'intero ciclo di vita dei dati.

Anche senza il ricorso a sistemi d'informazione, come finora gli accessi possono essere gestiti in modo differenziato. Dato che però la tematica dell'accesso è ora collocata a livelli architettonici superiori (layer del servizio dati e layer del servizio app), i diritti d'accesso non possono essere definiti soltanto grossolanamente a livello dei sistemi d'informazione, come avviene oggi, ma, oltre a ciò, anche in

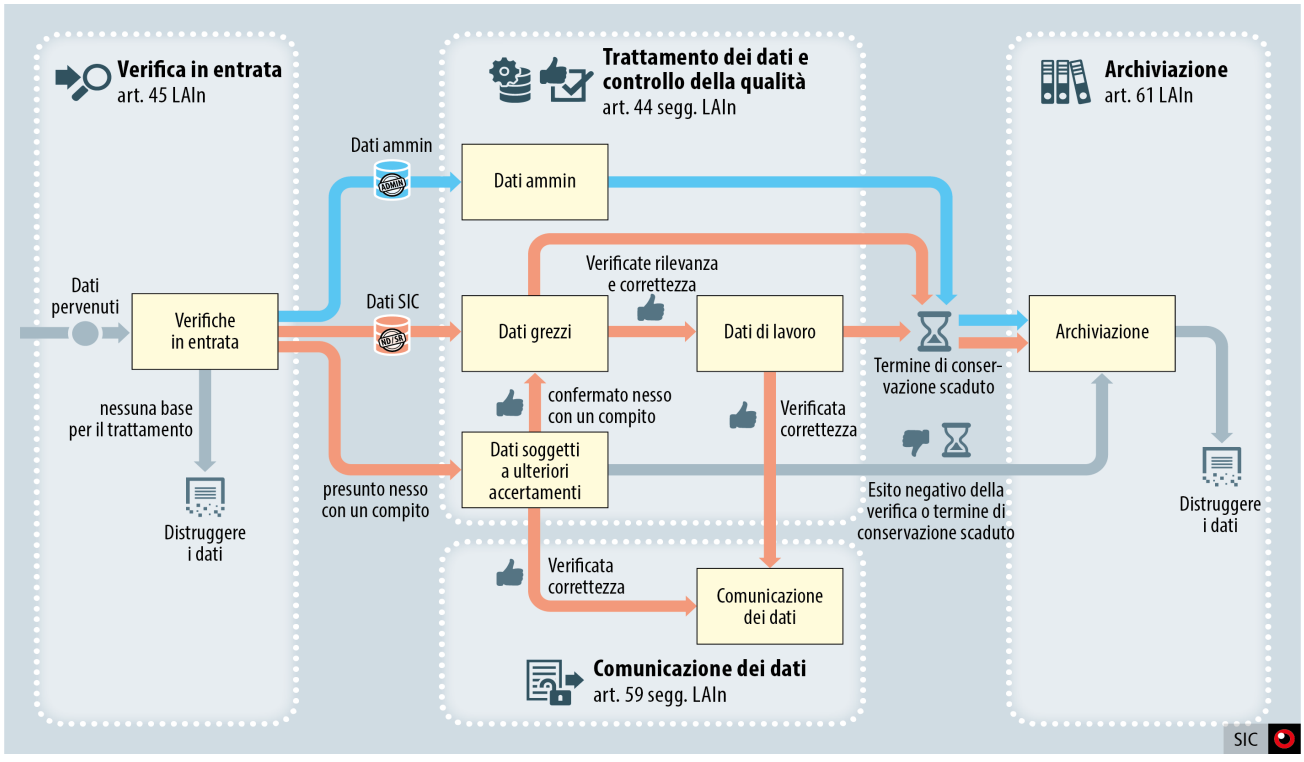
modo più preciso fino a livello di trattamento dei dati e di singole informazioni. Partendo da un concetto di accesso e di ruolo, sia le autorizzazioni funzionali (quali strumenti sono disponibili per quale ruolo), sia le autorizzazioni professionali (quali dati sono disponibili per quali ruoli e possono essere elaborati da questi ultimi) possono essere gestite con precisione. Pertanto, anche in futuro sarà possibile eseguire senza problemi oneri di diritto riguardanti gli accessi. Ora il disciplinamento nella legge segue le quattro fasi nel ciclo di vita dei dati: l'entrata dei dati, la loro utilizzazione, la comunicazione a servizi al di fuori del SIC e la cancellazione e l'archiviazione.

Nel presente commento ai vari articoli si fa di volta in volta riferimento alla LPD*riv*.



Panoramica sull’architettura informatica

Panoramica sul trattamento dei dati ai sensi della LAIn



All'entrata dei dati si verifica se si tratta di dati informativi o amministrativi (verifica in entrata). I dati amministrativi riguardano tutti i dati che il SIC tratta basandosi sulla LOGA e che, fondandosi sulla pertinente legislazione cantonale, le autorità d'esecuzione cantonali trattano a fini amministrativi, che dunque non servono all'adempimento dei compiti ai sensi dell'articolo 6 LAIn. Vi rientrano, tra l'altro, i dati relativi ai collaboratori del SIC e delle autorità d'esecuzione cantonali, alle persone che entrano in contatto con il SIC, ad esempio per richieste generali o richieste di informazioni, a progetti, ad affari politici ecc. I dati amministrativi vengono contrassegnati come tali e trattati ulteriormente secondo le rispettive basi legali. I dati informativi riguardano tutti i compiti elencati nell'articolo 6 LAIn. Si tratta dell'insieme dei dati trattati dal SIC e dalle autorità d'esecuzione cantonali per adempiere tali compiti, nonché dei dati che a loro volta servono per ottenere tali dati informativi. I dati informativi sono verificati in sequenza mediante le seguenti domande: èdato il nesso con i compiti di cui all'articolo 6? Si tratta di dati provenienti da fonti accessibili al pubblico? In caso di risposte negative, ne sono interessati i limiti posti al trattamento dei dati dell'articolo 5? In linea di massima, la verifica del nesso con i compiti ha luogo prima dell'esame di detti limiti. Idati provenienti da fonti accessibili al pubblico, come i media elettronici o cartacei, sono verificati all'entrata dei dati soltanto per ciò che riguarda il nesso con i compiti, poiché il SIC non è in grado di gestire il contenuto di tali comunicazioni e simili dati sono assai numerosi. La verifica si effettua però unicamente se il SIC vuole utilizzare tali dati per allestire prodotti informativi.

Quanto all'utilizzazione dei dati, si tratta in particolare dell'analisi, della compressione e della messa in rete di dati e dell'allestimento di prodotti. I dati amministrativi non hanno ulteriori sottocategorie legali e non saranno ulteriormente verificati durante la loro utilizzazione. Il loro ulteriore trattamento è determinato in particolare dalla LOGA.

Dopo la loro entrata, in base ai risultati della verifica in entrata i dati informativi sono categorizzati in modo differente: dati grezzi se è dato il nesso con i compiti (esclusi i dati provenienti da fonti accessibili al pubblico) e se ha avuto luogo la verifica dei limiti posti al trattamento dei dati. Tendenzialmente, i dati grezzi hanno una durata di conservazione media e sono periodicamente verificati a campione dall'organo di controllo della qualità del SIC. Non possono essere comunicati a terzi senza ulteriore verifica né essere utilizzati nei prodotti del SIC. Ha inoltre luogo una categorizzazione in dati di lavoro. Si tratta di dati grezzi informativi previsti per un ulteriore trattamento approfondito da parte del SIC e contrassegnati come tali, nonché dei prodotti risultanti da tali trattamenti di dati (ad es. rapporti d'analisi, rapporti di situazione, allarmi). I dati di lavoro hanno una durata di conservazione tendenzialmente più lunga. La verifica che tali dati siano destinati a un ulteriore trattamento approfondito è considerata la prima verifica periodica. I dati di lavoro vengono quindi controllati e gestiti a intervalli regolari dagli specialisti e verificati a campione dal summenzionato organo di controllo della qualità. Vengono poi verificati al momento di comunicarli, il che è a sua volta considerata una verifica periodica.

Nella comunicazione a terzi, i dati di lavoro sono soggetti a una verifica della comunicazione secondo tre criteri: la comunicazione è necessaria e adeguata e sono soddisfatti i presupposti giuridici per la comunicazione a terzi? In occasione della suddetta verifica ha luogo ogni volta anche una verifica critica per vedere se il SIC continua a necessitare dei pertinenti dati di lavoro per l'adempimento dei propri compiti. I dati che non sono più necessari vengono cancellati e quelli che continuano a esserlo confermati (verifica periodica).

Il SIC offre all'Archivio federale svizzero (AFS) sia i dati amministrativi che quelli informativi non appena essi non sono più necessari in modo permanente. L'AFS decide in merito alla necessità di archiviarli. Il SIC cede all'AFS i dati indicati da quest'ultimo come aventi un valore archivistico e li distrugge nei propri archivi. La relativa nomenclatura (cancellare, cedere, distruggere) è applicata in modo coerente nella LAIn.

Capitolo/titolo

Il capitolo 4 è stato riorganizzato per una migliore visione d'insieme (1° categorie, 2° verifica in entrata, 3° trattamento di dati di lavoro, 4° presentazione elettronica della situazione, 5° autorizzazioni d'accesso e 6° garanzia della qualità). Le disposizioni speciali sulla protezione dei dati e sull'archiviazione sono state spostate in un nuovo capitolo 4*a*. Per tale motivo è stato modificato anche il titolo del capitolo 4. Come già indicato, la sequenza segue quindi in gran parte le fasi del processo dall'entrata dei dati al SIC fino alla loro archiviazione/distruzione. Ai sensi della LPD*riv*, ora si parla in modo uniforme di dati e dati personali.

Sezione 1: Categorie di dati

Articolo 44

Capoverso 1

Nella presente disposizione si definiscono le due categorie principali cui sono assegnati i dati in entrata e quelli già memorizzati: i dati informativi, trattati dal SIC e dalle autorità d'esecuzione cantonali allo scopo di adempiere i propri compiti elencati nell'articolo 6, e i dati amministrativi, trattati allo scopo di adempiere i propri compiti amministrativi o per la manutenzione e l'ulteriore sviluppo di soluzioni informatiche (sul concetto di compiti amministrativi, cfr. anche l'elenco esemplificativo nelle osservazioni generali, v. sopra). In quest'ultimo caso, si intendono in particolare il codice sorgente o i dati di base delle applicazioni (ad es. carte o l'assegnazione di indirizzi a coordinate geografiche in un sistema di geoinformazioni).

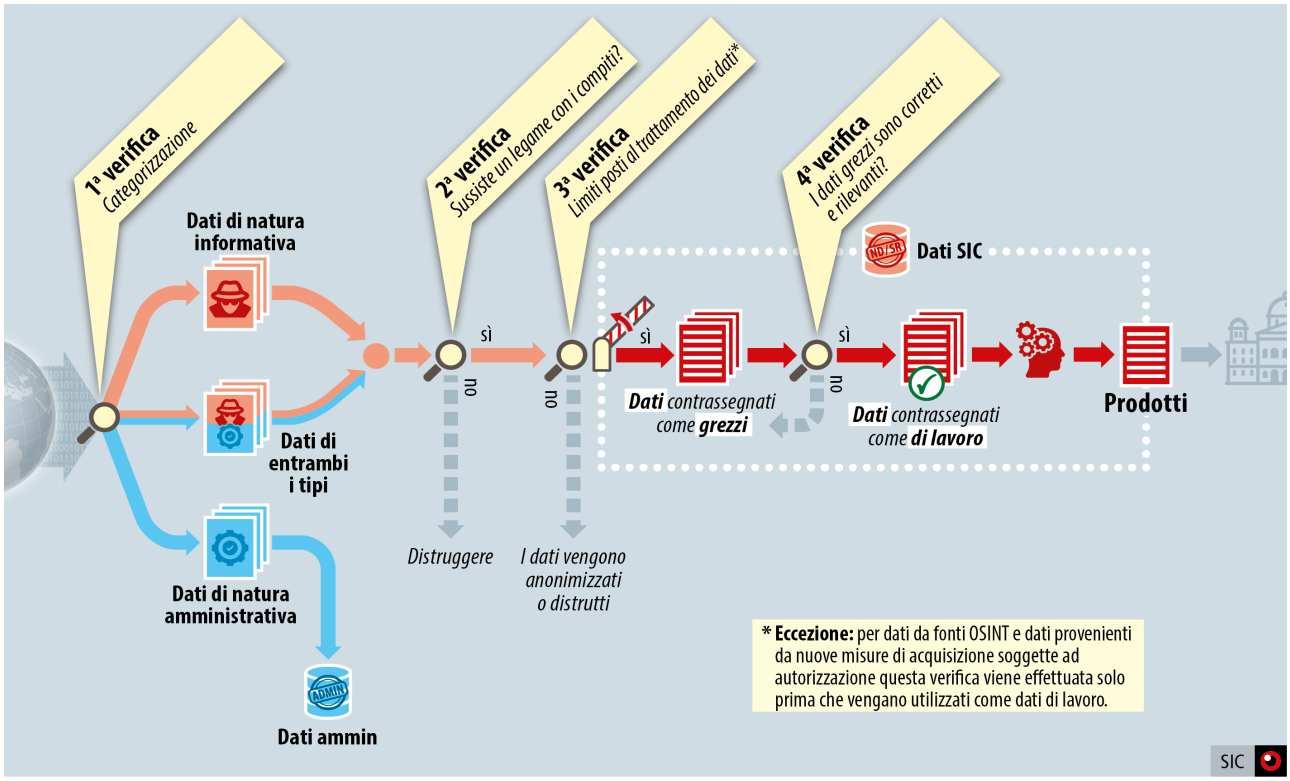
Capoverso 2

I dati informativi sono ulteriormente suddivisi in dati grezzi e dati di lavoro. Dopo la verifica in entrata, i dati informativi vengono memorizzati inizialmente solo presso il SIC e le autorità d'esecuzione cantonali. Senza la verifica dell'esattezza e della rilevanza, i dati grezzi non possono essere ulteriormente utilizzati. I dati di lavoro sono dati grezzi di cui è stata verificata l'esattezza e che in virtù della loro rilevanza attuale vengono davvero trattati ulteriormente, nonché i prodotti risultanti dall'ulteriore trattamento.

Sezione 2: Verifica in entrata

Articolo 45

Panoramica della verifica in entrata



Capoverso 1

Come menzionato in precedenza, in una prima fase il SIC e le autorità d'esecuzione cantonali verificano se i dati in entrata sono di natura informativa oppure amministrativa e li contrassegnano di conseguenza. Questa verifica è effettuata al momento della memorizzazione dei dati (di norma, entro un giorno lavorativo; cfr. però le eccezioni di cui agli art. 45 cpv. 4 e 46 cpv. 2).

Capoverso 2

Se i dati sono tanto di natura informativa quanto di natura amministrativa, vengono contrassegnati di conseguenza. Per assicurare il rispetto delle prescrizioni relative ai trattamenti di dati, più rigorose in caso di dubbio, essi vengono trattati alla stregua di dati informativi, fatta eccezione per il diritto d'accesso ai sensi della legge sulla protezione dei dati, dove sono gestiti secondo i disciplinamenti più trasparenti previsti per i dati amministrativi.

Capoverso 3

Se i dati non possono essere assegnati a nessuna delle due categorie, il SIC li distrugge o li anonimizza, oppure li rispedisce al mittente.

Capoverso 4

Può succedere che nel momento in cui entrano i dati non sia ancora chiaro se sussista un nesso con i compiti. Così è possibile, ad esempio, che un servizio partner faccia pervenire al SIC una richiesta di informazioni inerente a una persona che nel suo Paese diffonde idee razziste e di estrema destra, il che già motiva una competenza dell'autorità estera. Poiché detta persona ha soggiornato a lungo in Svizzera, il servizio partner desidera ora sapere se il SIC dispone di ulteriori informazioni al riguardo. In seguito, il SIC conferisce all'autorità d'esecuzione cantonale del Cantone in cui ha soggiornato la persona in questione un mandato affinché indaghi su quest'ultima. Soltanto il risultato del mandato dimostrerà se si tratta di un estremista *violento* e dunque se è dato il nesso con i compiti ed è quindi ammesso un ulteriore trattamento dei dati. È altresì ipotizzabile che in tale contesto si interpellino terzi (privati). Si pensi, ad esempio, a un informatore per il quale occorre chiarire determinate questioni, o ai genitori di un alunno di cui si presume si sia radicalizzato in forma violenta, oppure alla moglie di un presunto combattente straniero jihadista. In tali casi la comunicazione è quindi funzionale alla verifica in entrata, è soggetta ai limiti degli articoli 59–61 ed è consentita soltanto per quanto necessaria ad accertare il nesso con i compiti. Ovviamente ciò può verificarsi anche per i dati che pervengono alle autorità d'esecuzione cantonali. Per ragioni di trasparenza, la procedura da seguire per il necessario chiarimento del presunto nesso è ora sancita in modo esplicito nella LAIn.

Articolo 46

Capoverso 1

Se è dato il nesso con i compiti, il SIC e le autorità d'esecuzione cantonali si assicurano che i dati non contengano elementi soggetti ai limiti posti al trattamento dei dati dell'articolo 5 capoverso 5, se non si applica una delle eccezioni dell'articolo 5 capoversi 6 o 8. L'attuale disposizione dell'articolo 45 capoverso 1, secondo cui le informazioni contenenti più dati personali vengono valutate nel loro insieme, è abbandonata a causa delle critiche espresse dall'autorità di vigilanza parlamentare. Ora il SIC e le autorità d'esecuzione cantonali assicurano che le comunicazioni informative ricevute non contengono dati personali che violano i limiti posti al trattamento dei dati di cui all'articolo 5 capoverso 5, anche se la comunicazione contiene dati su più persone o fatti.

Capoverso 2

Poiché le informazioni pubblicate (come i media elettronici o cartacei) possono essere consultate in qualsiasi momento da chiunque, non ha alcun senso, in sede di mera memorizzazione, assoggettarle ai limiti posti al trattamento dei dati dell'articolo 5 capoverso 5 o valutarne l'esattezza. Spesso l'esattezza dei servizi dei media può essere giudicata soltanto dopo un po' di tempo ed essi non sono conformi alle prescrizioni della LAIn, così come devono essere rispettate nei rapporti delle autorità d'esecuzione cantonali. Nello specifico, i servizi in merito a eventi rilevanti per la LAIn (ad es. attentati terroristici e casi di spionaggio) spesso contengono dichiarazioni di esponenti politici in merito agli avvenimenti. Il SIC e le autorità d'esecuzione cantonali devono comunque poterli memorizzare senza dover ricorrere a una costosa e inefficiente censura preventiva. Nel caso di dati provenienti da fonti accessibili al pubblico, il SIC e le autorità continuano pertanto a verificare i limiti posti al trattamento dei dati soltanto prima di impiegarli quali dati di lavoro. Tale prassi è stata giudicata accettabile dall'UFG in un parere legale allestito per conto del DDPS nel febbraio del 2020.

Fanno eccezione anche i dati relativi a misure di acquisizione soggette ad autorizzazione, per le quali il SIC verifica il rispetto dei limiti posti al trattamento dei dati quando li contrassegna per un ulteriore trattamento approfondito dei dati. Ciò corrisponde alla procedura attuale che prevede la verifica nell'ambito della registrazione nel IASA SIC.

Articolo 47

Ove il SIC possa istruire e incaricare accuratamente i mittenti dei dati in entrata, può delegare loro la verifica del nesso con i compiti e dei limiti posti al trattamento dei dati e memorizzare i dati in modo automatizzato. Oggi, nell'ambito dei dati provenienti da fonti accessibili al pubblico, lo si fa con la Base d'aiuto alla condotta (BAC COE), che trasmette al SIC i dispacci d'agenzia e i comunicati stampa che presentano effettivamente un nesso con i compiti di cui all'articolo 6. I collaboratori della BAC COE ricevono ogni anno una formazione dall'organo di controllo della qualità del SIC. Sempre annualmente, esso verifica a campione se i dati entrati in questo modo presentano il nesso secondo l'articolo 6.

Articolo 48

Il SIC dispone già oggi dell'autorizzazione di memorizzare separatamente dati provenienti da operazioni di acquisizione all'estero comparabili a misure di acquisizione soggette ad autorizzazione, dati provenienti dalle misure di acquisizione soggette ad autorizzazione e dati degni di particolare protezione (cfr. art. 36 cpv. 5, art. 58 cpv. 1 LAIn e art. 7 cpv. 2 dell'ordinanza del 16 agosto 2017[19] sui sistemi d'informazione e di memorizzazione del Servizio delle attività informative della Confederazione, OSIME-SIC). Determinanti per la memorizzazione separata possono essere il volume dei dati, la tutela del segreto (in particolare la protezione delle fonti) o la sicurezza (in particolare il rischio di contaminazione della collezione di dati e dei sistemi informatici). La memorizzazione separata può però durare soltanto per un periodo di tempo limitato che il Consiglio federale deve definire e dovrà essere adeguata al tipo di dati e al motivo della memorizzazione stessa

Articolo 49

Capoverso 2

Nel presente articolo sono indicate le sottocategorie dei dati informativi. Esse sostituiscono l'attuale contrassegno secondo il sistema d'informazione e consentono al SIC di mantenere le diverse prescrizioni in materia di trattamento dei dati attualmente in vigore per i sistemi d'informazione, in particolare l'accesso selettivo. È possibile che i dati rientrino contemporaneamente in più sottocategorie. Le seguenti sottocategorie di dati corrispondono ai sistemi d'informazione esistenti:

lettera a:	IASA SIC, Quattro P, ISCO;
lettera b:	IASA-GEX SIC;
lettera c:	Portale OSINT;
lettera d:	sistemi di memorizzazione per misure di acquisizione soggette ad autorizzazione;
lettera e:	sistemi di memorizzazione per misure di acquisizione soggette ad autorizzazione;
lettera f:	archiviazione per dati degni di particolare protezione (cfr. art. 7 OSIME-SIC);
lettera g:	PES;
lettera h:	IASA SIC, IASA-GEX SIC e nel SICant INDEX di cui all'articolo 29 lettera b OSIME-SIC;
lettera i:	IASA SIC, IASA-GEX NDB e nel SICant INDEX di cui all'articolo 29 lettera b OSIME-SIC;

[19] RS **121.2**

lettera j: si tratta di dati del Laboratorio tecnico ciber SIC che vengono memorizzati e valutati su una rete separata. I dati tecnici servono per il lavoro di analisi dinamico in caso di reti e computer tecnicamente compromessi. Non vengono trattati dati personali. Oggi il riassunto / la valutazione dei dati avviene in IASA SIC;

lettera k: SICant INDEX di cui all'articolo 29 lettera b OSIME-SIC;

lettera l: archiviazione temporanea «controllo della memorizzazione»;

lettera m: IASA INDEX di cui all'articolo 29 lettera a OSIME-SIC.

Articolo 50

Capoverso 1

Il presente capoverso corrisponde in gran parte all'attuale articolo 58 capoverso 2. La nuova disposizione prevede che per questi dati la verifica in entrata debba essere effettuata al più tardi entro la fine dell'operazione di cui all'articolo 45. Ciò è necessario in quanto spesso (le collezioni d) i dati non possono essere sottoposte a verifica in entrata proprio al momento della loro memorizzazione e devono essere poste in unico contesto anche con altri dati raccolti nell'ambito dell'operazione. I dati possono però essere utilizzati soltanto dopo la verifica in entrata. Se i dati presentano un tale nesso, nell'ambito di detta verifica vengono contrassegnati quali dati grezzi o dati di lavoro. In caso contrario, devono essere distrutti e il criterio di collegamento del termine per la distruzione si modifica. Ciò è dovuto al fatto che un'operazione può durare diversi mesi o addirittura anni, mentre le singole misure possono essere concluse già dopo pochi giorni. In base all'esperienza fatta dal SIC, un'operazione dura in media da 6 mesi a 2 anni. Ne consegue che oggi devono essere distrutti dati anche se la loro analisi non è ancora stata affatto completata o la cui rilevanza avrebbe potuto essere valutata soltanto nell'ulteriore corso dell'operazione.

A titolo illustrativo, ecco alcuni esempi: il SIC conduce un'operazione riguardo a un agente dei servizi di intelligence straniero in Svizzera (persona A) che gli è noto, in relazione all'avvelenamento di un politico dell'opposizione all'estero onde chiarire il coinvolgimento dell'agente nell'avvelenamento. Nell'ambito di tale operazione vengono adottate misure di acquisizione soggette ad autorizzazione nei confronti della persona A e consultati i dati marginali dei suoi mezzi di comunicazione. In questi dati marginali il SIC scopre contatti della persona A con vari servizi statali, altri agenti dei servizi di intelligence e la persona B. Quest'ultima non è nota al SIC ed esso è tenuto a distruggere i dati che la riguardano un mese dopo la conclusione delle misure di acquisizione soggette ad autorizzazione, vale a dire dopo avere ricevuto i dati marginali. L'operazione prosegue e due mesi dopo al SIC è noto che una persona B è sospettata di essere parte del programma di armi chimiche del Paese in questione. Poiché i risultati derivanti dalle misure di acquisizione soggette ad autorizzazione sono già distrutti, il SIC non è in grado di stabilire alcuna connessione tra le persone A e B, sebbene l'operazione nel complesso non sia ancora terminata.

Innanzitutto nell'analisi di dati marginali retroattivi di collegamenti di telecomunicazione l'attuale termine mensile è molto problematico, poiché la misura di acquisizione soggetta ad autorizzazione si conclude con la consegna dei dati marginali di un periodo massimo di sei mesi, mentre l'analisi dei dati può richiedere molto più di un mese. Il SIC deve dapprima accertare e identificare gli abbonati e i presunti utenti dei partner di comunicazione della persona sottoposta a sorveglianza. In seguito è importante che i risultati delle varie misure di acquisizione soggette ad autorizzazione siano sottoposti a controlli incrociati per individuare eventuali persone chiave. Le identificazioni e gli accertamenti presso servizi partner esteri del SIC spesso durano fino alla fine dell'operazione. Una distruzione anticipata delle informazioni può così compromettere sia gli obiettivi dell'operazione sia la credibilità del SIC nei confronti dei partner.

È pertanto necessario fissare la data della distruzione a un mese dopo la conclusione dell'operazione.

Capoverso 2

Il presente capoverso corrisponde all'articolo 58 capoverso 3 e contiene soltanto chiarimenti formali.

Capoverso 3

Il presente capoverso corrisponde all'articolo 58 capoverso 4 e contiene soltanto chiarimenti formali.

Sezione 3: Trattamento di dati di lavoro

Articolo 51

Capoverso 1

Per verificare l'esattezza dei dati è necessario collocarli in un contesto con ulteriori informazioni. Non è possibile occuparsi del loro contenuto dal punto di vista informativo già al momento del salvataggio, mentre ciò avviene al momento del trasferimento dei dati grezzi ai dati di lavoro. Questa verifica viene registrata. I dati non verificati (dati grezzi) non possono, in linea di massima, essere utilizzati per la valutazione informativa e la produzione. Un'eccezione molto limitata riguarda unicamente il semplice accesso ai dati, provenienti da fonti accessibili al pubblico nell'articolo 57 capoverso 2, da parte delle autorità d'esecuzione cantonali. Anche in questo caso ogni ulteriore utilizzo comporta però una verifica dei dati preliminare.

Capoverso 2

I termini «disinformazione» e «false informazioni» sono stati sostituiti da «dati personali falsi». Il SIC deve potere trattare questi dati personali falsi non soltanto per valutare la situazione o una fonte, ma anche per altri compiti elencati nell'articolo 6. Negli ultimi anni sempre più spesso organi al vertice di governi esteri, ma anche privati, hanno impiegato false informazioni, ad esempio per influenzare elezioni o l'opinione pubblica, per sviare l'attenzione da un evento o pilotare un dibattito pubblico, destabilizzando così intere società di altri Paesi. A tal fine si attaccano direttamente persone e si diffondono false informazioni su di loro. Il SIC deve poterle trattare per adempiere i suoi compiti di cui all'articolo 6. Per consentire una chiara identificazione di questi dati, esso li contrassegna come inesatti.

Articolo 52

Capoverso 1

Nel presente capoverso vengono elencati gli scopi per i quali il SIC e le autorità d'esecuzione cantonali possono trattare dati. Oggi gli scopi del trattamento sono disciplinati presso i relativi sistemi d'informazione e sistemi di memorizzazione e rimangono invariati (cfr. in merito anche le considerazioni sull'art. 49).

Capoverso 2

Nella LPD*riv* non si utilizza più la nozione di profilo della personalità. Essa viene ora sostituita da «altri dati personali che consentono di valutare il livello di pericolosità di una persona o di un'organizzazione», ripreso qui.

In futuro, il SIC dovrà fare sempre più affidamento sull'analisi automatizzata dei suoi dati per potere, su tale base e in parte in modo automatizzato, essere in grado di riconoscere e valutare le caratteristiche di una persona o di confrontare in modo automatizzato dati in entrata oppure dati che ha acquisito esso stesso con i dati informativi esistenti. Ciò è ipotizzabile per valutare un profilo degli spostamenti di una persona scelta come obiettivo, per un'elaborazione temporale di eventi o per evidenziare eventuali cambiamenti nel comportamento delle persone (radicalizzazione ecc.). Oggi l'impiego di programmi d'apprendimento per la ricerca e la categorizzazione di informazioni è indispensabile per l'adempimento efficace dei compiti da parte del SIC ed è richiesto anche da organi di vigilanza. Non è invece previsto l'uso dell'intelligenza artificiale ai fini di decisioni individuali automatizzate (art. 21 LPD*riv*) o di un uso di supporto dell'intelligenza artificiale con il rischio di gravi ingerenze nei diritti fondamentali (art. 34 cpv. 2 lett. c LPD*riv*). Se si dovesse prevedere un tale impiego, si dovrebbero creare le basi legali adeguate. Si noti infine che la formulazione scelta nel presente disegno coincide, ad esempio, con quella della legge federale del 20 marzo 1981[20] sull'assicurazione contro gli infortuni.

Poiché attualmente il trattamento e l'analisi automatizzati dei dati (ossia in un sistema informatico e non su carta) è la regola, ora si rinuncia a un'apposita clausola di autorizzazione nella legge (finora art. 44 cpv. 4; cfr. in merito anche l'art. 7 LPD*riv*, che presuppone un trattamento dei dati automatizzato).

Capoverso 3

Per ragioni di trasparenza occorre ora disciplinare esplicitamente che il SIC e le autorità d'esecuzione cantonali possono anche trattare dati personali a discarico della persona. Ma ciò soltanto a condizione che siano già stati trattati dati personali a carico della stessa persona o della stessa organizzazione e che tali dati ora siano stati confutati in parte o del tutto. A seconda dell'importanza dei dati, ciò può comportare che in seguito vengano cancellati e archiviati anticipatamente o distrutti.

Capoverso 4

Il presente capoverso corrisponde in gran parte all'attuale articolo 47 capoverso 2. Le competenze in materia di trattamento dei dati sono state abrogate in quanto tali competenze risultano ogni volta dalla matrice delle autorizzazioni di accesso. A fini di trasparenza, nella lettera e è stata aggiunta la distruzione dei dati. Per quanto riguarda le singole competenze di delega, occorre osservare quanto segue:

- lettera a: attualmente il catalogo dei dati personali è disciplinato negli allegati dell'OSIME-SIC e non si prevede di modificarlo o di ampliarlo;
- lettera b: attualmente i diritti d'accesso individuali sono disciplinati negli allegati dell'OSIME-SIC e non si prevede di modificarli o di ampliarli (eccezioni: Aggruppamento Difesa, UDSC);
- lettera c: attualmente nell'OSIME-SIC la frequenza del controllo della qualità è disciplinata separatamente per ogni sistema d'informazione e non si prevede di modificarla o di ridurla;
- lettera d: attualmente nell'OSIME-SIC anche la durata di conservazione è disciplinata separatamente per ogni sistema d'informazione e non si prevede di modificarla o di ridurla;
- lettera e: attualmente la cancellazione e la distruzione di dati sono disciplinate negli articoli 8, 9 e 69 OSIME-SIC e non si prevede di modificare queste prescrizioni;
- lettera f: attualmente la sicurezza dei dati è disciplinata nell'articolo 13 OSIME-SIC e non si prevede di modificare queste prescrizioni.

Capoverso 5

Il presente capoverso corrisponde, in termini di contenuto, all'attuale articolo 55 capoversi 1 e 4.

Articolo 53

Capoverso 1

Il capoverso 1 corrisponde, in termini di contenuto, all'attuale disciplinamento dell'articolo 46 capoverso 1. Il termine «collezione di dati» è abrogato con la LPD*riv* e sostituito con «ambiente di lavoro». Le autorità d'esecuzione cantonali trattano i dati rilevanti per la LAIn nell'ambiente di lavoro messo a disposizione dal SIC. Non possono utilizzare strumenti informatici propri. Inoltre, per ragioni di trasparenza, si chiarisce che le autorità d'esecuzione cantonali sono autorizzate a memorizzare temporaneamente nel proprio ambiente di lavoro cantonale dati per il trasferimento nella rete appositamente protetta nella quale si trova l'ambiente di lavoro messo a disposizione dalla Confederazione. Per sua stessa natura ne risulta che le autorità d'esecuzione cantonali devono dapprima digitalizzare e memorizzare temporaneamente i dati che acquisiscono (ad es. fotografie, estratti di registri o estratti di Internet), prima di poterli

20 RS **832.20**

trattare nell'ambiente di lavoro messo a disposizione della Confederazione. Possono accedere ai dati nell'ambiente di lavoro cantonale soltanto il responsabile dell'autorità d'esecuzione cantonale o il suo supplente, nonché la persona che li ha memorizzati. Attualmente le autorità d'esecuzione cantonali sono tenute a distruggere i dati nell'ambiente di lavoro cantonale al più tardi 60 giorni dopo l'archiviazione, il che è soggetto a verifica a campione da parte dell'organo di controllo della qualità del SIC nell'ambito delle sue attività. I dati sono presi in considerazione nel trattamento delle richieste di informazioni inerenti alla protezione dei dati di cui all'articolo 63.

Capoverso 2

Il presente capoverso corrisponde all'attuale articolo 46 capoverso 2 e contiene soltanto chiarimenti formali. In particolare, si chiarisce che si tratta di dati cantonali se le autorità d'esecuzione cantonali diventano operative in applicazione del diritto cantonale (ad es. diritto di polizia). Questi dati devono essere tenuti rigorosamente separati dai dati che esse trattano fondandosi sulla LAIn.

Capoverso 3

I nuovi articoli 33 e 33bis OAIn disciplinano non solo la comunicazione di dati che i Cantoni hanno ricevuto dal SIC, ma anche la comunicazione di dati che i Cantoni hanno acquisito nell'ambito delle proprie competenze. Affinché vi sia una base legale sufficiente a tal fine, il presente capoverso viene integrato di conseguenza. Il termine «valutazione della situazione» è stato abrogato, poiché si tratta anche di dati ai sensi della LPD*riv*. La presente disposizione è stata inoltre adeguata a quella dell'articolo 6 capoverso 1, sostituendo «la salvaguardia della sicurezza o per sventare una minaccia considerevole» con «individuare tempestivamente e sventare minacce per la sicurezza interna o esterna».

Capoverso 4

Le autorità d'esecuzione cantonali devono poter continuare a conservare i risultati dei loro accertamenti preliminari per un massimo di cinque anni. Durante tale periodo hanno la possibilità di presentare rapporto al SIC. Il rapporto proroga il termine di conservazione delle relative informazioni e la cerchia delle persone autorizzate ad accedere viene estesa ai collaboratori autorizzati ad accedere del SIC e delle autorità d'esecuzione cantonali. Considerata la breve durata di conservazione, si continua anche a rinunciare a una verifica periodica degli accertamenti preliminari da parte delle autorità d'esecuzione cantonali.

Sezione 4: P*resentazione elettronica della situazione*

Articolo 54

Capoverso 1

Il presente capoverso corrisponde, in termini di contenuto, all'attuale articolo 53 capoversi 1 e 3 e conferisce al SIC l'autorizzazione di continuare a utilizzare il sistema d'informazione «Presentazione elettronica della situazione per la protezione della popolazione» (PES) dell'UFPP (cfr. al riguardo l'art. 55 cpv. 1 ordinanza dell'11 novembre 2020[21] sulla protezione della popolazione).

Capoverso 2

Oltre alle informazioni trattate dal SIC stesso, la PES contiene già informazioni di altre autorità che sono soggette a prescrizioni sulla protezione dei dati meno restrittive. Per questo motivo può essere che la PES contenga dati che secondo la LAIn il SIC stesso non potrebbe trattare. Tuttavia, la PES deve soddisfare non soltanto le esigenze del SIC, ma quelle di tutte le autorità di sicurezza della Svizzera. Ciò ha un effetto anche sul controllo della qualità dei dati nella PES: poiché anche in questo caso vi sono differenti prescrizioni a seconda dell'autorità competente, l'articolo 58*b* capoverso 4 prevede che in futuro sia competente l'autorità che ha memorizzato i dati. Oggi ciò è disciplinato per fedpol nell'articolo 44 capoverso 4 OSIME-SIC. Attualmente, nell'ottica di eventuali violazioni contro i limiti posti al trattamento dei dati del SIC, anche il termine di conservazione dei dati archiviati da fedpol è più breve (cfr. art. 45 cpv. 2 OSIME-SIC). Ciò deve continuare a valere per tutti i dati non memorizzati dalla SIC o dalle autorità d'esecuzione cantonali (cfr. le ulteriori considerazioni sulla rete informativa integrata anche nel commento all'art. 5 cpv. 5 lett. e).

Sezione 5: Diritti d'accesso

Il diritto d'accesso dell'autorità di vigilanza indipendente è disciplinato nell'articolo 78 capoverso 3.

Articolo 55

Capoverso 1

Per analogia con la normativa dell'articolo 51, le autorità d'esecuzione cantonali e le autorità federali non ottengono l'accesso a tutti i dati del SIC ma, in linea di principio, soltanto ai dati nel sistema INDEX necessari all'identificazione che, in adempimento dei propri compiti di cui all'articolo 6 capoverso 1, il SIC ha attribuito a una persona, a un'organizzazione, a un gruppo, a un oggetto o a un evento. Attualmente sono gli oggetti registrati in IASA-GEX SIC e IASA SIC a figurare nello IASA INDEX. Come avviene oggi, in futuro a queste autorità i dati attribuiti a una persona, un'organizzazione ecc. non saranno quindi resi noti mediante procedura di richiamo, ma è indicato un solo risultato, se ad esempio cognome, nome e data di nascita oppure la società corrispondono. Essi devono chiedere al SIC, tramite una procedura di assistenza amministrativa e con motivazione, la comunicazione di ulteriori dati (cfr. cpv. 2)

Rimangono invariati i diritti d'accesso sia in seno al SIC sia presso le autorità d'esecuzione cantonali e altri esterni che già oggi hanno accesso. Continua ad applicarsi il principio di proporzionalità che esige che l'accesso avvenga sulla base di ciò che occorre sapere

21 RS **520.12**

(« need-to-know »). Nell'articolo 52 capoverso 4 lettera b al Consiglio federale è conferito l'incarico di disciplinare, come finora, i diritti d'accesso dettagliati.

Lettera a

Il diritto d'accesso delle autorità d'esecuzione cantonali rimane invariato.

Lettera b

Il diritto d'accesso di fedpol rimane invariato (cfr. l'attuale art. 51 cpv. 4. lett. c). Continua a ottenere l'accesso per constatare se il SIC tratta dati informativi inerenti a una persona, un'organizzazione, un gruppo, un oggetto o un evento. I dati attribuiti a una persona, a un'organizzazione ecc. non sono resi noti a fedpol mediante procedura di richiamo; esso deve chiedere al SIC, motivandola, la comunicazione di tali dati.

Lettera c

Oggi ci sono due unità specializzate che svolgono controlli sulla sicurezza personale: una alla Cancelleria federale e una al DDPS. A tal fine, entrambi i servizi hanno accesso a dati informativi del SIC. Con una formulazione più generale inerente ai compiti, si intende ora impedire che in caso di un nuovo adeguamento dell'aggregamento organizzativo di un servizio specializzato si renda necessaria una modifica di legge. Inoltre, gli accessi per entrambi gli uffici specializzati vengono disciplinati nello stesso luogo e le modifiche sono quindi di natura puramente formale. Il diritto d'accesso rimane invariato (cfr. l'attuale art. 51 cpv. 4. lett. c). I servizi cui competono i controlli della sicurezza della persona continuano a ottenere l'accesso per constatare se il SIC tratta dati informativi inerenti a una persona, un'organizzazione, un gruppo, un oggetto o un evento. I dati attribuiti a una persona, a un'organizzazione ecc. non sono resi noti a detti servizi mediante procedura di richiamo; essi devono chiedere al SIC, tramite una procedura di assistenza amministrativa e con motivazione, la comunicazione di tali dati.

Lettera d

In virtù dei loro compiti legali, ora ottengono l'accesso anche i collaboratori dell'UDSC incaricati del perseguimento penale e dell'analisi dei rischi (cfr. lett. e). Anch'essi possono soltanto constatare se il SIC tratta dati informativi inerenti a una persona, un'organizzazione ecc. e devono chiedere, tramite una procedura di assistenza amministrativa e con motivazione, la comunicazione di ulteriori dati.

Tali accessi sono inseriti anche nella revisione della legge sulle dogane del 18 marzo 2005[22] (LD) e dunque nella nuova legge sui compiti d'esecuzione dell'UDSC[23] (LE-UDSC). I collaboratori dell'UDSC incaricati del perseguimento penale necessitano dell'accesso per adempiere questo tipo di compiti, se e nella misura in cui il diritto federale lo preveda. L'obiettivo è anche quello di ottenere un aumento dell'efficienza e di sostenere l'imperativo di celerità nei procedimenti penali. Ciò consente poi una valutazione più completa delle persone accusate e può produrre nuovi approcci investigativi, in particolare riguardo all'ambiente di tali persone. Così è inoltre possibile anche una valutazione migliore in merito alla comunicazione di persone che presentano un potenziale di minaccia nell'ambito di competenza del SIC e che compaiono in un procedimento penale dell'UDSC. I dati attribuiti a una persona, a un'organizzazione ecc. non sono resi noti a suddetti collaboratori mediante procedura di richiamo; essi devono chiedere al SIC, tramite una procedura di assistenza amministrativa e con motivazione, la comunicazione di tali dati.

Lettera e

I collaboratori dell'UDSC incaricati dell'analisi dei rischi necessitano dell'accesso per la sorveglianza [e il controllo] del traffico delle persone e delle merci attraverso il confine doganale. Anche tale scopo d'accesso coincide con la relativa formulazione del compito dell'UDSC. L'utilizzo dei dati aiuta l'analisi dei rischi da parte di quest'ultimo al fine di coordinare in modo mirato con il SIC i risultati delle analisi e di individuare possibili nessi tra vari avvenimenti. Ciò supporta anche la formulazione di istruzioni di controllo all'attenzione dei collaboratori dell'UDSC incaricati dei controlli delle persone, delle merci e dei mezzi di trasporto. I dati attribuiti a una persona, a un'organizzazione ecc. non sono resi noti a detti collaboratori mediante procedura di richiamo; essi devono chiedere al SIC, tramite una procedura di assistenza amministrativa e con motivazione, la comunicazione di tali dati.

Lettera f

L'Aggruppamento Difesa dell'Esercito svizzero ha ora il diritto d'accesso per la protezione preventiva dell'esercito dallo spionaggio, dal sabotaggio e da altri atti illeciti durante il servizio di promovimento della pace e il servizio attivo. Tale diritto tiene conto del fatto che, in relazione con il promovimento della pace (impiego dell'esercito nei Balcani), il Servizio per la protezione preventiva dell'esercito (SPPEs) deve accertare costantemente le persone. Nel 2020 ha presentato oltre 100 richieste scritte al SIC. In virtù dei compiti svolti nel servizio di promovimento della pace, il SPPEs ha accesso alle informazioni relative al terrorismo, all'estremismo violento e allo spionaggio. A causa della diaspora dei Balcani in Svizzera, spesso tali informazioni sono connesse con la sicurezza interna o, viceversa, con la sicurezza dell'Esercito svizzero nel servizio di promovimento della pace. Uno scambio di informazioni rapido ed efficiente può quindi essere determinante per la sicurezza. Grazie a un accesso mediante procedura di richiamo è possibile ridurre notevolmente gli oneri (in particolare per il 50 % circa non registrati). Devono avere il diritto d'accesso soltanto i collaboratori del SPPEs attivi negli affari operativi (funzione «Commissario SPPEs»). Anch'essi possono soltanto constatare se il SIC tratta dati informativi inerenti a una persona, un'organizzazione ecc.; devono chiedere al SIC, tramite procedura di assistenza amministrativa e con motivazione, la comunicazione di tali dati.

Capoverso 2

Per ragioni di trasparenza si indica ora che, dopo una consultazione con esito positivo, le autorità d'esecuzione cantonali e le autorità federali devono chiedere al SIC di comunicare loro ulteriori dati. La richiesta deve essere motivata e la comunicazione dei dati è soggetta alle limitazioni degli articoli 59−61.

22 RS **631.0**
23 FF **2020** 6514

Capoverso 3

Il SIC deve avere ora la possibilità di mettere a disposizione dei clienti online, per valutare le ripercussioni delle minacce in materia di politica di sicurezza e per la condotta in materia di politica di sicurezza, i propri prodotti (presentazioni della situazione, analisi e rapporti che si compongono dei dati di cui all'articolo 49 lettere a, b, c, g, h e i). Ciò si è rivelato efficace per le autorità d'esecuzione cantonali, in quanto il SIC memorizza i propri rapporti d'analisi classificati o prodotti di monitoraggio OSINT sulla piattaforma d'informazione dell'ambiente di lavoro messo a disposizione dalla Confederazione. In tal modo si può impedire che il SIC debba copiare questi prodotti e distribuirli con un'ampia cerchia di diffusione per posta elettronica o su carta. Si garantisce inoltre che esso possa occuparsi della manutenzione dei dati e cancellarli dopo un certo periodo di tempo, il che non può essere garantito per le altre forme di trasmissione. La comunicazione dei prodotti ha luogo con riserva degli articoli 59−61.

Capoverso 4

Il SIC è tenuto a garantire che non si faccia un uso improprio degli accessi concessi ai clienti. Perciò effettua verifiche a campione ed è autorizzato a chiedere loro di spiegare il motivo per cui hanno avuto accesso a quale prodotto e quando.

Articolo 56

Attualmente i diritti d'accesso dei collaboratori del SIC sono disciplinati presso i relativi sistemi d'informazione e sistemi di memorizzazione e, fatta salva un'eccezione, rimangono invariati. Ora anche alla Sicurezza SIC è concesso di accedere a dati informativi affinché, ad esempio al momento di assumere nuovi collaboratori del SIC, possa verificare se vi sono dati su di loro (sui compiti della Sicurezza SIC, cfr. anche l'art, 7 cpv. 1). Per quanto riguarda i diritti d'accesso dei collaboratori del SIC, continua ad applicarsi il principio di proporzionalità che esige che l'accesso avvenga sulla base di ciò che occorre sapere (« need-to-know »). Così, ad esempio, continueranno ad avere accesso a dati provenienti da misure di acquisizione soggette ad autorizzazione soltanto i collaboratori incaricati di eseguirne una e di valutarne i risultati.

Articolo 57

Capoverso 1

Il diritto d'accesso dei collaboratori delle autorità d'esecuzione cantonali rimane anch'esso invariato.

Capoverso 2

I collaboratori delle autorità d'esecuzione cantonali continuano ad avere inoltre accesso ai rapporti redatti di propria iniziativa o su mandato del SIC e presentati al SIC nonché ai dati informativi provenienti da fonti accessibili al pubblico. Oggi ciò è disciplinato allo stesso modo nell'articolo 51 capoverso 3 lettere b nonché nell'articolo 54 capoverso 4.

Capoverso 3

Alcune autorità d'esecuzione cantonali e la CCPCS hanno chiesto che le autorità d'esecuzione cantonali ottengano un accesso reciproco ai propri dati informativi. Questo per scoprire, senza oneri eccessivi, se l'autorità d'esecuzione cantonale di un Cantone limitrofo sta già trattando dati su una persona o su un'organizzazione. Ciò è particolarmente utile nel caso di accertamenti preliminari in corso, ossia quando la persona o l'organizzazione interessata non è stata ancora segnalata al SIC e lì registrata e le autorità d'esecuzione cantonali non sono in grado di constatare in tal modo se un'altra autorità d'esecuzione cantonale tratta dati sulla persona o sull'organizzazione interessata. Poiché non tutte le autorità d'esecuzione cantonali sono d'accordo su questa concessione dell'accesso, in questa sede ciò è disciplinato soltanto quale «clausola potestativa».

Capoverso 4

L'organo di controllo della qualità del SIC ha il compito di verificare a campione il trattamento dei dati delle autorità d'esecuzione cantonali (cfr. art. 58*c* cpv. 1). A tale scopo, l'organo ha accesso già oggi ai dati delle autorità d'esecuzione cantonali, il che verrà aggiornato per completezza.

Articolo 58

Capoverso 1

Il presente capoverso corrisponde in gran parte all'attuale articolo 53 capoverso 3. Considerata la stretta collaborazione nel settore della sicurezza, si intende ora concedere alla Polizia di Stato del Principato del Liechtenstein un accesso permanente al PES. Finora essa ha potuto accedere soltanto in caso di eventi particolari.

Capoverso 2

Il presente capoverso corrisponde all'attuale articolo 53 capoverso 4.

Articolo 58a

Capoversi 1 e 2

L'accesso ai dati amministrativi rimane invariato rispetto a oggi (cfr. art. 52 cpv. 3). Attualmente per le autorità d'esecuzione cantonali l'accesso alla loro gestione dei mandati indicato nell'articolo 29 lettera c OSIME-SIC non è però disciplinato in modo esplicito.

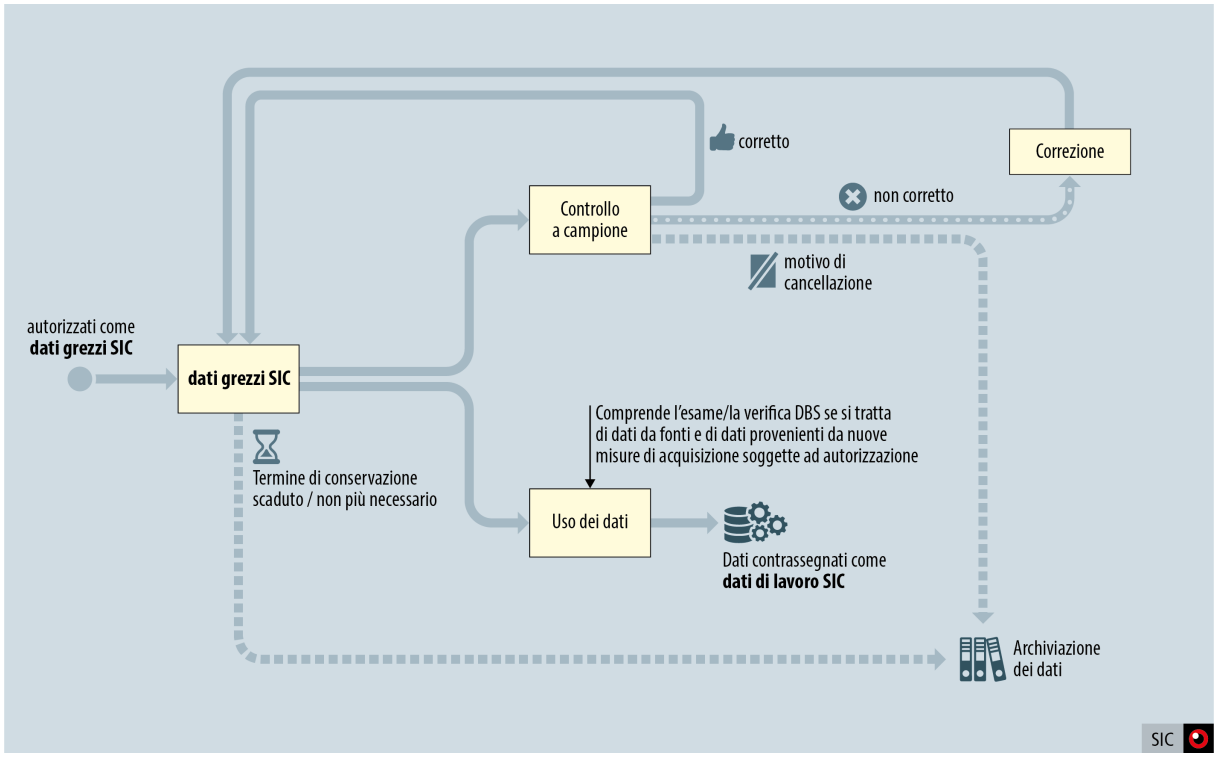
Capoverso 3

Per l'adempimento dei propri compiti il SIC dipende anche dalla collaborazione dei fornitori di prestazioni esterni. Da un lato, ciò è il caso per la manutenzione e l'ulteriore sviluppo della propria infrastruttura informatica. Data la complessità del software, spesso già

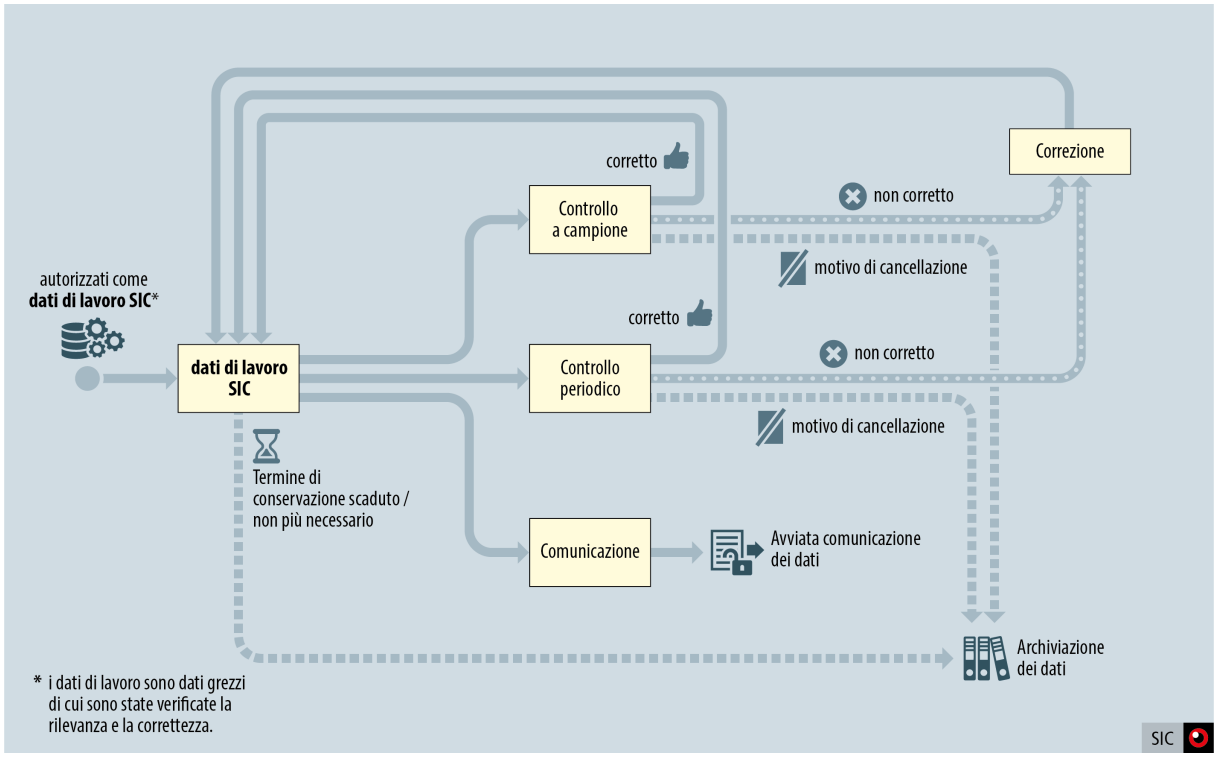
soltanto per individuare le cause dei problemi il SIC necessita di competenze esterne. Ciò vale a maggior ragione per la risoluzione dei problemi. Se, ad esempio, un collaboratore cancella per sbaglio un conto utente, soltanto il fornitore di prestazioni esterno è in grado di ripristinarlo con tutti i dati e i mandati e processi connessi. I fornitori di prestazioni esterni hanno però accesso soltanto ai metadati, non ai dati stessi. Si tratta però anche di lavori per l'ulteriore sviluppo, per i quali sono imperativamente necessarie conoscenze specialistiche esterne e devono essere trattati dati nei relativi fascicoli progettuali. Dall'altro lato, il SIC fa tradurre periodicamente testi da traduttori esterni nell'ambito di un rapporto di mandato. Il fatto che questi oggi non possano accedere ai dati amministrativi complica l'assegnazione dei mandati nonché il loro disbrigo e minaccia la sicurezza delle informazioni, dovendo essi sbrigare i mandati al di fuori della rete protetta del SIC.

Sezione 6: Controllo della qualità

Panoramica sul trattamento / controllo della qualità di dati grezzi



Panoramica sul trattamento / controllo della qualità di dati di lavoro



Articolo 58b

Capoverso 1

Il presente capoverso corrisponde, in termini di contenuto, all'attuale articolo 45 capoverso 4. Poiché la LAIn non disciplina diversi sistemi d'informazione, si parla di dati di lavoro. In passato il termine «registrazione strutturata» ha dato adito di continuo a equivoci e discussioni. Con la nuova formulazione si intende chiarire di che si tratta: dell'attribuzione di dati a persone o organizzazioni.

Capoverso 2

Il presente capoverso corrisponde, in termini di contenuto, all'ultima frase dell'attuale articolo 45 capoverso 4. Ovviamente i dati esplicitamente contrassegnati come falsi (cfr. art. 51 cpv. 2) non vengono corretti nell'ambito della verifica periodica. È stato inoltre adattato il rinvio alla riserva.

Capoverso 3

Il presente capoverso corrisponde in gran parte all'attuale articolo 45 capoverso 5. L'attuale lettera b, che prevedeva una verifica periodica dei rapporti delle autorità d'esecuzione cantonali da parte dell'organo di controllo della qualità del SIC, è stata abrogata senza essere sostituita, non essendoci alcun motivo di trattare in modo speciale tali dati. Anch'essi possono essere verificati periodicamente dagli specialisti competenti, così come prescrive il nuovo articolo 58b capoverso 1 per tutti i dati di lavoro che il SIC ha attribuito a una persona o un'organizzazione in adempimento dei propri compiti di cui all'articolo 6 capoverso 1

Oggi alle autorità d'esecuzione cantonali è vietato cancellare dati (cfr. l'attuale art. 45 cpv. 5. lett. d). Anche per tale divieto, però, non c'è più alcuna ragione plausibile. Questa prescrizione ha semmai portato a un complesso meccanismo di cancellazione che vincola inutilmente risorse da parte di suddette autorità e dell'organo di controllo della qualità del SIC. Anche la presente lettera viene pertanto abrogata senza essere sostituita. Così come avveniva prima dell'entrata in vigore della LAI, in futuro le autorità d'esecuzione cantonali dovranno poter di nuovo cancellare i propri dati se non ne hanno più bisogno o se il loro termine di conservazione è scaduto.

Con il termine «in particolare» si chiarisce inoltre che l'elenco non è esaustivo e l'organo di controllo della qualità del SIC adempie anche altri compiti.

Lettera a

La presente lettera corrisponde, in termini di contenuto, all'attuale articolo 45 capoverso 5 lettera a. Come avviene oggi, anche in futuro i dati nell'ambito dell'estremismo violento (riconoscibili grazie alla loro sottocategorizzazione, cfr. al riguardo le considerazioni sull'art. 49) dovranno essere verificati maggiormente e in una fase iniziale. Oggi ciò avviene subito dopo che i dati sono stati registrati in modo strutturato. In futuro si parlerà dell'attribuzione di dati a persone e organizzazioni, ma il momento della verifica rimane lo stesso. Nel presente disegno, il termine «rilevanza» viene sostituito sistematicamente da «nesso con i compiti». Ora si chiarisce che si verifica anche il rispetto dei limiti posti al trattamento dei dati.

Lettera b

La presente lettera corrisponde, in termini di contenuto, all'attuale articolo 45 capoverso 5 lettera c. Poiché la LAIn non disciplina più diversi sistemi d'informazione, la verifica a campione da parte dell'organo di controllo della qualità del SIC non si riferisce ai singoli sistemi d'informazione, bensì a tutti i dati informativi del SIC (dati grezzi e dati di lavoro). I termini «efficacia» e «adeguatezza» non vengono più utilizzati in quanto non figurano nel diritto in materia di protezione dei dati. Un trattamento dei dati è efficace se produce un effetto positivo; è adeguato se con tale effetto si consegue l'obiettivo perseguito. L'adeguatezza presuppone quindi concettualmente l'efficacia. Se una determinata misura consente di raggiungere lo scopo perseguito, essa è idonea. L'idoneità è una delle tre condizioni della proporzionalità. Se invece di verificare l'efficacia e l'adeguatezza si verifica la proporzionalità, il controllo della qualità viene sviluppato in quanto all'idoneità si aggiungono gli aspetti della necessità e della ragionevolezza. L'articolo 58*c* capoverso 1 disciplina i controlli a campione dei dati informativi delle autorità d'esecuzione cantonali.

Lettera c

Ora anche la persona responsabile della protezione dei dati del SIC sarà tenuta a organizzare corsi di formazione sul rispetto delle prescrizioni della presente legge con riferimento ai dati. Si chiarisce inoltre che anche i collaboratori delle autorità d'esecuzione cantonali ricevono una formazione.

Capoverso 4

Per ragioni di trasparenza, nel presente capoverso si segnala che nel sistema d'informazione PES il SIC può assumere una responsabilità di merito e garantirne la qualità soltanto riguardo ai dati trattati da esso stesso e dalle autorità d'esecuzione cantonali. Per i dati trattati da altri servizi (ad es. fedpol) sono competenti questi ultimi.

Articolo 58c

Capoverso 1

La verifica a campione dei dati informativi delle autorità d'esecuzione cantonali non è nuova, ma finora non era disciplinata in modo esplicito (cfr. l'attuale art. 45 cpv. 5. lett. c, in cui si parla soltanto di «tutti i sistemi d'informazione»). Sul concetto della proporzionalità si rinvia alle considerazioni sull'articolo 58*b* capoverso 3 lettera b.

Capoverso 2

Anche il rinvio al mittente dei rapporti delle autorità d'esecuzione cantonali, che del tutto o in parte non presentano alcun nesso con i compiti o che violano limiti posti al trattamento dei dati, attualmente non è disciplinato in modo esplicito nella LAIn (di certo però negli art. 3 cpv. 3 e 4 cpv. 2 OSIME-SIC, che già oggi prescrivono questo obbligo). Per ragioni di trasparenza e poiché in questi casi

deve essere corretto il trattamento dei dati da parte delle autorità d'esecuzione cantonali, ciò viene ora disciplinato esplicitamente. Questo *modus operandi* corrisponde alla prassi attuale.

Capitolo 4a: Disposizioni particolari sulla protezione dei dati

Con la nuova struttura, l'attuale sezione 4 del capitolo 4 diventa il capitolo 4*a*.

Sezione 1: Comunicazione di dati personali da parte del SIC

Come già menzionato all'inizio del capitolo 4, fatte salve poche eccezioni i dati grezzi non possono essere utilizzati o comunicati. Nel presente capitolo si tratta quindi, in linea di principio, di dati di lavoro che sono già stati oggetto di un esame approfondito (cfr. però le eccezioni degli artt. 5 cpv. 6 e 46 cpv. 3).

Articolo 59

Il presente articolo corrisponde in gran parte all'attuale articolo 59 e il suo contenuto rimane invariato. Per una migliore comprensione, nella rubrica si indica che si tratta della verifica di dati personali. Poiché per i prodotti informativi si tratta di dati personali, tale termine è stato soppresso. Si chiarisce inoltre che per dati personali si intendono anche dati personali degni di particolare protezione e dati personali risultanti da una profilazione. La limitazione delle prescrizioni alla LAIn è stata abrogata poiché la comunicazione deve rispettare tutte le prescrizioni legali applicabili.

Articolo 60

Il presente articolo corrisponde in gran parte all'attuale articolo 60.

Capoverso 1

Anche nel presente capoverso si chiarisce che per dati personali si intendono anche dati personali degni di particolare protezione e dati personali risultanti da una profilazione.

Capoverso 3

In linea con l'intero concetto della conservazione dei dati, nel presente capoverso il termine «dati» è semplicemente sostituito da «dati personali».

Articolo 61 capoverso 1

Anche nel presente capoverso si chiarisce che per dati personali si intendono anche dati personali degni di particolare protezione e dati personali risultanti da una profilazione. Poiché dal punto di vista della protezione dei dati non vi è alcuna differenza se i dati personali sono inclusi in un elenco, il riferimento a tali dati è stato abrogato. È importante unicamente che per ogni dato personale da comunicare sia garantito che sono soddisfatte le condizioni legali per la comunicazione.

Articolo 62

Anche nel presente articolo si chiarisce che per dati personali si intendono anche dati personali degni di particolare protezione e dati personali risultanti da una profilazione.

Lettera a

Il termine «trasmissione» è sostituito dal termine «comunicazione», utilizzato dalla LPD. Ciò non comporta alcuna modifica in termini di contenuto.

Lettera b

Qui il termine «minaccia» è sostituito dal termine «minacce», utilizzato dalla LAIn (cfr. art. 6 cpv. 1 lett. a). Non vi sono modifiche in termini di contenuto.

Lettera c

Qui il termine «domanda di informazioni» è sostituito dal termine «richiesta d'accesso». Ciò per chiarire che non si tratta di una richiesta di informazioni ai sensi degli articoli 63 e 63*a*, ma di una richiesta di accesso. Non vi sono modifiche in termini di contenuto.

Lettera d

Qui il riferimento alla comunicazione a terzi avviene nell'ambito dell'articolo 45 capoverso 4.

Sezione 2: Diritto d'accesso

L'attuale disciplinamento del diritto d'accesso è complicato ed è retto in parte dalla LPD e in parte dalle leggi speciali della LPD (per il sistema d'informazione GEVER SIC addirittura da entrambe le leggi). Ciò va semplificato, non da ultimo a favore di chi presenta richieste di informazioni.

Mentre per i dati amministrativi si dovrebbe continuare ad applicare la LPD*riv*, i dati informativi, nell'ottica della loro sensibilità, che è simile a quelli della fedpol, devono in linea di principio essere disciplinati dalla normativa attualmente prevista per fedpol per il

sistema di trattamento dei dati relativi ai reati federali (cfr. art. 8 legge federale del 13 giugno 2008[24] sui sistemi d'informazione di polizia della Confederazione, LSIP) e per le segnalazioni per l'arresto a scopo di estradizione (cfr. art. 8*a* LSIP). Ora il SIC deve poter differire l'informazione soltanto in via eccezionale e caso per caso. Se una persona che chiede informazioni non è registrata, il SIC può quindi comunicarle immediatamente la mancata registrazione.

Articolo 63

Analogamente a quanto avviene nella LSIP, le richieste di accesso a dati amministrativi (cfr. art 7 LSIP) e ai dati dei servizi d'informazione (cfr. artt. 8 e 8*a* LSIP) sono disciplinate in due articoli distinti. Ciò rende più facile evidenziare la differenza tra dati amministrativi, soggetti a una procedura amministrativa e a una decisione del SIC che può essere impugnata dinanzi al TAF e al TF, e dati informativi, per i quali c'è soltanto un diritto d'accesso indiretto.

Il diritto d'accesso per i dati esclusivamente amministrativi è quindi retto dagli articoli 25 e 26 LPDriv (cfr. art. 7 cpv. 1 LSIP).

Articolo 63a

È controverso se la rinuncia a un rimedio giuridico ordinario in caso di limitazione o di rifiuto del diritto d'accesso sia conforme alla Costituzione e al diritto internazionale ed è una questione che verrà chiarita in maniera approfondita nel corso della procedura di consultazione.

Capoverso 1

La limitazione dell'informazione è retta ora dai motivi elencati nell'articolo 26 LPD*riv*. Contrariamente all'articolo 8 capoverso 1 LSIP, non è prevista alcuna eccezione alle disposizioni della LPD*riv*. Il presente capoverso sostituisce i capoversi 1 e 2 dell'attuale articolo 63. Sempreché occorra fornire informazioni sui dati personali, nell'articolo 25 capoverso 2 lettera b della LPD*riv* si chiarisce che devono essere consegnati sempre soltanto i dati personali «in quanto tali» (e non copie di documenti).

Capoverso 2

Il presente capoverso corrisponde all'attuale articolo 63 capoverso 4. Oltre agli interessi statali al mantenimento del segreto, vi sono altri motivi per un rifiuto, una limitazione o un differimento, ovvero la protezione di terzi (ad es. una fonte). Esso può essere applicato anche dopo la scadenza del termine. Per ragioni di trasparenza si segnala pertanto che è possibile che, nonostante siano venuti meno i motivi di cui all'articolo 26 capoverso 1 LPD*riv*, persistano quelli di cui al capoverso 2 LPD*riv*. Contrariamente all'analoga disposizione dell'articolo 8 capoverso 6 LSIP, le persone per le quali i dati non sono trattati possono essere informate immediatamente riguardo a tale circostanza. Le esperienze fatte con il diritto d'accesso indiretto suggeriscono che l'interesse di una persona a sapere rapidamente che non sono trattati dati che la riguardano è di gran lunga superiore al rischio teorico di un'indagine sul livello di conoscenza del SIC.

Capoverso 3

Il presente capoverso corrisponde in gran parte all'attuale articolo 63 capoverso 3. Ora, oltre al differimento, vengono disciplinati il possibile rifiuto e la limitazione dell'informazione. Si prevede inoltre che l'IFPDT verifichi anche se l'informazione di cui al capoverso 1 sia stata fornita in modo corretto, cosa che non è prevista per la disposizione analoga dell'articolo 8 capoverso 2 LSIP. La correttezza dell'informazione non può però essere verificata in altro modo dato che non è possibile presentare alcun reclamo.

Capoverso 4

Il presente capoverso corrisponde all'attuale articolo 64 capoverso 1 (con rinvio adeguato). Ciò è conforme al concetto della LPD*riv* secondo il quale l'IFPDT ha facoltà di aprire un'inchiesta quando riscontra irregolarità. Pure qui si tratta ora anche del rifiuto e della limitazione dell'informazione (cfr. la disposizione analoga nell'art. 8 cpv. 3 LSIP).

Capoverso 5

La LPDriv conferisce ora all'IFPDT la competenza di emanare decisioni. Le attuali raccomandazioni (cfr. il vigente art. 64 cpv. 2) vengono abolite (cfr. la disposizione analoga nell'art. 8 cpv. 4 LSIP). Anche il contenuto dell'attuale capoverso 4 è così divenuto obsoleto.

Capoverso 6

In linea con il disciplinamento LSIP (art. 8 cpv. 5) si stabilisce che la comunicazione di cui al capoverso 4 deve sempre avere lo stesso tenore e non viene motivata. Contrariamente alla LSIP è però previsto di portare il ricorso dinanzi al TAF.

Capoverso 7

L'attuale articolo 64 capoverso 5 deve essere adeguato nel senso che ora l'ncaricato federale della protezione dei dati può ordinare al SIC di fornire immediatamente alla persona interessata le informazioni richieste, se sono soddisfatti i presupposti in virtù della presente disposizione. Anche in questo caso si tratta del rifiuto e della limitazione dell'informazione. Per unificare la terminologia, anche nel presente capoverso il termine «pericolo» viene sostituito dal temine «minaccia». La presente disposizione corrisponde all'attuale articolo 8 capoverso 7 LSIP.

Capoverso 8

Onde evitare procedure parallele, le informazioni di cui ai capoversi 1 e 2 e le comunicazioni di cui ai capoversi 3 e 4 non sono impugnabili.

[24] RS **361**

Articolo 64

Ovviamente il SIC può fornire informazioni soltanto su quei settori del PES in cui esso stesso o le autorità d'esecuzione cantonali trattano dati. Se il PES contiene dati personali di altre autorità, il SIC inoltra loro, affinché le trattino, le richieste di informazioni dei richiedenti.

Articolo 65

Capoverso 1

La presente disposizione corrisponde all'articolo 66 capoverso 1. È stato adeguato solo il rinvio alla verifica.

Capoverso 2

Il presente capoverso corrisponde all'articolo 66 capoverso 2. Poiché l'IFPDT non emana più raccomandazioni, sono state stralciate le pertinenti considerazioni.

Sezione 3: Archiviazione

Con la nuova struttura, l'attuale sezione 5 del capitolo 4 diventa la sezione 3.

Articolo 68

Il presente articolo corrisponde in gran parte all'attuale articolo 68.

Capoverso 1

Nella LAIn, e di conseguenza nelle ordinanze di esecuzione, si distingue tra «cancellare» ed «eliminare». Il SIC offre all'AFS, per l'archiviazione, i dati destinati a essere cancellati. I dati privi di valore archivistico e quelli già consegnati all'AFS vengono distrutti. Il capoverso 1 riguarda l'archiviazione dei dati di cui il SIC non necessita più costantemente. Per tale motivo in questa fase si tratta della «cancellazione» e non della «distruzione» di dati. Ora si chiarisce altresì che anche l'autorità di vigilanza indipendente mette a disposizione dell'AFS, affinché li archivi, i dati di cui non necessita più costantemente e destinati a essere cancellati, che tali dati sono custoditi in locali particolarmente protetti e che per essi si applica il termine di protezione prolungato. I dati dell'autorità di vigilanza indipendente provengono in gran parte dal SIC e dalle autorità d'esecuzione cantonali, motivo per cui l'interesse al mantenimento del segreto è altrettanto importante.

Capoverso 4

Qui si chiarisce che il SIC distrugge, subito dopo averli cancellati, i dati che l'AFS considera privi di valore archivistico, anche se il loro termine di protezione non è ancora scaduto. Lo stesso vale per l'autorità di vigilanza indipendente. La distruzione viene verbalizzata secondo l'ordinanza.

Articolo 70

Capoverso 1 lettera d

La lettera d dell'attuale articolo 70 capoverso 1 va abrogata per evitare doppioni. La condotta politica del SIC è sufficientemente coperta dalle altre disposizioni dell'articolo. Oggi non è più necessaria un'ulteriore valutazione annuale della situazione in materia di politica di sicurezza, tanto più che il Consiglio federale, con i rapporti sulla politica di sicurezza pubblicati ora ogni quattro anni fornisce informazioni molto più complete su detta valutazione. Il rapporto di politica di sicurezza e informativo del DDPS alle commissioni parlamentari competenti non è interessato dall'abrogazione (art. 80). Viene portato avanti secondo le esigenze del Parlamento.

Con l'abrogazione si elimina anche una certa contraddizione con il capoverso 2, in base alla quale i documenti in relazione con i compiti di cui al capoverso 1 non sono accessibili al pubblico. Il rapporto sulla situazione del SIC pubblicato annualmente, che presenta i principali sviluppi della situazione dal punto di vista informativo, mette in ogni caso al corrente il pubblico in merito alla valutazione della situazione.

Capoverso 3

La disposizione già esistente sull'autorizzazione del Consiglio federale a concludere autonomamente trattati internazionali nel settore informativo deve essere ampliata in termini di contenuto e, conformemente alla prassi internazionale, precisata nel senso che tali trattati possono essere tenuti segreti se devono essere classificati «segreto» secondo l'articolo 13 capoverso 3 LSIn. Attualmente c'è una tendenza verso una certa formalizzazione della collaborazione internazionale in materia di attività informative. Per contro, nel prossimo futuro, difficilmente un altro Paese sarà disposto a stipulare trattati resi pubblici in questo settore.

Nella nuova LSIn è prevista l'autorizzazione generale del Consiglio federale per la conclusione di trattati internazionali nel campo della sicurezza delle informazioni. Al fine di evitare confusioni, nella LAIn questa competenza continua a essere menzionata assieme ad altri settori nei quali il Governo può concludere autonomamente trattati internazionali sulla collaborazione internazionale in materia di attività informative.

Il Consiglio federale riferisce ogni anno all'Assemblea federale sui trattati conclusi da esso stesso. Soltanto la DelCG viene per contro informata dei trattati confidenziali o segreti (art. 48*a* cpv. 2 LOGA). Inoltre, gli organi di vigilanza informativa AVI-AIn e DelCG, fondandosi anche sui loro diritti di vigilanza, continueranno ovviamente ad avere il pieno diritto d'accesso a tali documenti. Sono così garantiti il controllo e la vigilanza.

Articolo 74 (v. commento all'art. 83*a* per la numerazione dei capoversi)

I capoversi abrogati qui vengono integrati nella nuova sezione riguardante le disposizioni penali, inserita prima delle disposizioni finali. In tal modo le prime vengono disciplinate, come di consueto, alla fine del testo di legge.

Sezione 2: Controllo e vigilanza del SIC

Nel corso dei dibattiti parlamentari, le commissioni competenti e il Consiglio federale hanno convenuto, in un primo tempo, di sviluppare l'AVI-AIn, istituita con la LAIn, e consentire all'ACI, esistente, di continuare a esercitare i propri controlli e di estenderli all'esplorazione di segnali via cavo. Oggi queste due autorità collaborano e coordinano le loro attività per evitare lacune nella vigilanza. L'obiettivo era di mantenere e persino rafforzare la vigilanza. In un secondo tempo si dovrebbe verificare una fusione delle due autorità con trasferimento delle conoscenze. Tra l'altro, verrebbe meno il coordinamento delle attività e l'alta vigilanza parlamentare e il SIC avrebbero soltanto più un interlocutore, che però esercita lo stesso controllo. L'indipendenza dell'autorità di vigilanza rimarrebbe garantita.

Dopo avere ponderato i vantaggi e gli svantaggi, i compiti dell'ACI vanno ora delegati all'AVI-AIn, che dispone già di ampie competenze in materia di vigilanza e verifica la legalità, l'adeguatezza e l'efficacia delle attività informative del SIC, delle autorità d'esecuzione cantonali e dei terzi incaricati dal SIC.

L'ACI verifica nello specifico la legalità dell'esplorazione radio e vigila sull'esecuzione dei mandati di esplorazione dei segnali via cavo che hanno ottenuto l'autorizzazione e il nullaosta. Per adempiere la propria attività di sorveglianza, entrambe le autorità hanno accesso a tutte le informazioni e a tutti i documenti utili nonché a tutti i locali dei servizi sottoposti a vigilanza e possono emanare raccomandazioni. Le due autorità lavorano periodicamente insieme.

Dato che le competenze di vigilanza dell'AVI-AIn coprono sostanzialmente anche quelle dell'ACI, attualmente ü sensato riunire le attività di vigilanza di questi due servizi indipendenti in un'unica autorità, che dispone già di un'ampia panoramica sulle attività informative. In tal modo è possibile garantire che la verifica dell'esplorazione radio e dell'esplorazione di segnali via cavo rimanga efficace e completa. Pertanto l'attuale articolo 79 LAIn decade e viene abrogato.

Inoltre, il più ampio mandato di sorveglianza dell'AVI-AIn garantisce anche una più ampia vigilanza che non si estende soltanto alla legalità delle attività informative, ma anche alla loro adeguatezza ed efficacia. E infine, la delega dei compiti consente anche di creare sinergie: l'AVI-AIn si occupa in via esclusiva della verifica delle attività informative. I membri dell'ACI lavorano invece secondo un sistema di miliziaI rapidi sviluppi tecnologici e le complesse questioni che ne risultano per i processi nelle operazioni quotidiane, rendono sempre più difficile per questa autorità mantenere, senza un onere sproporzionato, il livello di conoscenze necessario per le verifiche. In ragione degli altri compiti che deve adempiere, l'AVI-AIn, è comunque tenuta ad acquisire tali conoscenze. Già oggi annovera i pertinenti specialisti nell'effettivo del suo personale. Grazie alle sinergie esistenti, la qualità della vigilanza può continuare a essere garantita e adeguata agli sviluppi senza un onere sproporzionato. Venendo meno un'autorità di vigilanza, si riduce l'onere di coordinamento senza che i risultati delle verifiche perdano in qualità. Concentrando le forze (di vigilanza), ha luogo un controllo completo unificato. Con il trasferimento dei compiti e delle conoscenze dall'ACI all'AVI-AIn è inoltre possibile realizzare la soluzione presa in considerazione dal Parlamento nel 2015 nell'ambito del dibattito sulla LAIn.

La revisione della LAIn è anche un'opportunità per rendere più leggibile la legge semplificando la struttura. Per tale motivo si propone di suddividere l'articolo 78 in quattro disposizioni distinte, tenendo conto dei diversi compiti che l'AVI-AIn deve adempiere ai sensi della legge, vale a dire la vigilanza, il coordinamento nonché l'informazione al pubblico. Sempre ai fini di una migliore leggibilità e poiché il DDPS è anche responsabile dell'attuazione delle raccomandazioni dell'AVI-AIn, questo punto è ora oggetto di una propria disposizione.

Articolo 75

La LAIn utilizza altrimenti il termine «autorità d'esecuzione cantonali», che viene corretto in questo articolo.

Articolo 77 capoverso 2

Poiché, in linea di principio, a tal fine è necessaria una base legale formale, la procedura di presentazione, tramite il DDPS, del progetto di preventivo annuale dell'AVI-AIn al Consiglio federale e la sua trasmissione immutata all'Assemblea federale, finora disciplinate soltanto nell'articolo 4 dell'Ordinanza del 16 agosto 2017[25] concernente la vigilanza sulle attività informative (OVAIn), vengono ora integrate nell'articolo 77 capoverso 2 LAIn.

Articolo 78

La presente disposizione riproduce, invariati, i capoversi 1 e 4 dell'attuale articolo 78 (nuovi cpv. 1 e 2) e si concentra così sull'attività di vigilanza dell'autorità di vigilanza indipendente in senso stretto. Al fine di garantire l'adempimento dei propri compiti, in particolare nella vigilanza sull'esplorazione di segnali via cavo, nel nuovo capoverso 4 si precisa che l'AVI-AIn può esigere la collaborazione dei fornitori di servizi postali e di telecomunicazione e l'accesso ai loro locali.

I termini inerenti alla conservazione dei dati nel capoverso 3, che riprende l'attuale capoverso 5, sono adattati al nuovo concetto di conservazione dei dati e alla LPD*riv*. Ciò non comporta modifiche materiali.

25 RS **121.3**

Articolo 78a

La presente disposizione comprende i capoversi 6 e 7 dell'attuale articolo 78. Essa si concentra sulla forma del risultato delle verifiche effettuate dall'autorità di vigilanza e sul destinatario dei rapporti allestiti da quest'ultima e fissa la competenza per l'attuazione delle raccomandazioni formulate.

La DelCG ha chiesto chiarimenti in merito alle attività dell'AVI-AIn nell'ambito della vigilanza sulle autorità d'esecuzione cantonali e sulle eventuali raccomandazioni dell'AVI-AIn, motivo per cui la legge viene precisata. Mentre dall'articolo 78 capoverso 1 LAIn emerge chiaramente che l'attività di vigilanza dell'AVI-AIn si estende anche alle attività delle autorità d'esecuzione cantonali, la questione delle raccomandazioni dell'AVI-AIn rivolte a dette autorità finora è disciplinata soltanto parzialmente nell'OVAIn (art. 13 cpv. 1). Il nuovo articolo 78*a* corregge questa mancanza di univocità e nel capoverso 1 precisa che l'AVI-AIn può formulare raccomandazioni destinate a tutti i servizi su cui vigila secondo l'articolo 78 capoverso 1 LAIn. Grazie a questa precisazione è dunque chiaro che le raccomandazioni dell'AVI-AIn possono ora essere rivolte a un servizio o a più servizi se esse riguardano la collaborazione tra vari servizi. Inoltre, anche l'informazione agli organi di vigilanza cantonale viene elevata dal livello di ordinanza a quello di legge.

Indipendentemente dall'organo a cui si rivolgono, l'attuazione delle raccomandazioni dell'AVI-AIn è di competenza del DDPS o del servizio cantonale responsabile, come previsto dal nuovo articolo 78*a*, che riprende l'attuale articolo 78 capoverso 1 LAIn. Con riferimento alle raccomandazioni che sono di competenza cantonale, il nuovo capoverso 4 introduce una nuova procedura per la loro validazione ed eventualmente per il loro rifiuto da parte delle autorità cantonali. In tal modo la competenza decisionale nei Cantoni viene disciplinata in maniera analoga a quella a livello di Confederazione (cfr. capoverso 2) e viene tenuto conto di una richiesta della DelCG.

Articolo 78b

Riguardo al coordinamento interno dell'autorità di vigilanza indipendente, il capoverso 2 dell'attuale articolo 78 viene ripreso in un articolo separato.

Articolo 78c

I principi del coordinamento della vigilanza sui servizi informazioni con autorità estere vengono ora disciplinati nella legge. I dettagli di tale coordinamento internazionale vengono stabiliti nell'OVAIn. I motivi di tale adeguamento sono i seguenti.

Con l'intensificarsi della collaborazione transfrontaliera dei servizi informazioni e dello sviluppo tecnologico è aumentata anche la comunicazione reciproca di informazioni, in particolare di dati personali. Questo scambio di informazioni e di dati con servizi informazioni esteri, che può svolgersi in vario modo, oralmente o per scritto, è parte del lavoro quotidiano del SIC. La costante internazionalizzazione delle attività informative accresce anche l'importanza della cooperazione internazionale tra le autorità di vigilanza. Spesso tale cooperazione è il presupposto per un'efficace vigilanza sui servizi informazioni operanti a livello internazionale. Per tale motivo anche l'AVI-AIn deve avere la possibilità di scambiare informazioni ed esperienze con le sue autorità partner estere, così come possono farlo altre autorità di vigilanza svizzere (ad es. Autorità federale di vigilanza sui mercati finanziari [FINMA], IFPDT).

Il coordinamento internazionale con i partner stranieri svolge un ruolo importante anche nella formazione informativa dei membri dell'AVI-AIn. Lo sviluppo delle conoscenze di quest'ultima e dei suoi membri non può basarsi unicamente sulle informazioni fornite dalle autorità sottoposte a vigilanza.

Articolo 78d

L'articolo 78*d* riprende il testo dell'attuale articolo 78 capoverso 3.

Articolo 80

Come conseguenza della possibilità di assegnare un'identità fittizia anche a collaboratori di servizi svizzeri (v. art. 18), viene ampliata l'informazione al Consiglio federale e alla DelCG in merito allo scopo e al numero delle identità fittizie. Su richiesta della DelCG inoltre occorrerà chiarire che il rapporto informa anche in merito all'attribuzione di identità fittizie a fonti umane.

La LAIn utilizza il termine «autorità d'esecuzione cantonali», che viene unificato nel *capoverso 4*.

Articolo 83

Per gli stessi motivi addotti per altre decisioni, anche per quelle emanate in relazione con esplorazioni di segnali via cavo va tolto l'effetto sospensivo. Non si può attendere l'esito di una procedura di reclamo, altrimenti le informazioni fornite a posteriori potrebbero essere già obsolete e non più utilizzabili o i dati neanche più disponibili qualora i termini di conservazione legali siano già scaduti.

Capitolo 6a: Disposizioni penali, giurisdizione e comunicazione

Con questo nuovo capitolo, tutte le disposizioni penali vengono disciplinate, come di consueto, verso la fine del testo di legge.

Articoli 83a e 83b

L'articolo 83*a* riprende i capoversi 4, 4bis e 5, abrogati, dell'articolo 74. Il testo corrisponde alla versione approvata dal Parlamento il 25 settembre 2020 in relazione con la trasposizione nel diritto svizzero della Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, entrata in vigore per il nostro Paese il 1°luglio 2021.

Per la motivazione dell'introduzione della disposizione penale per il divieto di determinate attività, si veda il commento all'articolo 83*c*.

Poiché i divieti di determinate attività e di organizzazioni vengono emanati dal Consiglio federale, le relative disposizioni penali seguono norme differenti per il perseguimento penale che le altre infrazioni dell'articolo 83*c*.

Articolo 83c capoversi 1 e 2

Finora la LAIn non ha previsto sanzioni di esecuzione o penali speciali (ad es. disposizioni penali) nel caso in cui le persone interessate si oppongano a una richiesta di informazioni da parte del SIC, ad esempio ai sensi dell'articolo 25 capoverso 1 LAIn. Finalizzati a imporre il rispetto degli obblighi di legge da parte di chi viene meno agli obblighi che gli incombono, i mezzi coattivi amministrativi devono essere materialmente connessi con gli obblighi giuridici di cui si intende assicurare l'osservanza. Vi sono due categorie di mezzi coattivi: quelli di esecuzione e quelli repressivi. Il SIC dispone quindi al momento soltanto degli strumenti previsti nel diritto procedurale (art. 40 seg. della legge federale del 20 dicembre 1968[26] sulla procedura amministrativa) per imporre un ordine ai sensi dell'articolo 25 LAIn. L'unica possibilità è di minacciare l'interessato di una multa per disobbedienza ai sensi dell'articolo 292 del codice penale[27] (CP). Secondo l'articolo 106 capoverso 1 CP, il massimo di una multa di quel tipo è di 10 000 franchi. Se non si rispetta la decisione, il SIC può presentare al pubblico ministero cantonale competente una denuncia per disobbedienza a una decisione dell'autorità.

Il SIC può emanare ordini in relazione a obblighi di informazione dei privati (art. 25). Anche nel settore dell'esplorazione di segnali via cavo il servizio addetto all'esplorazione può emanare decisioni nei confronti di un gestore di reti filari o di un fornitore di servizi di telecomunicazione per richiedere dati (art. 43). In conformità con l'articolo 26 OAIn, il servizio preposto all'esecuzione è il COE, che fa parte dell'attuale BAC.

Qualora si violino gli obblighi previsti dalla presente legge e si ostacoli l'adempimento dei compiti legali della LAIn, una nuova disposizione dovrebbe consentire di punire i responsabili. La disposizione è riprodotta sulla base della disposizione penale nella legge federale del 18 marzo 2016[28] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT, art. 39) e ne riprende anche la multa. Il suo importo si giustifica anche dal fatto che una multa deve produrre un effetto punitivo adeguato. Proprio nel settore dell'esplorazione di segnali via cavo, una multa di appena diecimila franchi al massimo potrebbe non conseguire l'effetto sperato presso le persone responsabili di molti fornitori di telecomunicazione. Come per la pena secondo l'articolo 39 LSCPT, la pena prevista dal presente articolo deve aggiungersi soltanto in via sussidiaria a disposizioni penali più severe, che al contempo potrebbero essere rispettate ai sensi di altre leggi. A tale proposito, si pensi in particolare alla violazione di obblighi di segretezza (ed eventualmente al favoreggiamento) che sono oggetto di un disciplinamento dettagliato anche nel CP. È ipotizzabile anche la falsità in documenti secondo l'articolo 251 CP.

Se nell'esplorazione di segnali via cavo un gestore di reti filari o un fornitore di servizi di telecomunicazione non fornisce i dati richiesti dal servizio addetto all'esplorazione, le persone responsabili sono punibili. È ipotizzabile che lo stesso gestore di reti filari debba fornire dati per varie esplorazioni di segnali via cavo individuali. Qualora esso non ottemperi il proprio obbligo in varie esplorazioni, le persone responsabili sono punibili ripetutamente. In caso di recidiva è possibile aumentare la multa.

La violazione dell'obbligo di mantenere il segreto nei confronti di terzi di cui all'articolo 19 capoverso 3 e all'articolo 20 capoverso 2 equivale a una violazione del segreto d'ufficio di cui all'articolo 320 CP. Ecco perché la LAIn non contiene alcuna disposizione penale particolare a tale riguardo, ma soltanto una disposizione penale rivolta ai privati. Finora i privati non erano punibili per una violazione dell'obbligo di mantenere il segreto nei confronti di terzi.

Con il nuovo capoverso 2 si crea la possibilità, per i casi d'importanza esigua, di condannare la persona giuridica a pagare una multa in caso di violazione degli obblighi da parte di una persona che lavora nell'impresa. In tal modo l'autorità può evitare un onere d'inchiesta sproporzionato.

Articolo 83d

Capoverso 1

In base ai principi del diritto penale amministrativo, la presente disposizione consente al SIC e al servizio addetto all'esplorazione di procedere, in caso di esplorazioni di segnali via cavo, contro persone che non ottemperano agli obblighi stabiliti nei loro confronti. Lo stesso vale per la violazione dell'obbligo di mantenere il segreto. Nell'ambito di esplorazioni di segnali via cavo, il servizio addetto all'esplorazione emana ordini, motivo per cui anch'esso figura nel presente capoverso.

Capoverso 2

Il presente capoverso riprende il capoverso 6, abrogato, dell'articolo 74 ed è integrato dal perseguimento e dal giudizio della violazione del divieto di determinate attività.

Articolo 83e

In termini di contenuto il presente articolo riprende il capoverso 6, abrogato, dell'articolo 74. Concerne la violazione del divieto di organizzazioni nonché del divieto di determinate attività. L'iperonimo «decisioni» contempla tutti i generi di decisioni quali sentenze, decreti d'accusa, decisioni penali, decreti penali, decisioni di non doversi procedere e dichiarazioni di non doversi procedere.

26 RS **172.021**
27 RS **311.0**
28 RS **780.1**

Articolo 85 capoverso 2

Il presente capoverso può essere abrogato, dato che il suo contenuto normativo è stato ripreso nel nuovo articolo 9 capoverso 3.

Allegato

Osservazioni generali riguardanti i numeri 1 e 6

Le modifiche nella LMSI e nella LSIP tengono conto dell'attuazione della mozione Rieder 17.3862 «Divieto di espatrio nei confronti di potenziali estremisti violenti».

Legge federale del 21 marzo 1997[29] sulle misure per la salvaguardia della sicurezza interna

Articolo 2

Il capoverso 2 lettera f integra le misure preventive di polizia esistenti con quelle contro le attività di estremismo violento di cui all'articolo 24*h* segg. Se il divieto di recarsi in un Paese determinato si riferisce soltanto a eventi all'estero, è tuttavia presumibile che questa misura preventiva contribuirà a rafforzare la sicurezza interna della Svizzera. Questo perché i gruppi svizzeri che vogliono partecipare a disordini all'estero vengono indeboliti nelle loro azioni e nei loro obiettivi in generale. I divieti li priveranno di un palcoscenico sul quale poter esprimere le proprie proposte ricorrendo a un'estrema violenza. Per tale motivo i divieti di recarsi in un Paese determinato per gli estremisti gli estremisti violenti figurano nell'elenco delle misure per la salvaguardia della sicurezza interna.

Titolo intermedio sezione 5b: Misure contro atti violenti in occasione di dimostrazioni o manifestazioni

Per le nuove misure contro la violenza in occasione di dimostrazioni o manifestazioni sono necessari un titolo intermedio e una sezione supplementari. Quest'ultima viene inserita dopo la sezione 5*a* (Misure contro la violenza in occasione di manifestazioni sportive).

Articolo 24h Divieto di recarsi in un Paese determinato

Il *capoverso 1* sancisce che fedpol, in quanto autorità di polizia della Confederazione, è responsabile di pronunciare divieti di recarsi in un Paese determinato nei confronti di estremisti potenzialmente violenti. Il capoverso definisce i presupposti ai quali può essere pronunciato un tale divieto.

Secondo la *lettera a* la persona in questione deve aver esercitato violenza già in passato in occasione di una dimostrazione o manifestazione in Svizzera o all'estero. Per «dimostrazioni» e «manifestazioni» si intendono eventi con un contenuto ideologico e una funzione d'appello e sostenuti da più persone. Se uno dei gruppi che desidera esprimere una proposta politica rimane nel medesimo luogo, si tratta di una manifestazione. Le dimostrazioni sono caratterizzate dal fatto di avere un luogo di raduno, un corteo e un luogo di comizio conclusivo. I partecipanti devono quindi spostarsi dal primo al secondo luogo.

La prova di un comportamento violento in occasione di un evento passato è solitamente una sentenza o un decreto d'accusa emesso da un tribunale o un pubblico ministero in cui si constata che una persona ha commesso reati contro persone o oggetti. Gli atti di violenza contro persone o oggetti possono soddisfare varie fattispecie di reato. Per concretizzare tale criterio, nell'ordinanza viene inserito un elenco non esaustivo di possibili reati. L'elenco si rifarà alle disposizioni dell'ordinanza del 4 dicembre 2009[30] sulle misure di polizia amministrativa dell'Ufficio federale di polizia e sul sistema d'informazione HOOGAN (OMPAH) nella lotta contro la tifoseria violenta. In occasione di dimostrazioni e manifestazioni, infatti, dagli estremisti violenti parte una minaccia affine a quella dei tifosi violenti in occasione di manifestazioni sportive. Poiché si registrano anche episodi di violenza all'estero, possono fungere da prova anche sentenze straniere.

Se si impugna una sentenza o un decreto d'accusa, in pratica possono passare fino a cinque anni prima che una persona venga condannata con decisione passata in giudicato per un atto di violenza commesso in occasione di una dimostrazione o di una manifestazione. Attendere anni per un divieto di recarsi in un Paese determinato andrebbe però contro gli obiettivi preventivi della misura: le persone che partecipano ripetutamente a disordini violenti durante un evento di solito lo fanno per un periodo di tempo limitato. L'esperienza insegna che questa «fase acuta» del ricorso alla violenza dura un paio d'anni. Se tali persone vengono condannate in prima istanza e impugnano la decisione, possono volerci anni prima che sia pronunciata una condanna definitiva. Ma questo periodo è decisivo per l'evoluzione del comportamento violento. La misura dovrebbe pertanto applicarsi proprio in tale periodo.

Deve perciò essere possibile provare, in via eccezionale anche in modo diverso che con una sentenza, un comportamento violento avuto in passato in occasione di una dimostrazione o una manifestazione. Nel *capoverso 2* viene fornito un elenco esemplificativo di tali prove della polizia. L'elenco si rifà alle prove relative ai divieti limitati di lasciare la Svizzera pronunciati nei confronti dei tifosi violenti (art. 5 OMPAH).

In virtù delle sue competenze, la polizia è a conoscenza di persone e ambienti che notoriamente si manifestano in modo violento durante dimostrazioni e manifestazioni. Le prove di un comportamento violento si basano pertanto anche sulle attività di polizia. Per denunce a seguito di accertamenti della polizia si intendono quelle fatte dalla polizia stessa e non sono quindi incluse quelle dei privati. È prassi abituale che le persone che ricorrono alla violenza in occasione di dimostrazioni e manifestazioni, e che possono dunque essere arrestate

29 RS **120**
30 RS **120.52**

dalla polizia, ricevano una decisione di allontanamento e una decisione di tenuta a distanza per tutta la durata dell'evento. Siffatte decisioni possono anche servire da prova.

Il divieto di recarsi in un Paese determinato è uno strumento di polizia preventivo. L'obiettivo della misura è di impedire che un rischio concreto che si situa in futuro si trasformi in un danno a persone o oggetti. Dato il carattere preventivo del divieto occorre operare sulla base di previsioni che devono poggiare su criteri oggettivi ed essere sufficientemente verificabili per soddisfare i requisiti dello Stato di diritto. Cumulativamente al capoverso 1 lettera a ci devono perciò essere indizi in virtù dei quali si deve presumere che l'interessato intenda partecipare a disordini violenti in occasione di dimostrazioni e manifestazioni (lett. b).

La dimostrazione o manifestazione di cui alla lettera b deve avere carattere internazionale. In tal modo si coprono gli eventi di una certa importanza sotto il profilo della politica economica o sociale, quali i vertici del G7 / G20, visite di Stato ad alto livello, conferenze, convegni di partito o dimostrazioni di cerchie estremiste, interconnesse al di fuori dei confini nazionali. Il campo di applicazione comprende però anche eventi minori che sorgono a margine di siffatti grandi eventi, in particolare contromanifestazioni. In tali occasioni la polizia si trova sistematicamente confrontata a gravi disordini. Così, ad esempio, al vertice del G20 tenutosi ad Amburgo nel 2017 si sono avute varie condanne contro cittadini svizzeri per atti di violenza; nel 2016 un nostro connazionale è stato condannato a sette anni di detenzione in Francia per l'uso di estrema violenza fatto durante una dimostrazione. Con un divieto di recarsi in un Paese determinato si potrebbe impedire la partecipazione di persone provenienti dalla Svizzera e quindi anche il danno a persone e oggetti.

Di norma, il luogo e la data degli eventi di cui al capoverso 1 lettera b (molto importanti sotto il profilo della politica economica o sociale) sono noti con largo anticipo. Dimostrazioni e manifestazioni a margine di tali eventi, a favore o contro le proposte dell'evento principale, possono però anche insorgere spontaneamente. La probabilità che vi possa essere violenza durante questi eventi si valuta in base a informazioni di polizia e a valori empirici.

Vi sono ad esempio indizi concreti e attuali che suggeriscono l'intenzione di lasciare la Svizzera per recarsi a una dimostrazione o manifestazione e farvi uso di violenza, se la persona in questione ha dichiarato piani di viaggio concreti per partecipare a una dimostrazione o manifestazione all'estero, in cui con ogni probabilità vi è da attendersi notevole violenza contro oggetti o persone. L'autorità richiedente di cui all'articolo 24*i* deve motivare a sufficienza nei confronti di fedpol suddetti indizi.

Le persone che entrano in linea di conto per una misura di cui all'articolo 24*h* di norma sono note alla polizia e/o al SIC a causa dei loro precedenti. Fondandosi su valori empirici registrati sinora è presumibile che i divieti di recarsi in un Paese determinato si applichino soltanto a una cerchia assai ristretta di persone (numero basso in doppia cifra) e a un numero gestibile di eventi.

Lo strumento preventivo del divieto di recarsi in un Paese determinato è strutturato in modo proporzionato: per poter pronunciare un divieto di recarsi in un Paese determinato devono esserci fatti concreti e attuali che rendano abbastanza probabile che la persona intende effettivamente recarsi alla dimostrazione o manifestazione. L'onere della prova secondo la lettera b rappresenta un grosso ostacolo per le autorità. A ciò si aggiunge il fatto che la persona in questione già in passato deve essersi fatta notare per il suo comportamento violento e che deve esserci una prova in tal senso. Gli ostacoli cumulativi delle lettere a e b sono necessari per rispettare il principio della proporzionalità dell'attività dello Stato. Se tutti questi presupposti sono soddisfatti caso per caso, il divieto di recarsi in un Paese determinato è pronunciato per un breve periodo e un'area geografica limitata (cfr. art. 24*h* cpv. 2). Il principio della proporzionalità è peraltro rispettato anche nel senso che per motivi importanti si possono autorizzare eccezioni al divieto (cpv. 3).

Se si impedisce alle persone di partecipare a eventi politici di norma si tocca il loro diritto a esprimere liberamente le proprie opinioni. Questo disciplinamento è tuttavia applicabile soltanto a persone che molto probabilmente prenderanno parte ad atti di violenza. Esprimere la propria opinione mediante violenza contro altre persone o oggetti non rientra nel campo di applicazione del suddetto diritto e non è quindi tutelato.[31] Il previsto divieto di recarsi in un Paese determinato non pregiudica quindi il diritto fondamentale della libertà di esprimere opinioni, al contrario. Spesso gli estremisti violenti sfruttano gli eventi di cui al capoverso 1 quali fruitori abusivi e impediscono ad altri partecipanti pacifici di esprimere la propria opinione. Succede anche che, contro la volontà degli organizzatori dell'evento, estremisti violenti assumano il comando di manifestazioni pacifiche e ne abusino per i propri scopi, ossia commettere violenza o incitare alla violenza.

Per una violazione del divieto di recarsi in un Paese determinato viene comminata una multa (disobbedienza a decisioni dell'autorità ai sensi dell'articolo 292 CP). La legge non prevede ulteriori sanzioni per tale violazione.

Il *capoverso 3* prevede che non è soltanto vietato recarsi direttamente in un Paese determinato, ma anche recarsi in altri Paesi per eludere il divieto. L'obiettivo è di evitare che le persone interessate partecipino comunque alla manifestazione passando per rotte di viaggio alternative. Il divieto di recarsi in un Paese determinato include quindi il fatto di recarsi in determinati Paesi terzi al fine di impedire il viaggio verso il Paese determinato passando per un Paese terzo. Sono ammesse eccezioni al divieto se la persona interessata fa valere in modo credibile motivi importanti. Tali eccezioni possono essere un matrimonio o un funerale. In merito all'autorizzazione dell'eccezione decide fedpol nell'ambito di una ponderazione degli interessi.

Il *capoverso 4* specifica che il divieto di recarsi in un Paese determinato è segnalato nel sistema di ricerca informatizzato di polizia secondo l'articolo 15 LSIP (RIPOL), così che le autorità aventi accesso a RIPOL siano informate e possano attuare il divieto. Il sistema di ricerca RIPOL viene periodicamente consultato dai corpi delle guardie di confine. Essi ricevono anche una comunicazione e sono pertanto sensibilizzati in merito al periodo in questione. Inoltre fedpol informa le competenti autorità di polizia all'estero in modo che possano reagire al divieto, ad esempio con una restrizione d'entrata. La parte nazionale del Sistema d'informazione di Schengen (N-SIS; art. 16 LSIP) non prevede una categoria di segnalazione per i divieti di recarsi in un Paese determinato per estremisti violenti e pertanto le informazioni non possono essere fornite attraverso il canale SIS. La comunicazione dei dati ad autorità nazionali ed estere è retta dall'articolo 24*l* capoverso 3 in combinato disposto con l'articolo 24*h* capoverso 4.

[31] DTF 143 I 147 consid. 3.2

Le esperienze fatte con i tifosi violenti mostrano che i divieti di recarsi in un Paese determinato hanno un effetto preventivo: la persona nei confronti della quale è stato ordinato un tale divieto solitamente desiste dal recarvisi nell'ottica della pena di cui è passibile.

Articolo 24i Richiesta

Analogamente alle misure per la lotta al terrorismo, anche le misure contro estremisti potenzialmente violenti di norma vengono disposte su richiesta del SIC e delle autorità cantonali. Il diritto di presentare richiesta spetta quindi in primo luogo alle autorità che già dispongono di informazioni sulle persone interessate (risultanze derivanti dalla situazione di minaccia inerente alla sicurezza interna ed esterna e risultanze derivanti dal perseguimento penale di reati di matrice estremista-violenta). Non si può però escludere che fedpol agisca di propria iniziativa. Se i Cantoni hanno delegato compiti di sicurezza ai Comuni, anch'essi possono richiedere direttamente misure a fedpol.

La richiesta a fedpol da parte del SIC o della competente autorità cantonale o comunale dev'essere sufficientemente motivata. Fedpol accerta i fatti e verifica se vi sono i presupposti per il divieto di recarsi in un Paese determinato di cui agli articoli 24*h* e 24*k*. Se, ad esempio, il SIC ha indizi concreti che una persona vuole recarsi a una contromanifestazione a una conferenza internazionale in Germania e che tale persona è già stata condannata, in occasione di una dimostrazione o manifestazione, per sommossa ai sensi dell'articolo 260 CP in combinazione con lesioni gravi ai sensi dell'articolo 122 CP, il SIC richiede a fedpol il divieto di recarsi in un Paese determinato di cui all'articolo 24*h*. Fedpol verificherà se sono soddisfatti tutti i presupposti di cui all'articolo 24*h* e, sempreché lo siano, pronuncerà il divieto.

Articolo 24j Durata del divieto di recarsi in un Paese determinato

La restrizione della libertà di movimento può perdurare soltanto per il tempo strettamente necessario a impedire che la persona interessata partecipi ad atti di violenza. Il divieto di recarsi in un Paese determinato può perciò essere pronunciato per un periodo massimo di tre giorni prima dell'evento fino all'ultimo giorno dello stesso. In tal modo si garantisce che il divieto si applichi soltanto per una durata proporzionata.

Articolo 24k Limite di età

I divieti di recarsi in un Paese determinato per contrastare attività di estremismo violento possono essere pronunciati nei confronti di persone che hanno compiuto i 15 anni. Il limite di età basso tiene conto del fatto che anche i minori sono molto inclini alla violenza e sottolinea il carattere preventivo della misura: la prassi della polizia mostra che diverse persone molto giovani sono strumentalizzate per i propri fini da gruppi di estremisti violenti. Nel 2018, ad esempio, 40 minorenni hanno partecipato a una manifestazione non autorizzata in Svizzera. Persone incappucciate hanno causato un danno materiale di circa 100 000 franchi. Un totale di 147 persone, di cui 21 minorenni, sono state denunciate per vari reati (tra cui sommossa, disobbedienza a decisioni dell'autorità, impedimento di atti dell'autorità, violenza o minaccia contro le autorità e i funzionari, infrazione alla legge federale sugli esplosivi, danneggiamento). Al momento del fermo, la persona più giovane aveva 13 anni. Un divieto di recarsi in un Paese determinato ha quindi anche una funzione protettiva per i giovani, nel senso che sono confrontati a un ordine delle autorità che li dissuade dal partecipare ad attività violente organizzate.

Articolo 24l Trattamento e comunicazione dei dati

Capoverso 1 e capoverso 2: l'autorità che richiede un divieto di recarsi in un Paese determinato e l'autorità che lo pronuncia è tenuta a trattare dati personali degni di particolare protezione per motivarlo, per motivarne l'ordine (art. 24*h*), per verificare se sono adempiuti i presupposti per l'ordine nonché per eseguire il divieto. Queste disposizioni creano la base legale formale necessaria ai sensi dell'articolo 17 capoverso 2 dell'attuale LPD.

Il *capoverso 3* stabilisce che i collaboratori dell'Ufficio federale delle dogane e della sicurezza dei confini (UDSC) impiegati per il controllo delle persone possono trattare i relativi dati personali, inclusi quelli degni di particolare protezione, inerenti al divieto di recarsi in un Paese determinato, ai fini dell'applicazione del divieto.

Il *capoverso 4* consente lo scambio di dati personali tra le autorità che dispongono di informazioni necessarie per la decisione di fedpol e quelle che adempiono compiti nell'ambito della lotta contro attività di estremismo violento. Il migliore flusso di informazioni tra le autorità è richiesto dal Piano d'azione nazionale per prevenire e combattere la radicalizzazione e l'estremismo violento[32] (PAN; v. misura 15 lettera a)

Il *capoverso 5* disciplina la comunicazione dei dati alle autorità di sicurezza estere (guardie di confine e polizia). Poiché per i divieti di recarsi in un Paese determinato si tratta di dati degni di particolare protezione di cui all'articolo 3 lettera c numero 4 LPD, è opportuna a una base legale formale (art. 17 cpv. 2 LPD). Una comunicazione all'estero è ammessa soltanto se nel Paese in questione è possibile garantire una protezione dei dati adeguata (art. 6 LPD).

La misura può avere un effetto preventivo soltanto se la persona interessata sa che rischia di essere identificata sia al momento di attraversare il confine, sia nel Paese di destinazione. Perciò la comunicazione dei dati alle guardie di confine e alle autorità straniere si deve evincere dalla decisione. Tale trasparenza impone anche la protezione dei dati.

Le autorità di sicurezza del Paese in cui ha luogo l'evento hanno tutto l'interesse a essere informate di tali divieti di recarsi in un Paese determinato, poiché la situazione di pericolo in occasione di detti eventi politici è sistematicamente assai elevata e le misure di sicurezza sono onerose di conseguenza.

32 https://www.fedpol.admin.ch/dam/data/ejpd/aktuell/news/2017/2017-12-04/171204-nap-i.pdf

Articolo 24m Tutela giurisdizionale

Le decisioni possono essere impugnate con ricorso al TAF. In linea di principio, il ricorso non ha effetto sospensivo, onde non vanificare lo scopo del divieto di recarsi in un Paese determinato. L'effetto sospensivo può tuttavia essere accordato dal Tribunale se non ne risulta pregiudicato lo scopo della misura.

Legge federale del 16 dicembre 2005[33] sugli stranieri e la loro integrazione

L'accesso al sistema d'informazione per il rilascio a stranieri di documenti di viaggio svizzeri e permessi di ritorno (ISR) per l'identificazione di una persona è imprescindibile per la ricerca e l'identificazione complete. Senza tale accesso, il SIC spesso non è in grado di identificare una persona e dovrebbe ricorrere ad altre misure che potrebbero rappresentare una grande ingerenza nei diritti della personalità. Tutte le informazioni su possibili viaggi e l'acquisizione di documenti sono importanti, ad esempio, per individuare precocemente potenziali combattenti stranieri jihadisti o per impedire viaggi verso zone di guerra. L'accesso all'ISR consente al SIC di operare con mezzi più leggeri, aventi un migliore rapporto rispetto alla protezione della personalitàn.

Per alcune categorie di stranieri, l'ISR è l'equivalente del sistema d'informazione per documenti d'identità (ISA) di cui all'articolo 11 della legge federale del 22 giugno 2001[34] sui documenti d'identità dei cittadini svizzeri. L'accesso del SIC all'ISA è già stato disciplinato dal Parlamento il 25 settembre 2020 con la legge federale sulle misure di polizia per la lotta al terrorismo (MPT))[35].

Codice penale[36]

A seguito dell'abrogazione o dell'adeguamento dell'articolo 74 capoverso 4 LAIn viene adeguato un rinvio.

Legge federale del 13 dicembre 2002[37] sull'Assemblea federale

L'inserimento dell'AVI-AIn nell'articolo 142 capoverso 2 LParl è l'equivalente dell'articolo 77 capoverso 2 LAIn. In tal modo si potrà tenere pienamente conto dell'esigenza di una base legale formale. Il Consiglio federale ritiene che anche l'AVI-AIn dovrebbe essere inclusa nell'articolo 142 capoverso 3 LParl e che la stessa AVI-AIn sia nella posizione migliore per difendere il proprio preventivo dinnanzi all'Assemblea federale se ciò risulta necessario. Il testo si ispira alla versione approvata dal Parlamento il 25 settembre 2020 in relazione con la revisione della LPD.

Legge federale del 20 marzo 1981[38] sull'assistenza internazionale in materia penale

L'attuale articolo 11*a* capoverso 3 della legge sull'assistenza in materia penale (AIMP) è in vigore dal 1 gennaio 2010 e contiene ancora il rinvio all'esecuzione della LMSI[39] da parte del SIC. All'epoca vi era una divisione tra acquisizione in Svizzera e acquisizione all'estero, disciplinata in due diversi atti normativi (vecchia LSIC e LMSI). Con l'entrata in vigore della LAIn la divisione è stata eliminata. Le attività menzionate in questo articolo in esecuzione della LMSI da parte del SIC oggi sono integrate nella LAIn. Quando quest'ultima è stata approvata, non si è proceduto all'adeguamento nell'AIMP. Esso non contiene modifiche in termini di contenuto. Le relative ordinanze vengono quindi adeguate.

Legge federale del 13 giugno 2008[40] sui sistemi d'informazione di polizia della Confederazione

Articolo 15 capoverso 1 lettera h

Secondo l'articolo 24*h* capoverso 4 LMSI (v. sopra) i divieti di recarsi in un Paese determinato sono segnalati nel RIPOL. La base legale per quest'ultimo viene integrata con la lettera h.

Articolo 18 capoverso 5 lettera d

L'aggiunta della lettera d amplia l'elenco dei compiti per il sistema di gestione delle pratiche e degli atti di fedpol al fine di potervi trattare le misure decise da quest'ultimo di cui all'articolo 24*h* capoverso 3 LMSI (v. sopra). Il testo si ispira alla versione approvata dal Parlamento il 25 settembre 2020 in relazione con la revisione della LPD.

Articolo 18a

Capoverso 1

33 RS **142.20**
34 RS **143.1**
35 FF **2020** 6795
36 RS **311.0**
37 RS **171.10**
38 RS **351.1**
39 RS **120**
40 RS **361**

Con il nuovo articolo 7 capoverso 1 lettere e–h e 1bis–3 AP-LAIn, il SIC prevede misure supplementari per garantire la protezione e la sicurezza dei suoi collaboratori, delle sue installazioni e dei dati che tratta (v. sopra). Anche fedpol necessita di due di queste nuove misure, ovvero il controllo delle persone già impiegate presso fedpol e il controllo relativo alle persone nell'ambito di una procedura di assunzione. I compiti assunti da fedpol coprono l'intero spettro di attività di polizia giudiziaria nell'ambito delle forme gravi e molto gravi di criminalità fino alla gestione dei sistemi d'informazione di polizia, alla protezione di magistrati ed edifici della Confederazione nonché di persone ed edifici protetti in virtù del diritto internazionale. L'adempimento di tali compiti impone requisiti elevati all'affidabilità dei collaboratori.

Già oggi fedpol sottopone ad accertamento le persone nell'ambito della procedura di assunzione allo scopo di verificare se sono oggetto di un procedimento amministrativo o penale pendente, se è stata pronunciata una sanzione nei loro confronti o se vi sono altre constatazioni rilevanti sul piano del diritto penale. Gli accertamenti hanno luogo previo consenso della persona interessata in base all'articolo 17 capoverso 2 lettera c LPD. Tuttavia, è emerso che in futuro dovrà essere possibile eseguire tale misura in modo sistematico. Se sussistono indizi concreti di una minaccia per la sicurezza di fedpol e dei suoi collaboratori, tali controlli devono poter essere eseguiti anche nei confronti di persone che sono già impiegate presso fedpol. Con questo ampliamento del contenuto normativo, i controlli devono poter poggiare su una specifica base legale formale. Tale base legale è ora creata con l'introduzione del nuovo articolo 18a AP-LSIP, il cui tenore si ispira in larga parte a quello della normativa prevista dal SIC con l'articolo 7 capoverso 1 lettere f e g nonché 1bis AP-LAIn. Con il termine «controllo del personale da parte di fedpol» si intende effettuare una distinzione concettuale dai «controlli di sicurezza relativi alle persone» ai sensi della LSIn e dalle «verifiche dell'affidabilità» ai sensi dell'articolo 20b nLPers[41]. Il controllo del personale riguarda tutte le persone che sono già impiegate presso fedpol (lett. a) e le persone che rientrano nella rosa ristretta dei candidati ai fini di un'assunzione presso fedpol; il controllo deve comunque avvenire prima che la persona assuma la nuova funzione presso fedpol (lett. b).

Nella prassi sono consultati in particolare i seguenti sistemi d'informazione disciplinati nella LSIP, ovvero JANUS (art. 10, 11 e 13), IPAS (art. 12 e 14), RIPOL (art. 15), il registro nazionale di polizia (art. 17) e ORMA (art. 18) nonché il sistema d'informazione HOOGAN secondo l'articolo 24a della legge federale del 21 marzo 1997[42] sulle misure per la salvaguardia della sicurezza interna (LMSI). Analogamente ai controlli della sicurezza relativi alle persone ai sensi dell'articolo 7 capoverso 1 lettere f e g AP-LAIn, anche i controlli del personale da parte di fedpol ai sensi del capoverso 1 lettere a e b possono essere effettuati soltanto previo consenso della persona interessata. Qualora nei casi di cui alla lettera a venga accertato un presunto comportamento punibile, fedpol denuncia il caso alle autorità di perseguimento penale competenti.

Fedpol non dispone di una legge formale che disciplini in modo esaustivo i suoi compiti, come è invece il caso della LAIn per il SIC. Nel presente contesto è dunque opportuno inserire all'interno della LSIP la nuova disposizione legale concernente i controlli del personale da parte di fedpol. Da un lato, i sistemi d'informazione utilizzati dall'Ufficio nella maggior parte dei casi per effettuare tali controlli sono disciplinati nella LSIP e, dall'altro, con l'introduzione del nuovo articolo 17 capoverso 4 lettera l nLSIP nella versione conformemente alla LSIn[43], è già presente nella LSIP un'altra disposizione concernente l'ambito del controllo di sicurezza relativo alle persone. Il diritto del personale non è dunque un contenuto nuovo per la LSIP.

Capoverso 2

Il grado di ingerenza giuridica di un controllo del personale da parte di fedpol ai sensi del capoverso 1 lettera a, ovvero di una persona che ha un rapporto d'impiego con l'Ufficio federale, è diverso rispetto a quello relativo al controllo di un candidato ad assumere una funzione presso fedpol. Nel primo caso, infatti, tale controllo può, in extremis, portare al licenziamento. Per questo motivo è necessario il consenso scritto di un membro della direzione di fedpol. Se un collaboratore di fedpol si rifiuta di acconsentire al controllo del personale, il consenso scritto del membro della direzione prevale su tale rifiuto. Non sarebbe altrimenti possibile confermare o respingere in modo definitivo gli indizi concreti di minaccia per la sicurezza dell'Ufficio e dei suoi collaboratori.

Legge federale del 3 febbraio 1995[44] sull'esercito e sull'amministrazione militare

Articolo 99 capoverso 5

A seguito degli adeguamenti delle disposizioni sull'autorità di vigilanza indipendente AVI-AIn nella LAIn viene corretto un rinvio.

Legge federale del 20 giugno 1997[45] sulle armi, gli accessori di armi e le munizioni

Articolo 9

L'articolo 9 della legge sulle armi (LArm) è in vigore dal 12 dicembre 2008. In tale data a i compiti di fedpol e del servizio informazioni internoerano disciplinati nella LMSI e le autorità d'esecuzione cantonali erano le stesse per entrambi. Con l'entrata in vigore della LAIn i compiti dei due uffici sono stati chiaramente separati per legge. Un Cantone può così designare un'autorità d'esecuzione per l'esecuzione della LMSI e un'altra per l'esecuzione della LAIn. Poiché in pratica l'autorità d'esecuzione emette il parere sull'acquisto di armi conformemente alla LAIn, è sufficiente adeguare il rinvio a quest'ultima nell'articolo 9 LArm.

41 LSIn, allegato 1 (Modifica di altri atti normativi), n. 4: LPers, nuovo art. 20*b* (FF **2020** 8755, in particolare 8787).
42 RS **120**
43 LSIn, allegato 1 (Modifica di altri atti normativi), n. 11: LSIP, nuovo art. 17 cpv. 4, frase introduttiva e lett. l (FF **2020** 8755, in particolare 8791).
44 RS **510.10**
45 RS **514.54**

Articolo 32c

L'accesso al sistema d'informazione comune armonizzato (ARMADA) di cui all'articolo 32*a* capoverso 3 LArm consente al SIC di valutare meglio il potenziale di minaccia di una persona in quanto fornisce indizi in merito al possesso o al ritiro definitivo di un'arma o al rifiuto di una richiesta di acquistarla. L'argomento è diventato ancora più importante alla luce di vari omicidi di massa (ad es. Christchurch / Hanau) da parte di estremisti di destra. Inoltre, è noto che persone provenienti dal contesto salafista o islamista incline alla violenza cercano di armarsi. I chiarimenti tempestivi sono assolutamente necessari per effettuare una stima seria della minaccia alla sicurezza interna ed esterna.

Poiché anche la legge sulle dogane è sottoposta a revisione, a seconda dello stato dei lavori sarà necessario un coordinamento.

Legge federale del 17 giugno 2016[46] sul casellario giudiziale informatizzato VOSTRA

Si tratta di un adeguamento terminologico. La LAIn utilizza il termine «fonte umana» al posto di «informatori». L'articolo 9 LAIn statuisce quali autorità devono collaborare con il SIC. Il termine «autorità d'esecuzione cantonale» è la designazione impiegata a tal fine nella LAIn. L'entrata in vigore di quest'ultima rende obsoleto il rinvio alla LMSI e si rinvia pertanto al pertinente articolo della LAIn stessa.

La presente legge entrerà in vigore presumibilmente nel 2023.

Legge sulle dogane del 18 marzo 2005[47]

In particolare esponenti del contesto terrorista sono noti per i loro viaggi e i loro contatti all'estero. Combattenti stranieri jihadisti, ma anche reti di contatti degli ambienti islamisti con cerchie islamiste nei Paesi limitrofi, sono anch'essi noti e documentati dal SIC. Il «Sistema d'informazione dell'UDSC» dell'AFD contiene dati di grande interesse e importanza per chiarimenti delle circostanze dettagliati.

Nel settore dello spionaggio, i dati provenienti dal sistema d'informazione dell'UDSC possono essere utili per scoprire con chi e con quale veicolo ha viaggiato una persona. Inoltre, tali dati sono rilevanti anche per il settore della non proliferazione onde chiarire importazioni ed esportazioni di merci o per il fatto di portare seco somme di denaro contante vistosamente ingenti.

A causa del nuovo accesso del SIC è necessario adeguare l'allegato 4 dell'ordinanza del 23 agosto 2017[48] sul trattamento dei dati nell'AFD. L'adeguamento avverrà nell'ambito della revisione delle relative ordinanze successiva alla revisione della LAIn.

Poiché anche la presente legge è sottoposta a revisione, a seconda dello stato dei lavori sarà necessario un coordinamento, oppure le modifiche previste in questa sede risulteranno superate.

Legge federale del 19 dicembre 1958 sulla circolazione stradale[49]

Con l'entrata in vigore parziale della modifica del 15 giugno 2012 della legge federale del 19 dicembre 1958 sulla circolazione stradale (LCStr) il 1° gennaio 2019, gli accessi del SIC mediante procedura di richiamo, parzialmente ridisciplinati con l'entrata in vigore della LAIn, ai sistemi dell'Ufficio federale delle strade, che sono stati sostituiti dal sistema d'informazione sull'ammissione alla circolazione (SIAC), sono stati erroneamente stralciati. Si tratta di una svista normativa che viene corretta con la presente integrazione.

Legge federale del 18 marzo 2016[50] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni

Articolo 14a

Poiché al SIC non vi sono più sistemi d'informazione differenti, nella presente disposizione si parla ora soltanto di dati. I dati contenuti nel sistema di trattamento sono descritti nell'articolo 8 LSCPT e comprendono anche le indicazioni sui servizi di telecomunicazione (art. 8 lett. c LSCPT), ovvero le informazioni (art. 7 lett. c LSCPT). Non vi sono però modifiche in termini di contenuto. I dati possono continuare a essere copiati elettronicamente e trasmessi al SIC, così che possa trattarli. Le misure di cui al capoverso 1 lettera b sono le misure di acquisizione previste nella LAIn.

Articolo 39 capoverso 4

Come nell'articolo 83*c* LAIn, anche per la disposizione penale di diritto amministrativo nell'articolo 39 LSCPT occorre applicare il disciplinamento dell'articolo 7 DPA su multe che non superano 20 000 franchi e creare la possibilità di consentire di punire efficace-

46 FF **2016** 4315
47 RS **631.0**
48 RS **631.061**
49 RS **741.01**
50 RS **780.1**

mente le persone giuridiche assoggettate alla LSCPT qualora non ottemperino ai propri obblighi. L'attuale disposizione penale dell'articolo 39 è entrata in vigore il 18 marzo 2018. All'atto pratico, da allora sono sorte difficoltà con imprese renitenti che finora quasi non hanno potuto essere richiamate alle proprie responsabilità, una situazione che la presente disposizione è intesa a migliorare. Se nel nostro Paese, in linea di principio, si puniscono le persone fisiche che hanno commesso il reato, la «punizione» delle persone giuridiche costituisce quindi un'ingerenza in questo principio, che però si è dimostrata efficace nel settore del procedimento penale amministrativo, specialmente nella legislazione in materia di imposta sul valore aggiunto, doganale e di agenti terapeutici. In questa sede si rinvia anche al commento all'articolo 83*c* capoverso 3 LAIn.

Modifica di altri atti normativi: numeri 13−17

La LAIn utilizza il termine «autorità d'esecuzione cantonali», il che è reso uniforme in queste leggi.

3 Ripercussioni

3.1 Ripercussioni per la Confederazione sul piano finanziario e sull'effettivo del personale

L'AVI-AIn può compensare l'onere supplementare per l'assunzione dei compiti dell'ACI grazie agli incrementi di efficienza realizzati nell'ambito del consolidamento della propria organizzazione e delle proprie attività.

I nuovi compiti previsti secondo la LMSI comportano un certo onere supplementare per la fedpol e il SIC. Si prevede che il divieto di recarsi in un Paese determinato si applicherà a una cerchia di persone assai ristretta (numero basso in doppia cifra) e a un numero gestibile di eventi. I divieti di recarsi in un Paese determinato, paragonabili, nell'ambito delle misure contro la violenza in occasione di manifestazioni sportive (art. 24*c* LMSI) causano per ogni decisione un onere di, mediamente, 1−2 giorni lavorativi, mentre in caso di reclamo contro la decisione è da prevedere un onere lavorativo di 3−5 giorni. Fedpol gestirà questo onere con le risorse esistenti.

Le altre modifiche richieste non comportano per la Confederazione oneri maggiori in termini finanziari e di personale in quanto attualmente l'effettivo del personale del SIC viene aumentato affinché possa adempiere i propri compiti con la necessaria capacità di resistenza.

3.2 Ripercussioni per i Cantoni e i Comuni, nonché le città, gli agglomerati e le regioni di montagna

I nuovi divieti di recarsi in un Paese determinato secondo la LMSI possono comportare oneri supplementari per i Cantoni, poiché essi devono motivare le proprie richieste nei confronti di fedpol.

Per Cantoni, Comuni, città, agglomerati e regioni di montagna le modifiche richieste non comporteranno alcuna ripercussione significativa sul piano finanziario e sull'effettivo del personale.

3.3 Ripercussioni sull'economia, la società e l'ambiente

Non sono da attendersi ripercussioni negative su economia, società e ambiente. Le modifiche proposte, invece, migliorano l'esecuzione della LAIn, con un impatto positivo sulla situazione della sicurezza in Svizzera.

La nuova misura ai sensi della LMSI contribuisce alla sicurezza pubblica in Svizzera e all'estero (impedire l'esportazione di attività di estremismo violento). Ha inoltre un effetto protettivo preventivo, in particolare sui giovani che si trovano in un ambiente di estremisti violenti e sono quindi esposti a un contesto incline alla violenza se non addirittura violento.

4 Rapporto con il programma di legislatura e le strategie del Consiglio federale

Il presente disegno è annunciato nel messaggio del 29 gennaio 2020[51] sul programma di legislatura 2019–2023.

5 Aspetti giuridici

5.1 Costituzionalità

L'avamprogetto si basa sull'articolo 54 capoverso 1 della Costituzione federale[52] (Cost.) per l'ambito della sicurezza esterna della Svizzera e, in materia di protezione dello Stato in Svizzera, sulla competenza intrinseca della Confederazione ad adottare le misure necessarie per la propria salvaguardia e per quella dei propri organi e delle proprie istituzioni (per la quale nell'ingresso si fa riferimento all'articolo 173 capoverso 2 Cost.).

51 FF **2020** 1565, 1684
52 RS **101**

Con la presente revisione, il Consiglio federale non va oltre quanto già oggi è di competenza della Confederazione ai sensi della Cost. Di conseguenza, esso si fonda su una base costituzionale sufficiente. Considerazioni più dettagliate in merito si trovano nel messaggio concernente la LAIn (FF 2014 2007).

È controverso se la rinuncia a un rimedio giuridico ordinario in caso di limitazione o di rifiuto del diritto d'accesso sia conforme alla Costituzione e al diritto internazionale ed è una questione che verrà chiarita in maniera approfondita nel corso della procedura di consultazione.

5.2 Conseguenze in materia di diritto di protezione dei dati

Il presente disegno di revisione si basa su una valutazione d'impatto sulla protezione dei dati che il SIC aveva preparato con l'appoggio dell'autore del *Kommentar zum Schweizerischen Datenschutzgesetz* (commento alla legge svizzera sulla protezione dei dati), David Rosenthal, in vista dell'elaborazione del disciplinamento alternativo del trattamento dei dati. La valutazione d'impatto sulla protezione dei dati contiene una descrizione dell'attuale trattamento dei dati informativi e una valutazione dei rischi per la personalità e i diritti fondamentali degli interessati, indica le misure volte a proteggere personalità e diritti ed evidenzia punti deboli e possibilità di miglioramento. Tale valutazione tiene inoltre conto delle raccomandazioni della DelCG e dell'AVI-AIn.

Essa elenca le numerose misure derivanti dai settori archiviazione e gestione degli atti, garanzia di cancellazioni, garanzia della qualità dei dati in entrata e in uscita, controllo della qualità e garanzia di un'adeguata governance. Indica inoltre i rischi per gli interessati e altri rischi ai sensi della legge sulla protezione dei dati. Ai rischi sono stati contrapposti le possibili cause, i possibili danni e le misure tecniche e organizzative già adottate dal SIC per evitare danni. In seguito è stata effettuata una valutazione dei rischi nella quale si sono stimate l'entità del danno e la probabilità che esso si verifichi. Infine, per ogni rischio vi è stata una dichiarazione su come il SIC tratta il rischio residuo rilevato, comprese eventuali misure che intende attuare in tale contesto.

A seguito delle risultanze di tale stima, il presente disegno consente un notevole progresso nella protezione dei dati. È tecnologicamente neutro e molto meno complesso rispetto all'attuale disciplinamento. Inoltre, i seguenti rischi identificati nella valutazione d'impatto sulla protezione dei dati e valutati da medi a elevati in futuro saranno ulteriormente ridotti come segue:

- il rischio che il SIC tratti dati su persone non rilevanti per la LAIn è attenuato dall'introduzione di una verifica verifica dei dati in entrata (art. 45). Le comunicazioni in entrata non sono più valutate nel loro insieme, bensì nel dettaglio. Tutti i contenuti che non presentano un nesso con i compiti o che rientrano nei limiti posti al trattamento dei dati vengono resi anonimi. Per i dati provenienti da fonti accessibili al pubblico e per i dati memorizzati separatamente provenienti da misure di acquisizione soggette ad autorizzazione, la verifica dei limiti posti al trattamento dei dati avviene soltanto prima che suddetti dati vengano impiegati quali dati di lavoro. Fino ad allora sono soggetti a un blocco dell'utilizzazione. Il SIC ha ora inoltre l'obbligo di informare le autorità d'esecuzione cantonali quando queste le fanno pervenire rapporti che presentano dati che non hanno alcun nesso con i compiti di cui all'articolo 6 o che violano i limiti posti al trattamento dei dati dell'articolo 5 capoverso 5. Tali dati devono essere distrutti o resi anonimi sia presso il SIC, sia presso le autorità d'esecuzione cantonali (art. 58*c* cpv. 2);
- il rischio che il SIC tratti dati falsi su persone e che i prodotti informativi del SIC siano allestiti sulla base di dati falsi è attenuato dal fatto che i dati grezzi possono essere utilizzati soltanto se sono stati sottoposti a una verifica dell'esattezza (art. 51 cpv. 1). Fino a quel momento sono soggetti a un blocco dell'utilizzazione. Inoltre, l'organo di controllo della qualità del SIC ottiene l'accesso sistematicamente a tutti i dati di quest'ultimo e delle autorità d'esecuzione cantonali;
- il rischio che gli interessati non sappiano chi è responsabile del trattamento dei loro dati personali da parte del SIC e delle autorità d'esecuzione cantonali è attenuato dal fatto che nell'articolo 9 capoverso 4 la responsabilità è chiaramente attribuita al SIC. Ciò comporta anche che gli interessati abbiano soltanto ancora un interlocutore, il che facilita l'esercizio di diritti degli interessati;
- il rischio dell'esperienza inquietante (una persona sa o crede che il SIC tratti dati su di lei, ma ne ignora la ragione) è attenuato dal fatto che il diritto di accesso viene assoggettato al regime analogo della LSIP. Le persone possono pertanto essere informate molto più rapidamente di quanto non sia stato finora possibile a seconda della concezione giuridica;
- il rischio che i dati vengano trattati più a lungo del necessario è attenuato dalla rinuncia a depositi di dati separati in singoli sistemi d'informazione. Ora non si lavora più con copie di dati che eventualmente non vengono rese anonime o cancellate insieme all'originale. Ciò attenua anche il rischio che gli stessi dati siano soggetti a norme di trattamento dei dati differenti a seconda del sistema d'informazione (ad es., oggi vengono resi anonimi in IASA-GEX SIC, ma non in GEVER SIC, o cancellati dopo 15 anni nel primo, ma dopo 20 anni nel secondo). Inoltre, sarà ora possibile gestire ogni singolo file attraverso i suoi metadati (ad es. riguardo ad accessi e termini di conservazione) e garantirne la qualità, mentre attualmente si lavora ancora con cartelle e registri elettronici;
- il rischio che una persona sia sospettata dal SIC più a lungo del necessario è attenuato dal fatto che il SIC può trattare anche dati a discarico e aggiungerli a quelli a carico fino a che il sospetto non è stato completamente fugato e i dati possono essere cancellati (art. 52 cpv. 3).

La rinuncia alla definizione di sistemi d'informazione è compatibile con la concezione della LPD*riv*. Non vengono più disciplinate collezioni di dati, bensì attività di trattamento. Non ci si concentra più sul dove dati vengono memorizzati, bensì su quello che se ne fa. Ora i dati personali trattati vengono assegnati a tali attività di trattamento (art. 49). Così il loro trattamento può ora essere disciplinato in modo neutrale dal punto di vista tecnologico. Tale adeguamento è conforme anche allo sviluppo della tecnologia dell'informazione. Non vi è connessa o prevista un'estensione del trattamento dei dati ma, al contrario, occorre poterlo controllare meglio.

Nel processo legislativo attuale, che si trova ancora nella fase iniziale, non sembra opportuno allestire una nuova valutazione d'impatto sulla protezione dei dati riguardante il presente disegno. Verrà comunque elaborata in tempo per il progetto definitivo da presentare al Parlamento, come richiesto dalla LPD*riv*.

5.3 Compatibilità con gli impegni internazionali della Svizzera

Le modifiche della LAIn proposte sono compatibili con gli obblighi assunti dalla Svizzera sul piano internazionale.

5.4 Forma dell'atto

Conformemente all'articolo 164 Cost. e all'articolo 22 capoverso 1 LParl, l'Assemblea federale emana sotto forma di legge federale tutte le disposizioni importanti che contengono norme di diritto.

5.5 Subordinazione al freno alle spese

Il presente avamprogetto non è subordinato al freno alle spese ai sensi dell'articolo 159 capoverso 3 lettera b Cost. poiché non contiene disposizioni in materia di sussidi e non comporta neanche le basi per la costituzione di crediti d'impegno o dotazioni finanziarie.

5.6 Rispetto del principio di sussidiarietà e del principio dell'equivalenza fiscale

5.7 Conformità alla legge sui sussidi

Il presente avamprogetto non introduce disposizioni nuove o adeguate che incidono sui principi della legge sui sussidi.

5.8 Delega di competenze legislative

Come avveniva finora, il Consiglio federale è incaricato di disciplinare i dettagli del trattamento dei dati. Si tratta dell'adeguamento logico della previgente delega per gli attuali sistemi d'informazione e sistemi di memorizzazione.

5.9 Protezione dei dati

Il presente avamprogetto disciplina scopo, contenuto e cerchia di utenti del trattamento dei dati nonché il diritto di accesso che ora è retto dalle disposizioni della LPD*riv*.

La trasmissione e il trattamento di dati personali degni di particolare protezione necessitano di una base legale formale (art. 34 cpv. 1 LPD*riv*). Le prescrizioni in materia di protezione dei dati sono garantite dalla presente base legale formale.