Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Servizio delle attività informative della Confederazione SIC

Rapporto esplicativo concernente l'ordinanza sulle attività informative (OAIn) e l'ordinanza sui sistemi d'informazione e di memorizzazione del Servizio delle attività informative della Confederazione (OSIM-SIC)

1 Premessa

Per la legge sulle attività informative (LAIn) sono previste due ordinanze: l'ordinanza «generale» sulle attività informative (OAIn) e l'ordinanza «tecnica» sui sistemi d'informazione e di memorizzazione del Servizio delle attività informative della Confederazione (OSIM-SIC). La struttura dell'OAIn non segue strettamente quella della LAIn, bensì è focalizzata anzitutto sugli utenti esterni e tratta soltanto alla fine gli aspetti interni al SIC.

2 Commento alle disposizioni dell'OAIn

Capitolo 1: Collaborazione

Sezione 1: Collaborazione del SIC con organi in Svizzera

La prima sezione ha per oggetto i principi generali della collaborazione con i principali partner del SIC in Svizzera. Tali principi corrispondono allo status quo e si ispirano alla regola del reciproco appoggio. Questa sezione non tratta invece delle forme concrete di collaborazione, e in particolare della collaborazione con le autorità d'esecuzione cantonali. Le relative facoltà e competenze in materia di acquisizione autonoma di informazioni sono già esaustivamente disciplinate all'articolo 85 LAIn (Esecuzione da parte dei Cantoni). Ovviamente, il SIC ha la possibilità di affidare alle competenti autorità cantonali anche l'esecuzione di ulteriori misure. Di conseguenza, in quest'ambito le autorità d'esecuzione cantonali non operano autonomamente, bensì su formale mandato del SIC, il quale ne assume dunque anche la responsabilità.

Articolo 1 Collaborazione del SIC con organi e persone in Svizzera

Nell'ordinanza si è rinunciato a menzionare esplicitamente sia la collaborazione e l'assegnazione di mandati nell'ambito dell'acquisizione secondo l'articolo 34 LAIn, sia la comunicazione di dati personali a terzi secondo l'articolo 62 della stessa legge, poiché le due cose sono entrambe espressamente previste nella legge e quindi senz'altro applicabili, ma soprattutto per evitare inutili ridondanze tra legge e ordinanza.

Articolo 5 Collaborazione del SIC con fedpol

La disposizione prevede espressamente che il SIC e fedpol si sostengano reciprocamente nell'impiego e nell'utilizzazione di risorse e mezzi operativi, onde evitare che, compatibilmente con la diversità dei compiti svolti, si debbano acquistare due volte costose apparecchiature e di conseguenza si debba spendere anche il doppio nella loro manutenzione, oppure si creino doppioni a livello di formazione. La trasmissione di informazioni secondo il capoverso 2 non è disciplinata esaustivamente; fedpol e il SIC collaborano strettamente ad esempio anche in comitati direttivi e organi comuni, quali quelli deputati al coordinamento operativo della lotta antiterrorismo o nello Stato maggiore speciale Presa di ostaggi e ricatto. La prassi sinora seguita, disciplinata in passato da accordi tra il SIC e fedpol, viene dunque mantenuta.

Sezione 2: Collaborazione del SIC con servizi esteri

La collaborazione con i servizi esteri si ispira alla situazione giuridica attuale, integrata dalla prassi consolidata.

Articolo 7 Definizione annua dei principi della collaborazione

La definizione annua dei principi della collaborazione corrisponde alla prassi attuale e viene ora sancita a livello di ordinanza. Una valutazione sommaria della rilevanza di questi contatti a livello di Consiglio federale appare gerarchicamente corretta ed è giustificata anche in considerazione del fatto che, prima che l'affare venga trattato in Consiglio federale, la Delegazione Sicurezza (DelSic) lo discute preliminarmente e in tale sede è possibile effettuare anche approfonditi accertamenti.

Articolo 8 Competenze

Come finora, nel quadro della LAIn il SIC continuerà a fungere da «single point of contact» per i contatti con i servizi esteri che adempiono compiti ai sensi di detta legge. Il concetto sinora applicato ha dato buone prove e sarà dunque mantenuto. Il SIC rappresenta anche la Svizzera nei consessi internazionali dell'intelligence. In entrambi i casi sono possibili deroghe con l'autorizzazione del SIC. In campo militare, l'interlocutore del SIC per la definizione di una politica comune nei confronti dei servizi partner e l'elaborazione di una pianificazione dei contatti è il Servizio informazioni militare (SIM), che a sua volta ha in particolare scambi con il Comando forze speciali (CFS) e con SWISSINT (Swiss Armed Forces International Command).

Articolo 9 Tipi di collaborazione

Questa disposizione concretizza l'articolo 12 capoverso 1 lettera c LAIn, il quale dispone che il SIC può svolgere attività congiunte con servizi delle attività informative e autorità di sicurezza esteri per acquisire e analizzare informazioni e per valutare la situazione di minaccia. Come già previsto oggi, il SIC può collaborare in varie forme con servizi esteri. Oltre all'acquisizione di informazioni e alla condotta congiunta di operazioni, l'ordinanza prevede la realizzazione congiunta di prodotti (per prodotti secondo l'art. 9 cpv. 2 lett. c OAIn si intendono ad es. analisi, valutazioni della situazione e altre valutazioni), la collaborazione nel campo della formazione (ad es. nel campo delle attività di analisi o della sicurezza) e la realizzazione di progetti congiunti (ad es. lo sviluppo di mezzi di comunicazione protetti tra i servizi o la suddivisione del lavoro di analisi di fonti aperte (OSINT)).

Articolo 10 Trattati internazionali di portata limitata

Il SIC sarà ora autorizzato a concludere autonomamente trattati internazionali con servizi delle attività informative esteri o con altri servizi esteri che adempiono compiti ai sensi della LAIn. In virtù dell'articolo 48*a* della legge del 21 marzo 1997 sull'organizzazione del Governo e dell'Amministrazione (LOGA; RS 172.010), il Consiglio federale può delegare a un

dipartimento la competenza di concludere trattati internazionali. Per trattati di portata limitata, può delegare questa competenza anche a un aggruppamento o a un ufficio federale. Di conseguenza, il SIC è competente a titolo esclusivo per concludere autonomamente trattati internazionali di portata limitata su questioni tecniche in materia di attività informative. Si pensi ad esempio a un accordo sugli standard tecnici applicabili a un sistema ammesso dal diritto svizzero per lo scambio di informazioni con un servizio estero. Naturalmente, qualora fossero (eccezionalmente) adempiute le condizioni previste all'articolo 80 capoverso 3 LAIn, anche questi trattati dovrebbero essere sottoposti al Consiglio federale per approvazione.

Capitolo 2: Acquisizione di informazioni

Sezione 1: Principi

Articolo 12 Operazioni

Il termine «operazione» va necessariamente definito, poiché per le misure di acquisizione soggette ad autorizzazione la conclusione di un'operazione fa scattare l'obbligo di comunicazione previsto dall'articolo 33 LAIn (risp. il differimento o la rinuncia). Occorre inoltre permettere la distinzione tra il semplice trattamento di questioni di intelligence e la gestione di una costellazione di casi molto più estesa, generalmente complessa e soggetta a particolare attenzione da parte degli organi di vigilanza. Per di più, il SIC deve iniziare e concludere le operazioni in modo formale e documentarle separatamente. Occorre infine evidenziare che gli organi di vigilanza, a prescindere al fatto che eventi correlati siano qualificati «operazioni», hanno completo accesso a tutte le informazioni e a tutti i documenti utili nonché a tutti i locali del SIC.

Articoli 13 – 16 Collaborazione e mandati nell'ambito dell'acquisizione con o da parte di servizi svizzeri, collaborazione e mandati nell'ambito dell'acquisizione con o da parte di servizi esteri in Svizzera, collaborazione e mandati nell'ambito dell'acquisizione con o da parte di privati in Svizzera; collaborazione e acquisizione con o da parte di servizi o privati all'estero

In virtù dell'articolo 34 LAIn, il SIC «può eseguire esso stesso le misure di acquisizione, collaborare con servizi svizzeri o esteri oppure demandarne l'esecuzione a tali servizi, sempre che offrano la garanzia di eseguire l'acquisizione conformemente alle disposizioni della presente legge. Il SIC può eccezionalmente collaborare anche con privati o assegnare loro mandati, se è necessario per motivi tecnici o di accesso all'oggetto dell'acquisizione ed essi offrono la garanzia di eseguire l'acquisizione conformemente alle disposizioni della presente legge».

Sussiste soprattutto la necessità di disciplinare la collaborazione *in Svizzera con*

- *servizi svizzeri,*
- *servizi esteri,*
- *privati.*

Secondo l'ordinanza, l'acquisizione in Svizzera è conforme alla legge se

- nel caso di un servizio svizzero, l'acquisizione avviene nell'ambito dell'attività ordinaria del servizio in questione o se lo stesso sembra idoneo all'acquisizione di informazioni e inoltre possiede le capacità necessarie all'acquisizione e sono date le pertinenti disposizioni di legge o il SIC l'ha accuratamente istruito al riguardo;
- le pertinenti disposizioni di diritto svizzero in materia di acquisizione di informazioni sono state comunicate al servizio estero o al privato e per quanto necessario spiegate e il servizio estero o il privato in questione dichiara di voler rispettare tali disposizioni.

Per la collaborazione e l'assegnazione di mandati nell'ambito dell'acquisizione con o da parte di servizi esteri o privati *all'estero* si applicano condizioni agevolate. Ciò è giustificato dal fatto che il SIC cura contatti con oltre un centinaio di autorità di sicurezza estere del mondo intero e occorre quindi tener conto delle peculiarità dei rispettivi Paesi e della sovranità dei servizi di sicurezza esteri.

Articolo 18 Protezione delle fonti

Per quanto riguarda la protezione delle fonti, i principi cardine sono già contemplati nell'articolo 35 LAIn. A livello di ordinanza si precisa ora ciò che si intende per fonte in ambito informativo. Si tratta delle fonti umane, dei servizi delle attività informative e delle autorità di sicurezza svizzeri ed esteri con cui il SIC collabora nonché delle fonti tecniche. Per i casi non ancora disciplinati nella legge, l'ordinanza sancisce il principio della ponderazione degli interessi nel singolo caso tra la fonte che richiede le informazioni e la fonte da proteggere. Una fonte umana deve essere protetta in modo assoluto se è esposta a un serio pericolo per la sua integrità fisica o psichica. Come sinora, se le circostanze lo esigono la protezione si estende anche alle persone vicine alla fonte in questione (ad es. familiari, partner ecc.). Le fonti tecniche devono essere protette nella misura in cui la divulgazione di indicazioni su di esse potrebbe compromettere l'adempimento della missione del SIC. Occorre infine sottolineare che la protezione delle fonti riveste il massimo interesse per il SIC, poiché se non potesse garantire tale protezione sarebbe facilmente e prontamente escluso dallo scambio di informazioni a livello internazionale, con le relative conseguenze per la sicurezza della Svizzera. La collaborazione con fedpol nel singolo caso, prevista per le fonti umane al capoverso 4, si basa sull'articolo 14 LOGA e riguarda le misure di protezione da adottare. Il SIC si accolla i costi complessivi, quantunque in casi particolari occorra elaborare una soluzione con l'AFF e fedpol.

Sezione 2: Obbligo di informazione in caso di minaccia concreta

Il disciplinamento degli obblighi di informazione e comunicazione riprende per l'essenziale la normativa attuale, con procedure collaudate: il SIC collabora strettamente con i Cantoni, ma nell'adempimento del mandato concede loro una grande autonomia.

Dato che il fermo a scopo di identificazione e interrogatorio ora previsto all'articolo 24 LAIn può essere operato esclusivamente da agenti di un corpo di polizia cantonale, non sussiste alcuna necessità di disciplinamento a livello dell'OAIn.

Articolo 19 capoverso 2 Obbligo di informazione in caso di minaccia concreta

Nell'elenco delle organizzazioni di cui all'allegato 1, alle quali la Confederazione o i Cantoni hanno delegato compiti pubblici, sono state aggiunte l'Autorità federale di vigilanza sui mercati finanziari (FINMA), la Commissione federale dell'energia elettrica (ElCom) e la Commissione federale delle comunicazioni (ComCom).

Secondo l'articolo 20 capoverso 4 LAIn, il Consiglio federale stabilisce in un elenco non pubblico quali fatti e constatazioni devono essere comunicati spontaneamente al SIC. Definisce l'estensione dell'obbligo di comunicazione e la procedura per fornire le informazioni. Questo elenco non pubblico può contenere, nonostante il commento (in parte ambiguo) dovuto a una svista redazionale contenuto nel messaggio concernente la LAIn, sia obblighi di comunicazione su eventi e constatazioni che per ragioni di segretezza non possono essere pubblicati, sia altri che invece non soggiacciono ad alcun obbligo di segretezza. Dato che gli obblighi di comunicazione riguardano l'acquisizione di informazioni, occorre tener conto anche dell'articolo 67 LAIn, secondo cui i documenti ufficiali riguardanti l'acquisizione di informazioni sono espressamente sottratti al principio di trasparenza e quindi, logicamente, non devono nemmeno essere pubblicati.

Sezione 3: Misure di acquisizione soggette ad autorizzazione

La legge disciplina le misure di acquisizione soggette ad autorizzazione in modo assai dettagliato e completo. A livello di ordinanza non sussiste pertanto alcuna necessità di disciplinamento.

Articolo 20 Perquisizioni di locali, veicoli e contenitori

La perquisizione di locali, veicoli e contenitori deve essere documentata. Dato che si tratta di perquisizioni eseguite in segreto, vale a dire in assenza della persona interessata, la documentazione deve servire in primo luogo a confutare eventuali accuse di abuso e/o richieste di risarcimento che potrebbero essere formulate in seguito nei confronti del SIC. Se le condizioni in loco lo consentono, la documentazione può essere effettuata anche con registrazioni video o audio.

Articolo 21 Procedura di autorizzazione e nullaosta

La procedura di autorizzazione e di nullaosta deve essere sempre documentata dal SIC e dal DDPS in modo da garantire la tracciabilità.

Articolo 22 Tutela di segreti professionali

La protezione prevista all'articolo 28 LAIn per le persone appartenenti a una delle categorie professionali menzionate agli articoli 171 – 173 CPP viene precisata a livello di ordinanza: se una *persona oggetto di indagini* è sottoposta a sorveglianza in applicazione dell'articolo 27 LAIn e appartiene a una delle categorie professionali menzionate agli articoli 171 – 173 CPP, occorre operare una selezione preliminare («cernita») dei dati raccolti nell'ambito dell'acquisizione, onde garantire che il SIC non venga a conoscenza di segreti professionali, a meno che la minaccia concreta non venga intenzionalmente celata sfruttando il pretesto di un tale segreto. In determinate circostanze il SIC deve pertanto indicare questo aspetto e richiedere un'opportuna selezione delle informazioni. La cernita e distruzione dei dati protetti avvengono sotto la vigilanza del Tribunale amministrativo federale. Non è invece ammesso ordinare una misura di acquisizione soggetta ad approvazione nei confronti di *terzi* appartenenti a una delle categorie professionali menzionate agli articoli 171 – 173 CPP.

Sezione 4: Infiltrazione in sistemi e reti informatici ubicati all'estero

Articolo 23

In virtù dell'articolo 37 capoverso 1 LAIn, il SIC può infiltrarsi in sistemi e reti informatici ubicati all'estero utilizzati per l'infiltrazione in infrastrutture critiche in Svizzera. Le decisioni in merito all'attuazione di queste misure spetta al Consiglio federale. Da queste attività occorre distinguere la penetrazione in sistemi e reti informatici ubicati all'estero ai sensi dell'articolo 37 capoverso 2 LAIn per acquisire informazioni ivi disponibili o trasmesse da tali sistemi e reti su fatti che avvengono all'estero. In tal caso, il capo del DDPS decide in merito all'esecuzione di tale misura previa consultazione del capo del DFAE e del capo del DFGP.
Per sgravare i decisori e garantire la tempestività delle decisioni, l'ordinanza prevede che nell'affrontare un caso o una costellazione di casi (ad es. rapimento di XY) la consultazione del capo del DFAE o del DFGP e quindi la decisione del capo del DDPS possano avvenire anche in una volta sola. Una simile autorizzazione per un caso o una costellazione di casi copre, se necessario, anche l'infiltrazione plurima in sistemi e reti informatici, nel caso della stessa persona o di persone diverse (sempre che sussista un collegamento tra queste e il caso o la costellazione di casi oggetto dell'autorizzazione). In altre parole, si tratta di un'autorizzazione che, per quanto ampia, è limitata a un caso o a una costellazione di casi (autorizzazione ampia ma circoscritta, ad es. all'infiltrazione in sistemi informatici dei rapitori in un caso di rapimento, oppure, dopo un attacco informatico respinto, all'infiltrazione per un certo tempo nei sistemi informatici dell'aggressore al fine di scoprire l'identità degli autori dell'attacco e/o ulteriori attacchi e/o vittime).

Sezione 5: Esplorazione di segnali via cavo

Il mandante dell'esplorazione di segnali via cavo è il SIC, ma il mandato viene eseguito dal servizio preposto all'esecuzione, ossia il Centro per le operazioni elettroniche (COE) della Base d'aiuto alla condotta dell'esercito. Il COE garantisce anzitutto, per mezzo di misure interne, che l'adempimento del mandato avvenga entro i limiti dell'autorizzazione rilasciata dal Tribunale amministrativo federale. Inoltre, acquista le installazioni tecniche necessarie e funge da organo di contatto nei rapporti con i gestori di reti filari e con i fornitori di servizi di telecomunicazione. Questi devono permettere in qualsiasi

momento al COE di accedere ai locali necessari per l'esplorazione dei cavi, onde consentirgli di installare i componenti tecnici per il rilevamento dei dati tecnici o per l'adempimento di mandati di esplorazione.

Nell'ambito del rilevamento dei dati tecnici da parte dei gestori di reti filari e dei fornitori di servizi di telecomunicazione o del COE non vengono memorizzati contenuti delle comunicazioni, ma rilevati regolarmente dati statistici sui flussi di dati che transitano sulle reti cablate, per poter identificare i Paesi mittenti e destinatari nonché i protocolli e i processi tecnici utilizzati. I dati così raccolti permettono di definire il tipo e la quantità di apparecchiature necessari per una eventuale successiva captazione di dati. Tali dati statistici sono indispensabili per poter presentare al Tribunale amministrativo federale una domanda giuridicamente conforme e possibilmente sostanziata e consentono, in un caso concreto di applicazione, di indicare a detto tribunale presso quale gestore di rete o fornitore di servizi di telecomunicazione si trovano i dati potenzialmente rilevanti.

Per il resto, i dati registrati nell'ambito di un'esplorazione radio possono essere impiegati anche per i mandati di esplorazione di segnali via cavo.

I contatti informativi del COE con i servizi esteri specializzati avvengono per il tramite del SIC.

Articolo 29 capoversi 2 e 3 Trattamento dei dati

Per dati si intende l'insieme di tutte le registrazioni provenienti dall'esplorazione radio e dei segnali via cavo (termine generico). Tale concetto ingloba sia il concetto di comunicazione, ossia il vero e proprio contenuto di comunicazione dei dati registrati (ad es. lingua, testo, immagini), sia il concetto di dati di collegamento. Questi sono quella parte dei dati registrati che non sono «comunicazione», completati dalle informazioni aggiunte dai sistemi di registrazione («Session Related Informations», tra cui ad es. il momento della registrazione). Da essi occorre distinguere il concetto di risultato, che rappresenta, piuttosto che parte del concetto di dati, i prodotti derivanti dai dati (vale a dire le informazioni conformi al mandato) trasmessi al SIC.

I termini di 18 mesi (per la distruzione delle comunicazioni registrate) e 5 anni (distruzione dei dati di collegamento registrati) coincidono con i termini previsti per la distruzione delle comunicazioni e dei dati di collegamento registrati con l'esplorazione radio (cfr. art. 4 dell'ordinanza del 17 ottobre 2012 sulla condotta della guerra elettronica e sull'esplorazione radio, OCGE; RS 510.292, sottoposta a revisione totale alla fine del 2012). Come per l'esplorazione radio, anche per l'esplorazione di segnali via cavo il termine di 18 mesi corrisponde al periodo in cui una ricerca retrospettiva, ossia la ricerca tra i contenuti di comunicazioni registrate per un nuovo mandato di esplorazione di segnali via cavo o per il riorientamento di un mandato in corso promette ancora risultati rilevanti dal punto di vista informativo o è ancora rilevante per una retrospettiva (termine di 5 anni).

Articolo 29 Indennità per i gestori di reti filari e i fornitori di servizi di telecomunicazione

I gestori di reti filari e i fornitori di servizi di telecomunicazione hanno diritto a un'indennità per le prestazioni da essi fornite nell'ambito dell'esplorazione di segnali via cavo. Nell'ambito della revisione in corso della legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT; RS 780.1), è stata mantenuta la prassi attuale che non prevede un indennizzo integrale per l'utilizzo dell'infrastruttura di sorveglianza, ma solamente un'indennità appropriata nel caso di specie; questo principio viene ripreso anche per l'esplorazione di segnali via cavo. Altrimenti verrebbe a mancare segnatamente, per i gestori di reti filari e i fornitori di servizi di telecomunicazione, la motivazione a cercare soluzioni a basso costo.

Capitolo 3: Protezione dei dati e archiviazione

Sezione 1: Disposizioni particolari sulla protezione dei dati e deroghe al principio di trasparenza

Il disciplinamento previsto dal diritto vigente per la comunicazione di dati personali ha dato buone prove; esso viene pertanto ampiamente ripreso nell'ordinanza.

Articolo 32 Comunicazione di dati personali da parte delle autorità d'esecuzione cantonali

La base dell'articolo 32 è costituita in primo luogo dall'articolo 46 capoverso 3 LAIn, che disciplina il trattamento dei dati da parte dei Cantoni.

La comunicazione di dati ai sensi del capoverso 3 di questa disposizione ha carattere derogatorio ed è intesa soltanto a consentire alle autorità di intervenire rapidamente in situazioni d'emergenza o in stato di necessità. Le autorità d'esecuzione cantonali decidono sotto la propria responsabilità se sussiste una situazione di questo tipo. In virtù del capoverso 4, il SIC deve essere in seguito immediatamente informato, proprio come negli altri casi d'urgenza.

Articolo 33 Comunicazione di informazioni alle autorità di perseguimento penale

Per quanto riguarda le autorità di perseguimento penale in ambito civile basta rimandare all'articolo 12 CPP. In ambito militare, le autorità di perseguimento penale sono l'Ufficio dell'uditore in capo, la Giustizia militare e la Polizia militare, sicché anche per queste autorità esiste una base legale per lo scambio di informazioni.

Articolo 35 Deroga al principio di trasparenza

La differenza rispetto allo stato attuale consiste nel fatto che secondo l'articolo 67 LAIn la legge del 17 dicembre 2004 sulla trasparenza (LTras; RS 152.3) non si applica (più) all'accesso a documenti ufficiali riguardanti l'acquisizione di informazioni. L'ordinanza precisa che la deroga riguarda i documenti ufficiali che direttamente o indirettamente consentono di risalire all'acquisizione di informazioni ed enumera a titolo di esempio e senza pretese di esaustività tre tipici casi di applicazione (ad es. informazioni sui mezzi operativi, sui metodi e sui contatti del SIC). Per quanto riguarda i prodotti informativi menzionati alla lettera a (ad es. i rapporti al Consiglio federale) va sottolineato che essi comprendono soltanto i prodotti la cui conoscenza da parte di persone non autorizzate può nuocere agli interessi nazionali. L'enumerazione non

essendo esaustiva, la deroga può trovare applicazione anche ad altri documenti ufficiali. Potrebbe trattarsi ad esempio di documenti che contengono conclusioni di tattica investigativa tratte dalle informazioni acquisite o che consentono di risalire a ulteriori misure di acquisizione.

Sezione 2: Archiviazione

Articolo 36

Si rimanda al commento all'articolo 57*a*.

Capitolo 4: Direzione politica e divieti

Articolo 37 Tutela di altri interessi nazionali importanti

Il campo ristretto della polizia di sicurezza è coperto dalla LAIn nell'ambito di competenza del DDPS. Le domande relative alla tutela di altri interessi nazionali importanti dovrebbero perciò essere presentate principalmente da autorità esterne al DDPS. Si potrebbe ad esempio immaginare che il Dipartimento federale delle finanze (DFF) chieda l'intervento del SIC per acquisire informazioni in merito alle intenzioni di Stati esteri che per ragioni economiche si propongono di nuocere alla piazza finanziaria svizzera. La disposizione è una norma d'ordine volta a garantire che il SIC possa effettivamente intervenire in caso di richiesta.

Qualsiasi Dipartimento o Cantone può presentare una domanda per un intervento di questo tipo. A titolo di norma d'ordine, l'ordinanza prevede una consultazione preliminare del SIC per garantire che l'intervento auspicato del SIC sia anche realmente fattibile. La richiesta deve esprimersi in particolare sulla minaccia concreta in quanto tale e sulla durata dell'intervento auspicato, e conseguentemente la relativa decisione del Consiglio federale deve prevedere dei limiti di tempo per l'intervento. Se la durata dell'intervento non può essere stabilita in giorni, mesi o anni, occorrerà stabilire le scadenze alle quali l'intervento del SIC dovrà essere verificato e/o quali criteri faranno stato per il suo proseguimento o la sua cessazione. Dovranno essere concretizzati anche i mezzi informativi da impiegare. A questo riguardo ci si dovrà chiedere in primo luogo se è possibile rinunciare all'impiego di determinati mezzi informativi, quali ad esempio l'infiltrazione in sistemi informatici ubicati all'estero (art. 37 cpv. 2 LAIn) o il reclutamento di fonti umane all'estero.

Per poter sperare in un successo, i mandati che richiedono l'impiego di particolari risorse di personale e di conoscenze specifiche dovranno protrarsi per un certo tempo. Il SIC non dispone né costituirà risorse di personale o finanziarie di riserva.

Articoli 38 e 39 Procedura di controllo, sospensione della procedura di controllo

La procedura di controllo non è prevista espressamente nella LAIn. Essa è volta ad accertare se una persona, un'organizzazione o un gruppo deve essere inserito nella lista d'osservazione. A tal fine, il SIC raccoglie e tratta tutti i dati utili allo scopo; è applicabile l'articolo 5 capoverso 8 LAIn. Una volta chiarito il seguito, la procedura va sospesa. Il seguito è chiarito in sostanza quando si decide per un inserimento nella lista d'osservazione (il sospetto trova conferma) o quando gli elementi che hanno motivato la procedura di controllo vengono smentiti, e quindi non si procede all'inserimento nella lista (il sospetto non trova conferma) oppure se entro due anni dall'avvio della procedura di controllo non si ottengono ulteriori riscontri rilevanti per la sicurezza (il sospetto iniziale viene a cadere a causa del tempo trascorso). Una procedura di controllo sospesa può essere riattivata se le condizioni sono realizzate.

Articolo 41 Divieto di determinate attività

in virtù dell'articolo 73 capoverso 3 LAIn, il Dipartimento che ha richiesto il divieto verifica periodicamente se le condizioni sono ancora adempiute. L'ordinanza definisce una periodicità annuale per il controllo. Tale periodicità appare adeguata, poiché il divieto di determinate attività è pronunciato sulla base di una decisione del Consiglio federale, e dunque su un accertamento completo dei fatti e del diritto, la sua durata può essere fissata a cinque anni al massimo e può essere sottoposto a un controllo esaustivo da parte del Tribunale amministrativo federale, la cui decisione può essere impugnata dinanzi al Tribunale federale. Inoltre, si possono vietare soltanto attività che minacciano concretamente la sicurezza interna o esterna, e volte a favorire attività violente di matrice estremistica. Quindi, il divieto pronunciato nei confronti degli interessati si limita a priori ad attività indesiderate dal punto di vista della politica di sicurezza. Altre attività rimangono sempre possibili. Oltretutto, se l'autorità non ha più informazioni sicure in merito alle pertinenti attività, non se ne può dedurre necessariamente che il divieto debba essere mantenuto (ad es. perché la persona interessata ha adeguato il suo modo di comunicare o può nasconderlo alle autorità oppure incarica verbalmente terzi di provvedere alla comunicazione ecc.). La decisione riguardante il mantenimento del divieto di determinate attività deve dunque prioritariamente consistere soltanto nel verificare se e come il divieto influisce sull'attività terroristica o sull'attività violenta di matrice estremistica dei gruppi (o degli individui) che il divieto intende reprimere. Pertanto, in definitiva, un controllo a scadenza annuale sembra appropriato.

Del rimanente, la natura giuridica concreta del divieto di determinate attività è attualmente oggetto di accurati accertamenti da parte dell'Ufficio federale di giustizia.

Articolo 42 Divieto di organizzazioni

In virtù dell'articolo 74 capoverso 2 LAIn, il divieto pronunciato nei confronti di un'organizzazione deve fondarsi su una pertinente decisione delle Nazioni Unite o dell'Organizzazione per la sicurezza e la cooperazione in Europa. Secondo l'ordinanza, questo presupposto è adempiuto se l'organizzazione o il gruppo da vietare vengono espressamente menzionati nella decisione (lett. a) o gli scopi e i mezzi corrispondono a quelli di un'organizzazione o un gruppo espressamente menzionati nella decisione (lett. b). La lettera b consente al Consiglio federale di reagire tempestivamente e con la debita flessibilità al rapido mutare delle circostanze, sempreché e nella misura in cui si tratti del mutamento semplicemente formale di una minaccia riconosciuta per la sicurezza della Svizzera che in sostanza però permane (ad es. costituzione di un'organizzazione di facciata o sostituitiva). Lo stesso dicasi per quanto riguarda il controllo volto a determinare se un

divieto va prorogato oltre la scadenza: determinante sarà stabilire se l'organizzazione o il gruppo vietati sono ancora inseriti nella lista e se si profila ancora una minaccia concreta per la sicurezza interna o esterna della Svizzera qualora l'organizzazione o il gruppo oggetto del divieto potessero continuare a svolgere le loro attività.

L'impiego di esperti svizzeri nell'ambito della politica istituzionale di pace, dei diritti umani e umanitaria (ad es. osservatori elettorali) non mira a promuovere o sostenere organizzazioni o gruppi vietati, e pertanto non configura un comportamento perseguibile. Per la presenza eventualmente necessaria in territorio svizzero di persone di per sé perseguibili (ad es. per la partecipazione a negoziati di pace) va trovata, in collaborazione con le competenti autorità penali e politiche ed eventualmente con altre autorità implicate, una soluzione adeguata in base alle circostanze del caso concreto.

Capitolo 5: Prestazioni

Articolo 44 Emolumenti

Le prestazioni fornite dal SIC sono di principio soggette a emolumenti. Dato che questo principio non appare sempre adeguato, l'ordinanza stabilisce che a determinate condizioni è possibile rinunciare integralmente all'emolumento o quantomeno ridurlo, ad esempio nel caso in cui la riscossione di un emolumento genererebbe un onere superiore al costo della prestazione stessa, o se altri motivi riguardanti la prestazione o l'assoggettato all'emolumento facciano apparire sproporzionata la riscossione di un emolumento.

Capitolo 6: Controlli

Articolo 45 Autocontrollo internamente al SIC

Il capoverso 4 svolge una funzione trasversale rispetto all'ordinanza sui sistemi d'informazione e di memorizzazione del Servizio delle attività informative della Confederazione (OSIM-SIC): l'applicazione SCC (Sensor Control Center), con la quale è gestito il sistema d'informazione ISCO (cfr. art. 55 segg. OSIM-SIC), potrà essere utilizzata anche per la gestione di altri sensori (IMINT, TECHINT). I dati così ottenuti, tuttavia, non pertengono al sistema ISCO (esplorazione radio e di segnali via cavo), sicché non possono essere disciplinati nelle disposizioni particolari relative a ISCO. Dato però che né la parte generale dell'OSIM-SIC né la parte relativa a GEVER SIC si prestano per il disciplinamento dell'applicazione in questione, essa deve essere inserita nell'obbligo di autocontrollo secondo l'articolo 45 OAIn. Per il resto, il trattamento di dati personali provenienti da questa forma di acquisizione di informazioni è retto dalle disposizioni dell'OSIM-SIC.

Capitolo 7: Misure interne di protezione e di sicurezza

Per quanto riguarda le misure di protezione e di sicurezza, l'ordinanza riprende ampiamente il contenuto normativo delle collaudate prescrizioni oggi esistenti a livello di istruzioni e della prassi invalsa.

Articolo 47 Servizio preposto all'esecuzione

Il disegno di ordinanza prevede che il SIC possa far capo a terzi per controlli di effetti personali, persone e locali. Non si tratta dunque di delegare la responsabilità per l'esecuzione di una misura (la quale rimane integralmente al SIC), bensì unicamente di far capo ad «ausiliari» che agiscano sotto la responsabilità del SIC.

Articolo 48 Controlli di persone e effetti personali

La facoltà del SIC, prevista nella LAIn in quanto base legale formale, di effettuare controlli di persone e effetti personali include, nel quadro del principio di proporzionalità, la costrizione necessaria per la sua attuazione e eventualmente anche per la sua imposizione. I controlli possono dunque essere effettuati direttamente dal SIC medesimo. Se dal controllo risulta che potrebbero essere riuniti gli elementi di un crimine o delitto (ad es. furto di dati), il SIC è autorizzato, in virtù dell'articolo 218 CPP, ad arrestare provvisoriamente che è colto in flagranza di reato fino all'arrivo della polizia (arresto provvisorio), benché occorra anche in questo caso rispettare il principio della proporzionalità. La misura può essere impiegata soltanto in caso di assoluta necessità e l'uso della forza è lecito soltanto come mezzo estremo (art. 200 CPP). Se una misura meno drastica è sufficiente per assicurare una persona alla giustizia, l'arresto non è consentito. Come ulteriore misura di protezione deve essere data anche la possibilità di verificare a campione il contenuto della posta in uscita. Le norme sulla corrispondenza postale e sul traffico delle telecomunicazioni non sono violate, poiché il controllo riguarda la posta ufficiale del SIC e non la posta privata (il SIC come mittente apre la propria posta destinata alla spedizione).

Articolo 51 Impiego di apparecchi per la registrazione e la trasmissione di immagini e porto di apparecchi elettronici

I principali complementi riguardano l'impiego di apparecchi per la registrazione e la trasmissione di immagini in archivi, camere blindate e depositi e nelle aree di accesso ai locali del SIC. A questo riguardo, l'ordinanza precisa che le persone interessate devono essere informate in merito agli apparecchi per la registrazione e trasmissione di immagini per mezzo di cartelli indicatori ben visibili, e che in caso di mancato utilizzo le registrazioni devono essere cancellate il più rapidamente possibile, vale a dire di norma entro 30 giorni, a meno che la registrazione serva a documentare prove in un caso di abuso. Soltanto a questa condizione può essere conservata fino alla definitiva conclusione del relativo procedimento. Il termine di 30 giorni è adeguato, poiché, a differenza di quanto normalmente previsto per l'impiego di sistemi video, non si tratta di evitare atti vandalici bensì di impedire o accertare a posteriori furti o manipolazioni di dati, la cui scoperta richiede generalmente un certo tempo.

Capitolo 8: Dotazione di armi

Per quanto riguarda la dotazione di armi, l'ordinanza riprende ampiamente il contenuto della vigente normativa.

Articolo 53 Autorizzazione al porto di un'arma di servizio

In virtù dell'articolo 3 LAIn, il Consiglio federale designa la categoria dei collaboratori armati. Si tratta dei collaboratori del SIC che nell'esercizio della loro funzione e dei loro compiti ufficiali sono esposti a particolari pericoli. Con il rilascio dell'autorizzazione a portare un'arma di servizio il direttore del SIC conferma l'appartenenza alla corrispondente categoria. Per arma di servizio si intendono, come sinora, sostanze irritanti e armi da fuoco il cui impiego è ammesso soltanto per difesa personale e soltanto in caso di legittima difesa e stato di necessità e nel rispetto del principio di proporzionalità.

Capitolo 9: Disposizioni finali

Articolo 57a Disposizione transitoria sull'archiviazione

Per gli atti ricevuti prima dell'entrata in vigore della LAIn, il disegno di ordinanza prevede una disposizione transitoria (art. 57a), secondo la quale il termine di protezione è prorogato di 30 anni (con corrispondente informazione dell'Archivio federale) per tutti gli incarti (e quindi non solo per quelli che contengono comunicazioni di servizi di sicurezza esteri). Per i dati da fornire all'Archivio federale dopo l'entrata in vigore della LAIn, invece, si applicherà senza restrizioni il disciplinamento previsto all'articolo 68 LAIn.

Allegato 3: Comunicazione di dati personali ad autorità e servizi svizzeri

Numero 8.3.13

Fedpol riceve dal SIC anche dati personali rilevanti per la sicurezza dei passeggeri che volano su aeromobili svizzeri. Sarà la legge federale del 21 dicembre 1948 sulla navigazione aerea (LNA; RS 748.0) a definire i dati che possono essere trattati da fedpol per l'elaborazione di analisi dei rischi e della minaccia e di piani d'intervento in rapporto con l'impiego di incaricati della sicurezza nel traffico aereo, i diritti d'accesso e la comunicazione di dati (art. 21*b* segg. D-LNA, posta in consultazione nell'autunno 2015). La comunicazione di dati dal SIC a fedpol deve tuttavia essere disciplinata nell'OAIn.

Allegato 4: Abrogazione e modifica di altri atti normativi

Abrogazione:

1. Ordinanza LMSI sulle prestazioni finanziarie

Con l'adozione della LAIn, la maggior parte delle disposizioni dell'ordinanza del 1° dicembre 1999[1] sulle prestazioni finanziarie ai Cantoni per la salvaguardia della sicurezza interna (Ordinanza LMSI sulle prestazioni finanziarie) viene privata del proprio oggetto, ragion per cui le disposizioni superstiti, ossia gli articoli 3, 4 e 4*a*, vengono ora integrate nell'ordinanza del 27 giugno 2001 sui Servizi di sicurezza di competenza federale (OSF; RS 120.72), e l'articolo 5 nell'ordinanza del 30 novembre 2001 sull'adempimento di compiti di polizia giudiziaria in seno all'Ufficio federale di polizia (RS 360.1). L'ordinanza LMSI sulle prestazioni finanziarie può dunque essere abrogata.

Modifica:

2. Ordinanza sui Servizi di sicurezza di competenza federale

La modifica dell'ordinanza del 27 giugno 2001[2] sui Servizi di sicurezza di competenza federale (OSF; RS 120.72) consegue alla modifica della legge federale del 21 marzo 1997[3] sulle misure per la salvaguardia della sicurezza interna (LMSI; RS 120) operata nell'ambito dell'adozione della LAIn. Le modifiche materiali comportano inoltre adeguamenti formali.

L'articolo 2 capoverso 4 riprende il disciplinamento attualmente previsto all'articolo 3 capoverso 2 lettera a.

L'articolo 3 ha una nuova rubrica e dunque si limita alle considerazioni relative all'immediata polizia sugli edifici. Il capoverso 1 riprende dalla legge vigente (art. 23 cpv. 2 LMSI) la disposizione che stabilisce concretamente chi esercita l'immediata polizia, mentre la legge contiene ora soltanto una formulazione generale («Confederazione»). Il capoverso 2 riprende il contenuto dell'attuale capoverso 1. L'attuale capoverso 2 lettera b deve essere abrogato, poiché viene abrogata anche la pertinente base legale (attuale art. 23 cpv. 1 lett. c LMSI).

L'articolo 6 capoversi 1^{bis} e 1^{ter} e l'articolo 7 capoverso 1^{bis} vengono adeguati alla nuova base legale (art. 23 cpv. 1^{bis} LMSI). Le persone protette dal diritto internazionale pubblico sono enumerate separatamente all'articolo 6 capoverso 1^{bis} lettera c, poiché sono assoggettate ad altre basi legali, in particolare a vari trattati internazionali[4] e al diritto consuetudinario internazionale in combinato disposto con l'articolo 4 della legge del 22 giugno 2007[5] sui privilegi, le immunità e le facilitazioni, nonché sugli aiuti finanziari accordati dalla Svizzera quale Stato ospite (Legge sullo Stato ospite, LSO) e con l'articolo 24 LMSI.

Con l'abrogazione dell'ordinanza LMSI sulle prestazioni finanziarie, le disposizioni sulle indennità dovute ai Cantoni che devono in ampia misura adempiere compiti di protezione a tutela di persone ed edifici (art. 28 cpv. 2 LMSI) sono ora attuate dal DDPS. I nuovi articoli 12*a*–12*c* OSF corrispondono ai vigenti articoli 3–4*a* dell'ordinanza LMSI sulle prestazioni finanziarie.

---

1 RS **120.6**
2 RS **120.72**
3 RS **120**
4 Art. 39 Convenzione di Vienna del 18 aprile 1961 sulle relazioni diplomatiche (RS 0.191.01);
Art. 53 Convenzione di Vienna del 24 aprile 1963 sulle relazioni consolari (RS 0.191.02);
Art. 43 Convenzione dell'8 dicembre 1969 sulle missioni speciali (RS 0.191.2)
5 RS 192.12

L'*articolo 13* concretizza la nuova base legale formale introdotta agli articoli 23*a*–23*c* LMSI. Esso riguarda il sistema di informazione e documentazione del Servizio federale di sicurezza (SFS) di fedpol. L'SFS deve possedere e trattare dati sugli eventi rilevanti per la sicurezza e sulle persone ad essi collegate per poter svolgere i compiti di protezione previsti dalla sezione 5 della LMSI.

Si rinuncia invece agli attuali rimandi concreti contemplati all'*articolo 15 capoversi 2 e 3* (all'art. 23 cpv. 2 LMSI e all'art. 20 dell'ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (OLPD; RS 235.11) e all'ordinanza del 9 dicembre 2011 concernente l'informatica e la telecomunicazione nell'Amministrazione federale (Ordinanza sull'informatica nell'Amministrazione federale, OIAF; RS 172.010.58)), poiché questi atti normativi sono stati modificati o abrogati. Il rimando sulla sicurezza dei dati contenuto al *capoverso 3* comprende tutte le disposizioni rilevanti in materia di protezione dei dati. Per adeguare la normativa alle attuali circostanze, al *capoverso 2* si aggiunge che i detentori dell'immediata polizia sugli edifici presso l'SFS possono richiedere l'impiego di telecamere non solo all'interno ma anche all'esterno di un edificio per poterne sorvegliare le immediate adiacenze. La nuova norma prevista all'articolo 23*a* capoverso 3 LMSI, secondo cui i dati devono essere distrutti al più tardi cinque anni dopo la cessazione della necessità di protezione, deve essere concretamente precisata per quanto riguarda le registrazioni di immagini. Il termine sinora previsto al *capoverso 5* per la distruzione di registrazioni di immagini contenenti dati personali (al più tardi 14 giorni dopo la registrazione) si è rivelato decisamente troppo breve nei casi in cui i dati vengono sequestrati per un procedimento penale, civile o amministrativa. Secondo l'articolo 15 capoverso 4, i dati dell'SFS possono infatti essere consegnati soltanto in virtù di una decisione del giudice. Nella prassi, è praticamente impossibile che in caso di reato (ad es. furto con scasso) i fatti vengano scoperti, accertati e denunciati e che venga emanata una decisione giudiziaria entro soli 14 giorni. Il termine viene pertanto prolungato a 30 giorni. Di conseguenza, i dati non devono essere già distrutti dopo 14 giorni.

5. Ordinanza del 30 novembre 2001[6] sull'adempimento di compiti di polizia giudiziaria in seno all'Ufficio federale di polizia

Come già esposto al numero 1, l'articolo 5 dell'ordinanza LMSI sulle prestazioni finanziarie viene ora ripreso all'articolo 12bis dell'ordinanza del 30 novembre 2001 sull'adempimento di compiti di polizia giudiziaria in seno all'Ufficio federale di polizia.

7. Ordinanza del 15 ottobre 2008[7] sul sistema di ricerca informatizzato della polizia

In virtù dell'articolo 5 lettera j dell'ordinanza del 15 ottobre 2008[8] sul sistema di ricerca informatizzato della polizia (ordinanza RIPOL), per contrastare i pericoli per la pubblica sicurezza il SIC può accedere a RIPOL, conformemente alla LAIn, per accertare il luogo in cui si trovano persone e veicoli e ora anche per la sorveglianza discreta o per il controllo mirato di persone e veicoli. Questa modifica è dovuta all'adeguamento dell'articolo 15 capoverso 4 lettera i della legge federale del 13 giugno 2008 sui sistemi d'informazione di polizia della Confederazione (LSIP; RS 361).

8. Ordinanza dell'8 marzo 2013[9] sulla parte nazionale del Sistema d'informazione di Schengen (N-SIS) e sull'ufficio SIRENE (Ordinanza N-SIS)

In virtù dell'articolo 7 lettera h dell'ordinanza N-SIS, ai fini dell'esecuzione della LAIn le unità competenti del SIC possono accedere ai dati del SIS per accertare il luogo in cui si trovano persone e veicoli e ora anche per procedere alla sorveglianza discreta o al controllo mirato di persone e veicoli.

3 Commento alle disposizioni della OSIM-SIC

Struttura

Il disegno riprende sostanzialmente la struttura della vigente ordinanza dell'8 ottobre 2014[10] sui sistemi d'informazione del Servizio delle attività informative della Confederazione (OSIC-SIC). Per ragioni di trasparenza, le disposizioni generali sono state però suddivise tra disposizioni generali sul trattamento e l'archiviazione dei dati e disposizioni sulla protezione e la sicurezza dei dati.

Le disposizioni particolari sui sistemi d'informazione del SIC sono raccolte nelle sezioni 4-12. La sezione 13 disciplina i sistemi di memorizzazione e la sezione 14 contiene le disposizioni finali. Il catalogo dei dati personali e i diritti individuali di accesso ai sistemi d'informazione e memorizzazione sono disciplinati negli allegati 1-18.

6 RS **360.1**
7 **RS 361.0**
8 **RS 361.0**
9 **RS 362.0**
10 RS **121.2**

Sezione 1: Oggetto e definizioni

Art. 1 Oggetto

L'articolo 1 enumera i sistemi di informazione e memorizzazione disciplinati nel presente disegno di ordinanza. I sistemi di informazione hanno una base legale formale agli articoli 47 segg. LAIn, i sistemi di memorizzazione all'articolo 36 capoverso 5 e all'articolo 58 della stessa legge.

Art. 2 Definizioni

I termini utilizzati riprendono in larga misura quelli previsti dalla vigente OSI-SIC.

La definizione di «terzi» è stata resa più comprensibile, ma dal punto di vista del contenuto rimane immutata. Il ricorso a terzi per il rilevamento, come sinora avveniva nel Sistema di informazione per la sicurezza interna (ISIS), è previsto in futuro nel Sistema di analisi integrale dell'estremismo violento (IASA-GEX SIC).

La funzione SIDRED e la rete SiLAN sono oggi descritte agli articoli 4 e 10 OSI-SIC.

Sezione 2: Disposizioni generali concernenti il trattamento dei dati e l'archiviazione

Art. 3 Archiviazione dei dati

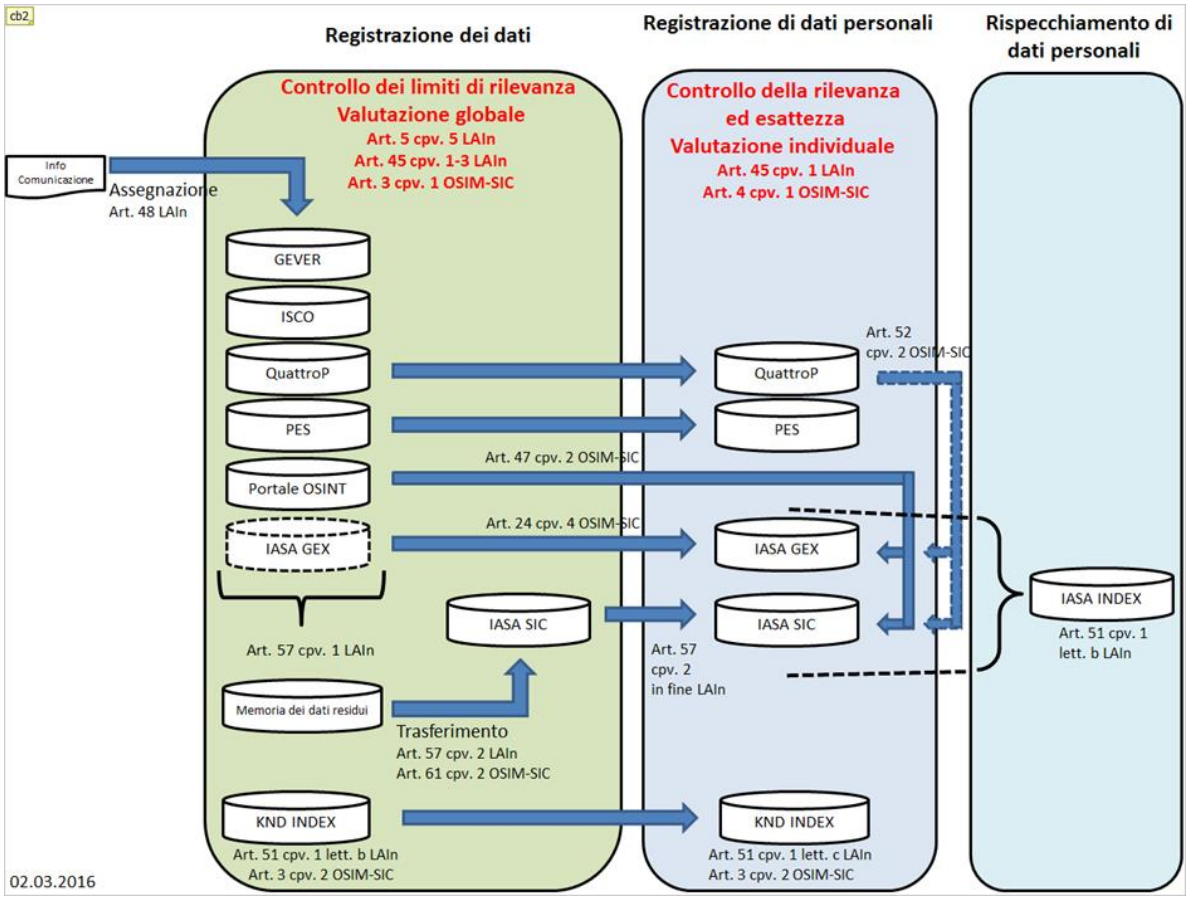
Secondo il capoverso 1, i collaboratori addetti allo smistamento sono tenuti, nell'assegnare i dati ai sistemi d'informazione del portale OSINT e della memoria dei dati residui, a esaminare se vi sono sufficienti indizi per stabilire il necessario nesso con i compiti di cui all'articolo 6 LAIn. Le comunicazioni riguardanti più dati personali vengono considerate come un tutt'uno. Essendo responsabili dello smistamento iniziale di tutti i dati che pervengono al SIC in modo non automatico, i collaboratori addetti allo smistamento non possono esaminare in modo approfondito ogni singola comunicazione. Sono però in grado, ad esempio, di valutare perfettamente le fonti da cui provengono i dati e di procedere al predetto esame in base all'oggetto della segnalazione. Parte delle comunicazioni che pervengono è costituita da risposte o risultati di mandati, e questo aspetto ne facilita senz'altro la valutazione. Inoltre, secondo la sistematica del presente disegno d'ordinanza, soltanto i dati archiviati non possono essere utilizzati o trasmessi prima di essere inseriti nel Sistema di analisi integrale (IASA SIC) o in IASA-GEX SIC, approfonditamente esaminati e registrati in modo strutturato. Se dovessero avere qualche esitazione, i collaboratori addetti allo smistamento iniziale sono tenuti a esaminare le comunicazioni in arrivo anche a livello di contenuto, facendo capo eventualmente anche ai collaboratori addetti alla registrazione dei dati o a specialisti di altri settori. Come già oggi avviene, in caso di esito negativo dell'esame i dati devono essere distrutti, o restituiti se provengono da un'autorità cantonale d'esecuzione.

Allo stesso esame devono procedere anche le autorità d'esecuzione cantonali quando archiviano dati in INDEX SIC (cfr. cpv. 2).

La tecnica OCR corrisponde al diritto vigente. A patto che vengano rispettate determinate condizioni, è d'accordo con questa scelta anche la Delegazione delle Commissioni della gestione (DelCG), la quale esige ad esempio che il diritto d'accesso alle informazioni sulla propria persona sia applicato senza restrizioni a tutte le persone che risultano in ISIS da una ricerca a testo libero, e che quando una persona viene cancellata da IASA/IASA-GEX vengano cancellati anche tutti i passaggi di testo che la riguardano nelle comunicazioni in cui può essere eseguita la ricerca. Inoltre, la ricerca nel testo non deve comprendere comunicazioni riguardanti l'attività politica di persone, tranne se si sospetta che tali attività vengano esercitate abusivamente allo scopo di agire ai danni dello Stato. La possibilità di effettuare ricerche in documenti originali con l'ausilio di metodi di riconoscimento ottico dei caratteri (tecnica OCR) e di distruggere documenti cartacei digitalizzati e registrati come documenti originali corrisponde al diritto vigente (cfr. cpv. 3 e 4 del presente disegno e art. 5 OSI-SIC).

Art. 4 Valutazione individuale e registrazione di dati personali

Secondo l'articolo 45 capoversi 1 e 2 LAIn, prima di registrare dati personali in un sistema d'informazione il SIC deve valutarne la rilevanza e l'esattezza, come pure l'esistenza di un nesso con i compiti di cui all'articolo 6 LAIn. Quest'obbligo ora non riguarda più soltanto i collaboratori del SIC addetti alla registrazione dei dati (cfr. cpv.1), ma anche i collaboratori delle autorità d'esecuzione cantonali che registrano accertamenti preliminari in INDEX SIC (cfr. cpv. 2). Di conseguenza, questi ultimi dovranno ora essere anche adeguatamente formati. In caso di esito negativo dell'esame, i dati dovranno come sinora essere distrutti, o restituiti se provengono da un'autorità cantonale d'esecuzione.



Art. 5 Concessione e revoca di diritti d'accesso

Come nel diritto vigente (cfr. art. 3 OSI-SIC), i diritti d'accesso ai vari sistemi d'informazione vengono accordati soltanto su richiesta individuale e limitatamente a determinati individui (cfr. cpv. 1). Questo principio si applica ora anche per i sistemi di memorizzazione di cui all'articolo 1 capoverso 2 del presente disegno d'ordinanza. Nel caso di PES l'accesso può essere disciplinato anche in base alla funzione, poiché è una caratteristica propria di questa banca dati che in caso di eventi particolari debba essere prontamente accessibile a una cerchia di persone di cui non è possibile conoscere il nome in anticipo. Inoltre, il personale dei servizi di picchetto esterni che devono poter accedere a PES cambia continuamente. In tale ambito è semplicemente impensabile, con un impiego ragionevole di risorse, accordare il diritto d'accesso a livello individuale. L'individualizzazione avviene però a livello funzionale. Il profilo di accesso, che inizialmente viene rilasciato soltanto per la funzione interessata, è poi assegnato a un determinato individuo al momento dell'utilizzo. L'organizzazione utente è tenuta a documentare i nomi delle persone che hanno acceduto a PES e i relativi momenti. L'obbligo di documentazione garantisce così che gli accessi possano così essere ricostruiti in qualsiasi momento.

Ora il disciplinamento prevede esplicitamente che la richiesta debba comprendere non solo le generalità del richiedente e la sua funzione, ma anche indicare il riferimento a un utilizzo sancito dalla LAIn (cfr. cpv. 2). Questa regola corrisponde alla vigente prassi e costituisce un presupposto indispensabile affinché la richiesta venga formalmente esaminata.

Ora l'esame formale delle richieste di accesso non spetterà più al responsabile del settore di direzione (cfr. cpv. 3). I diritti d'accesso in tutto il SIC e per tutti i sistemi di informazione e di memorizzazione dovranno dunque essere centralizzati, e assegnati secondo gli stessi criteri. La nuova normativa prevede inoltre esplicitamente che il diritto di accesso venga revocato se non viene più utilizzato da sei mesi (cfr. cpv. 4). Già oggi la Gestione delle applicazioni del SIC è incaricata di svolgere questo compito.

Al capoverso 5 l'articolo precisa che il SIC è competente soltanto per l'attuazione dei diritti d'accesso ai sistemi di informazione da esso gestiti.

Art. 6 Accesso trasversale e valutazione temporanea

Le autorizzazioni trasversali disciplinate ai capoversi 1 e 2 (riguardanti l'accesso a tutti i sistemi d'informazione), per la registrazione in più sistemi (riguardanti soltanto IASA SIC e IASA-GEX SIC) e per la ricerca e distribuzione di informazioni corrispondono al diritto vigente (cfr. art. 4 OSI-SIC). I sistemi di memorizzazione di cui all'articolo 1 capoverso 2 OSIM-SIC ne sono deliberatamente esclusi, poiché sono a disposizione esclusiva degli specialisti competenti e non devono essere collegati con i sistemi d'informazione del SIC.

Il capoverso 3 specifica che, per coordinare l'acquisizione di informazioni o ai fini dell'analisi operativa nell'ambito di progetti di durata limitata (task force, gruppi di lavoro ecc.), i dati dei sistemi d'informazione e di memorizzazione del SIC possono essere copiati provvisoriamente, archiviati separatamente in SiLAN e resi accessibili soltanto ai membri del

progetto interessato. Questa possibilità può essere indicata per adempiere l'obbligo di protezione delle fonti disposta all'articolo 35 LAIn e corrisponde alla prassi attuale e al concetto del SIC per la gestione dei dati. Queste valutazioni temporanee devono essere autorizzate dal SIC, e precisamente dal servizio interno designato nel concetto per la protezione dei dati. Al termine dei lavori, tutti i risultati vengono trasferiti nei sistemi d'informazione ordinari del SIC e le copie dei dati sulla piattaforma di valutazione temporanea vengono distrutti.

Il servizio del SIC incaricato dei controlli di qualità includerà queste valutazioni e la verifica del loro carattere indispensabile nella propria attività di controllo a campione.

Gli archivi temporanei vengono creati ad esempio nei casi di rapimento. I collaboratori che trattano il caso devono fare in modo che tutte le informazioni relative al rapimento tratte dai sistemi d'informazione del SIC possano essere raccolte e valutate insieme su un'unica piattaforma. Al termine dei lavori tutti i risultati vengono trasferiti nei sistemi d'informazione ordinari del SIC e le copie dei dati sulla piattaforma di valutazione temporanea vengono cancellati.

Art. 7 Dati relativi alle operazioni

Per ragioni inerenti alla protezione delle fonti ai sensi dell'articolo 35 LAIn o per proteggere lo svolgimento di un'operazione, è opportuno tenere separati i dati relativi alle operazioni (ad es. informazioni necessarie operativamente su fonti umane del SIC e sulla loro identità e selezione, sulla valutazione dei rischi, sulla gestione delle fonti ecc.), gestendoli esternamente ai sistemi d'informazione del SIC (cfr. cpv. 1). La gestione separata di questi dati delicati assicura che siano accessibili soltanto a un numero ridottissimo di persone, ossia la persona incaricata di gestire un'operazione o il suo sostituto (cfr. cpv. 3). Per questi dati non esistono possibilità di ricerca online.

Per motivi di sicurezza, questi dati vengono conservati in contenitori o locali particolarmente protetti (ad es. in cassaforte o in luoghi con restrizioni di accesso) (cfr. cpv. 2).

Le indicazioni di intelligence fornite dalle fonti umane vengono anonimizzate e aggiunte sotto forma di rapporti HUMINT agli altri dati rilevanti per le attività informative (IASA SIC o IASA-GEX SIC) (cfr. cpv. 4). Il diritto d'accesso delle persone interessate viene dunque garantito basandosi, da un lato, su questi sistemi e, dall'altro, sulle piattaforme che contengono i dati relativi alle operazioni.

La persona responsabile del settore di direzione Acquisizione ha l'obbligo di verificare periodicamente se alla luce delle circostanze attuali i dati sono ancora necessari per l'adempimento dei compiti del SIC ai sensi dell'articolo 6 LAIn (cfr. cpv. 5).

Come secondo il diritto vigente, questi dati possono essere conservati al massimo per 45 anni (cfr. cpv. 6).

Art. 8 Cancellazione dei dati

Le disposizioni di questo articolo corrispondono al diritto attualmente vigente (cfr. art. 7 OSI-SIC).

La durata massima di conservazione è disciplinata per i singoli sistemi di informazione e memorizzazione e varia a seconda dell'origine dei dati, dello scopo del trattamento e del settore di compiti (cfr. cpv. 1).

In IASA SIC e IASA-GEX SIC, gli oggetti devono essere cancellati quando non sono più collegati ad altre informazioni (metadocumenti), affinché non rimangano registrate persone su cui non si hanno altre informazioni e di cui non si può più sapere per quale motivo siano state registrate in passato (cfr. cpv. 2).

Come nell'attuale sistema ISIS, anche in IASA-GEX SIC si possono archiviare documenti originali soltanto se sono registrati in modo strutturato con metadocumenti e oggetti (cfr. il disciplinamento ora esplicito di cui all'art. 24 cpv. 4 del presente disegno). Inversamente, la cancellazione dell'ultimo metadocumento comporta obbligatoriamente la cancellazione del documento originale referenziato (cfr. cpv. 3), poiché il controllo delle registrazioni previsto per i dati contenuti in IASA-GEX SIC è possibile unicamente se i documenti originali sono registrati in modo strutturato.

Questa prescrizione non è prevista per IASA SIC, dove se necessario si possono conservare – fino alla durata massima prevista – anche documenti originali non referenziati (cfr. cpv. 4).

Non presenta novità di contenuto neppure il capoverso 5, il quale precisa però chiaramente che possono essere versati nel modulo di archiviazione soltanto i dati cancellati e destinati all'archiviazione, e che i dati cancellati non devono però essere consegnati all'Archivio federale (ad es. registrazioni sbagliate, informazioni già consegnate da altri uffici, informazioni trasferite in un altro sistema di informazione e da questo consegnate ecc.) non devono essere versati nel modulo di archiviazione e devono essere distrutti.

Art. 9 Archiviazione

L'offerta all'Archivio federale di dati provenienti dai sistemi d'informazione del SIC è disciplinata esaustivamente all'articolo 68 LAIn.

Se l'adempimento dei compiti ai sensi dell'articolo 6 capoverso 1 LAIn lo richiede, i dati provenienti dagli accertamenti preliminari e i dati delle autorità d'esecuzione cantonali sulla gestione dei mandati confluiscono in IASA SIC, IASA-GEX SIC, INDEX SIC o nel Sistema d'informazione per la gestione degli affari del SIC (GEVER) e vengono consegnati tramite questi sistemi (cfr. cpv. 2). Una doppia consegna non avrebbe alcun senso.

Sezione 3: Disposizioni generali concernenti la protezione dei dati e la sicurezza dei dati

Art. 10 Diritto d'accesso delle persone interessate

Il diritto d'accesso delle persone interessate è disciplinato esaustivamente all'articolo 63 LAIn.

Art. 11 Controllo della qualità

L'articolo 11 del presente disegno d'ordinanza rappresenta la disposizione cardine per il controllo della qualità dei dati del SIC. Secondo l'articolo 45 capoverso 4 LAIn, il SIC è tenuto a verificare periodicamente in tutti i sistemi d'informazione se gli insiemi di dati personali registrati sono ancora necessari per l'adempimento dei suoi compiti. Il fatto che questa mansione venga svolta principalmente dai servizi incaricati della registrazione, vale a dire da specialisti, consente di integrare maggiormente nel controllo della qualità le conoscenze specifiche, ad esempio in materia di analisi. Questa integrazione delle conoscenze specifiche in materia di analisi nel controllo della qualità dei dati risponde a un'esplicita richiesta presentata dalla DelCG nel rapporto del 2010 sul trattamento dei dati nel Sistema di trattamento dei dati relativi alla protezione dello Stato ISIS ed è già stata avallata dal Consiglio federale, nell'ambito della revisione della LSIC, per il controllo dei dati del SIC provenienti dall'estero. Le competenze, i termini e l'estensione dei controlli periodici sono disciplinati nelle disposizioni speciali concernenti i singoli sistemi d'informazione (cfr. cpv. 1).

Il capoverso 2 corrisponde nel principio all'attuale articolo 13 capoverso 4 OSI-SIC, ma l'obbligo di effettuare verifiche a campione viene esteso a tutti i sistemi d'informazione (attualmente ne sono esclusi sia il sistema ISIS sia il Sistema d'informazione Sicurezza esterna ISAS). A differenza di quanto previsto per i controlli periodici, che incombono principalmente ai servizi incaricati della registrazione, la verifica a campione è di spettanza esclusiva dell'organo di controllo della qualità del SIC. Questa verifica non include tutti i dati dei sistemi d'informazione, bensì soltanto una scelta di dati selezionati. L'esito delle verifiche a campione confluisce in raccomandazioni e corsi, destinati in particolar modo ai servizi incaricati della registrazione dei dati.

Attualmente l'organo di controllo della qualità del SIC verifica già, dopo l'approvazione della lista d'osservazione da parte del Consiglio federale, i record di dati su organizzazioni e gruppi radiati dalla lista e cancella i dati che ricadono nel campo d'applicazione dei limiti di trattamento di cui all'articolo 3 della legge federale del 21 marzo 1997[11] sulle misure per la salvaguardia della sicurezza interna (LMSI). Queste verifiche verranno ancora effettuate anche sotto il regime della LAIn. Ora riguarderanno anche IASA-GEX SIC e IASA SIC, come disposto esplicitamente al capoverso 3. I limiti di trattamento finora previsti all'articolo 3 LMSI saranno disciplinati in futuro all'articolo 5 capoverso 5 LAIn.

Se in via eccezionale vengono acquisiti dati ai sensi dell'articolo 5 capoverso 5 LAIn al di fuori della lista d'osservazione o di una procedura di controllo, e questi dati vengono registrati con riferimenti a persone, occorre garantire che essi vengano cancellati se vengono escluse attività elencate all'articolo 5 capoverso 6 LAIn, o se entro un anno dalla registrazione non è stato possibile comprovare alcuna di queste attività. Pertanto, l'organo di controllo della qualità del SIC viene ora incaricato di controllare almeno una volta l'anno – e se del caso cancellare – i record di dati contenenti dati di questo tipo (cfr. cpv. 4). Secondo il diritto attualmente vigente, questa verifica veniva effettuata soltanto nell'ambito delle valutazioni globali.

Il ruolo più completo dell'organo di controllo della qualità del SIC viene ulteriormente rafforzato affidando a tale organo il compito di provvedere, con corsi interni e controlli regolari, al rispetto delle disposizioni della presente ordinanza (cfr. cpv. 5).

Come già previsto dal vigente diritto, il direttore del SIC ha la possibilità di affidare all'organo di controllo della qualità il compito di effettuare ulteriori verifiche all'interno dei sistemi d'informazione e di memorizzazione (cfr. cpv. 6).

Art. 12 Responsabilità e competenze

Responsabilità e competenze rimangono immutate. La presente disposizione corrisponde all'attuale articolo 13 capoversi 1-3 OSI-SIC, pur senza presentare un eccessivo grado di dettaglio riguardo ai regolamenti per il trattamento.

Art. 13 Sicurezza dei dati

Non cambiano, rispetto ad oggi, neppure le disposizioni concernenti la sicurezza dei dati, le quali corrispondono al disciplinamento attualmente previsto all'articolo 8 OSI-SIC.

Art. 14 SiLAN

Non subiscono alcun cambiamento rispetto ad oggi neppure l'utilizzo e la gestione di SiLAN. Secondo il capoverso 2, in SiLAN possono essere ancora trattati dati di tutti i livelli di classificazione.

Ora avranno accesso a SiLAN anche i collaboratori delle autorità d'esecuzione cantonali, che potranno effettuarvi i loro accertamenti preliminari (KND INDEX) e gestire i loro rapporti e mandati in un ambiente TIC particolarmente protetto (cfr. cpv. 3). Questa concessione si è resa necessaria in virtù del fatto che secondo l'articolo 46 LAIn i servizi informazioni cantonali (SICant) non possono più gestire alcuna collezione di dati propria. Essa non genera tuttavia maggiori oneri finanziari.

Art. 15 Trasmissione dei dati al di fuori di SiLAN

Anche questa disposizione corrisponde ampiamente al diritto vigente (cfr. art. 11 OSI-SIC).

Ora occorre però finanziare l'accesso dei Cantoni a SiLAN e ai dati in esso gestiti, e non più la trasmissione dei dati a loro destinati (cfr. cpv. 2).

Sezione 4: Disposizioni particolari relativi a IASA SIC

Art. 16 Struttura

La struttura di IASA SIC corrisponde a quella attuale dei sistemi ISAS e ISIS. L'indice in cui accertare se il SIC tratta in IASA SIC dati su una persona fisica o giuridica, un evento o una cosa è ora disciplinato separatamente nella sezione 6 concernente le disposizioni particolari relative a INDEX SIC.

[11] RS **120**

Art. 17 Dati

IASA SIC riprende largamente la funzione degli attuali sistemi d'informazione ISIS e ISAS. Esso serve dunque per la registrazione di dati di intelligence, la ricerca e l'analisi di dati su persone fisiche e giuridiche, cose ed eventi provenienti da tutti i settori di compiti del SIC – eccettuati quelli relativi all'estremismo violento – e ai relativi controlli di qualità (cfr. cpv. 1).

I capoversi 2, 4 e 5 corrispondono al diritto attualmente vigente e sono stati ripresi dai capoversi 2, 3 e 4 dell'articolo 16 OSI-SIC. Inoltre, possono ancora essere visualizzati graficamente e memorizzati gli oggetti e i metadocumenti nonché le reciproche relazioni. Il catalogo dei dati personali figura nell'allegato 1. I campi di dati continueranno a essere definiti dal Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) (cfr. la vigente ordinanza del DDPS del 27.7.2015[12] concernente i campi di dati e i diritti d'accesso dei sistemi d'informazione ISAS e ISIS).

Il capoverso 3 è ripreso dall'articolo 6*c* capoverso 2 LSIC. Già oggi è possibile trattare nel sistema ISAS (e nel sistema ISIS) anche dati personali degni di particolare protezione e profili della personalità. Questa possibilità sarà mantenuta anche in futuro (cfr. art. 44 cpv. 1 LAIn).

Art. 18 Registrazione dei dati

Secondo l'articolo 45 capoverso 1 e 2 LAIn e l'articolo 4 capoverso 1 del presente disegno di ordinanza, prima della registrazione di dati nei sistemi d'informazione del SIC, i competenti collaboratori del SIC (e delle autorità d'esecuzione cantonali) devono valutare il nesso con i compiti secondo l'articolo 6 LAIn, la rilevanza e l'esattezza dei dati personali da registrare e rispettare i limiti posti al trattamento dei dati dall'articolo 5 capoverso 5 LAIn. Questa regola si applica in particolare anche per la registrazione di dati personali in IASA SIC (cfr. cpv. 1).

Inoltre, per facilitare l'analisi dei dati e i successivi controlli di qualità, occorre contrassegnare i dati valutati come disinformazione o informazione falsa, ma questi dati devono comunque essere registrati, poiché sono necessari per la valutazione della situazione o di una fonte (cfr. cpv. 2 lett. a e art. 44 cpv. 2 LAIn). Per la stessa ragione devono essere contrassegnate anche le informazioni rilevate in via eccezionale in virtù dell'articolo 5 capoverso 6 LAIn (cfr. lett. b) e le informazioni rilevate sulla base della lista d'osservazione di cui all'articolo 72 LAIn o di una procedura di controllo (cfr. lett. c).

Art. 19 Diritti d'accesso

I diritti d'accesso a IASA SIC sono retti dall'articolo 49 capoverso 3 LAIn, sicché il capoverso 1 rinvia semplicemente a tale disposizione. Essi corrispondono agli attuali diritti d'accesso ai sistemi ISIS e ISAS, mentre le autorizzazioni d'accesso a INDEX SIC sono ora disciplinate separatamente nella sezione 6 concernente le disposizioni particolari relative a tale indice.

Come già previsto dal diritto vigente, il capoverso 2 rimanda, per un catalogo dei diritti d'accesso individuali, all'allegato 2.

Art. 20 Verifica periodica dei dati personali

Al capoverso 1 viene ripreso l'obbligo di verifica periodica dei dati personali previsto dal diritto vigente per il sistema ISAS (cfr. art. 18 cpv. 1 OSI-SIC). L'unica differenza consiste nel fatto che ora (come nell'intero disegno di ordinanza) si parla, anziché di persone o di organizzazioni, di persone fisiche e giuridiche. I settori specialistici responsabili della registrazione dei dati rimangono competenti, ciascuno nel proprio ambito specifico, per l'esecuzione delle verifiche periodiche dei dati memorizzati in IASA SIC, ciò che, come già evocato, garantisce un maggior coinvolgimento delle conoscenze specialistiche nel controllo della qualità.

Non mutano, rispetto ad oggi, neppure i compiti che devono essere svolti in questo contesto dalle persone incaricate delle verifiche (cfr. cpv. 2 e art. 18 cpv. 2 OSI-SIC). La nuova ordinanza chiarisce tuttavia che l'esito della verifica deve essere registrato soltanto se un record di dati è stato rettificato o non completamente cancellato. Se un record di dati non viene rettificato, la verifica effettuata viene automaticamente registrata dal sistema.

Il disciplinamento attualmente previsto all'articolo 18 capoverso 3 OSI-SIC, secondo cui la verifica periodica dev'essere eseguita ogni qual volta si proceda al completamento di un record di dati, ha provocato nella prassi un improduttivo assorbimento di risorse e inutili ripetizioni, in particolare quando uno stesso record di dati veniva completato e verificato più volte al giorno da diversi collaboratori. Per rimediare a queste insufficienze e considerato che in avvenire i dati del sistema ISIS saranno trattati in gran parte in IASA SIC, il disegno di ordinanza riprende, per la verifica periodica, le regole attualmente vigenti per il sistema ISIS (cfr. art. 25 OSI-SIC). Ciò significa che i record di dati devono essere verificati al più tardi entro la scadenza dei termini massimi previsti dalla registrazione in un sistema d'informazione o dall'ultima verifica periodica (cfr. cpv. 3). I termini massimi sono invece stati ripresi dalle disposizioni attualmente vigenti per ISAS (art. 18 cpv. 3 OSI-SIC: 10 anni per i dati sul terrorismo internazionale, 15 anni per i dati relativi allo spionaggio e alla proliferazione delle armi di distruzione di massa, 20 anni per le altre informazioni rilevanti in materia di politica di sicurezza). Il capoverso 4 prevede ora espressamente che per i record di dati contenenti metadocumenti provenienti da diversi ambiti (e quindi sottoposti a termini massimi diversi) si applica il termine massimo più breve.

Art. 21 Durata di conservazione

I termini di conservazione per i dati registrati in IASA SIC corrispondono esattamente a quelli attualmente previsti per ISAS (cfr. art. 19 OSI-SIC).

[12] RS **121.22**

Sezione 5: Disposizioni particolari relative a IASA-GEX SIC

Art. 22 Struttura

La struttura di IASA-GEX SIC corrisponde a quella attuale dei sistemi ISAS e ISIS. L'indice in cui accertare se il SIC tratta in IASA-GEX SIC dati su una persona fisica o giuridica è ora disciplinato separatamente nella sezione 6 concernente le disposizioni particolari relative a INDEX SIC.

Art. 23 Dati

IASA-GEX SIC contiene dati che per la maggior parte provengono dall'attuale sistema ISIS. Esso serve per la registrazione di dati di intelligence, la ricerca, l'analisi e il controllo della qualità di dati su persone fisiche e giuridiche, cose ed eventi relativi all'ambito dell'estremismo violento. I dati personali trattati in IASA-GEX SIC hanno un nesso con i gruppi designati dal Consiglio federale secondo l'articolo 70 capoverso 1 lettera c LAIn (cfr. cpv. 1 lett. a) oppure concernono persone fisiche o giuridiche che negano la democrazia, i diritti dell'uomo e lo Stato di diritto e che allo scopo di raggiungere i loro obiettivi commettono, incoraggiano o approvano atti violenti (cfr. cpv. 1 lett. b). Se una persona fisica o giuridica presenta un nesso soltanto indiretto con l'estremismo violento così definito, i suoi dati possono essere contrassegnati in IASA-GEX SIC come dati concernenti terzi (cfr. art. 2 lett. g OSIM-SIC) e saranno quindi cancellati in occasione della prima verifica periodica (cfr. art. 27 cpv. 4 OSIM-SIC).

I capoversi 2 - 5 sono ripresi dall'articolo 22 capoverso 3 e 4 e dall'articolo 23 capoverso 3 OSI-SIC e corrispondono dunque al diritto vigente. I campi di dati saranno disciplinati anche in futuro dal DDPS.

Art. 24 Registrazione dei dati

Il capoverso 1, ripreso senza modifiche dall'attuale articolo 23 capoverso 1 OSI-SIC, dispone che prima di registrare una nuova informazione i collaboratori del SIC dovranno anche in futuro sottoporla obbligatoriamente a una valutazione che confermi o smentisca la rilevanza della persona fisica o giuridica in questione per l'adempimento dei compiti informativi secondo la LAIn. In caso di smentita, il record di dati deve essere cancellato da IASA-GEX SIC.

Come sinora, per facilitare l'analisi dei dati, il successivo controllo delle registrazioni e i controlli di qualità, i collaboratori competenti per la registrazione dei dati devono valutare i dati registrati e contrassegnarli opportunamente (cfr. cpv. 2). Questo compito viene svolto (come in IASA SIC) a livello di metadocumento e riguarda le informazioni di dubbia attendibilità, le informazioni rilevate sulla base della lista d'osservazione di cui all'articolo 72 LAIn o di una procedura di controllo secondo l'articolo 38 OAIn e ora anche quelle valutate come disinformazione o informazione falsa e quelle rilevate in via eccezionale sulla base dell'articolo 5 capoverso 6 LAIn.

Come già esposto, gli oggetti concernenti persone fisiche o giuridiche che presentano un nesso soltanto indiretto con l'estremismo violento devono essere contrassegnati come dati riguardanti terzi. Gli oggetti concernenti persone fisiche o giuridiche non appartenenti a un gruppo designato dal Consiglio federale secondo l'articolo 70 capoverso 1 lettera c LAIn devono essere anch'essi appositamente contrassegnati, affinché il Consiglio federale possa essere informato annualmente in merito al numero di questi oggetti (cfr. cpv. 3). Si possono creare soltanto oggetti relativi a persone fisiche e giuridiche di cui si suppone che rappresentino un pericolo per la sicurezza della Svizzera.

Il capoverso 4 prevede ora esplicitamente che in IASA-GEX SIC si possono archiviare documenti originali soltanto se sono correlati in modo strutturato con metadocumenti e oggetti. Questa regola si applica già oggi per il sistema ISIS, ma ha potuto essere derivata soltanto dalle disposizioni sulla cancellazione di dati nel sistema ISIS (cfr. art. 7 cpv. 4 OSI-SIC). La ragione di questa circostanza è legata al controllo delle registrazioni previsto per IASA-GEX SIC, che può essere eseguito soltanto se i dati personali rilevanti dei documenti originali vengono registrati in modo strutturato (ossia con metadato, oggetto e relazioni).

Come attualmente previsto per il sistema ISIS, i dati in IASA-GEX SIC vengono registrati dapprima provvisoriamente e quindi diventano definitivi soltanto dopo il controllo della registrazione (cfr. cpv. 5).

Se un documento originale contiene dati su persone fisiche o giuridiche per le quali non è ancora stato creato un oggetto in IASA-GEX SIC, questi dati possono essere utilizzati o trasmessi soltanto dopo aver creato gli oggetti corrispondenti nel sistema e averli sottoposti al controllo delle registrazioni (cfr. cpv. 6). Questa regola è già prevista attualmente per il sistema ISIS all'articolo 23 capoverso 5 OSI-SIC.

Art. 25 Controllo della registrazione

Questa disposizione è stata ripresa senza modifiche dall'articolo 24 OSI-SIC. È stato aggiornato soltanto il rimando ai limiti posti al trattamento dei dati, poiché tali limiti sono ora disciplinati all'articolo 5 capoverso 5 LAIn. Il controllo della registrazione viene dunque mantenuto nella forma attualmente prevista per il sistema ISIS. I dati che l'organo di controllo della qualità del SIC non ha confermato devono essere distrutti e il servizio che ha registrato i dati deve esserne informato, affinché la qualità delle registrazioni possa essere costantemente migliorata (cfr. cpv. 3).

Art. 26 Diritto d'accesso

I diritti d'accesso a IASA-GEX SIC sono retti dall'articolo 50 capoverso 3 LAIn, sicché il capoverso 1 rimanda semplicemente a tale disposizione. Essi corrispondono agli attuali diritti d'accesso al sistema ISIS, mentre le autorizzazioni d'accesso a INDEX SIC sono ora disciplinate separatamente nella sezione 6 concernente le disposizioni particolari relative a tale indice.

Come già previsto dal diritto vigente, il capoverso 2 rimanda, per un catalogo dei diritti d'accesso individuali, all'allegato 2.

Art. 27 Verifica periodica dei dati personali

Lo strumento della verifica periodica viene ripreso senza modifiche dalle disposizioni vigenti per il sistema ISIS (cfr. art. 25 OSI-SIC). L'organo di controllo della qualità del SIC verifica i record di dati al più tardi cinque anni dopo la registrazione iniziale in un sistema d'informazione del SIC. Successivamente esegue almeno ogni tre anni una verifica periodica dei record di dati.

Per ragioni di trasparenza, il capoverso 2 precisa ora in dettaglio i punti che l'organo di controllo della qualità del SIC deve verificare e dispone che esso deve registrare il risultato della verifica. La verifica corrisponde, per contenuto ed estensione, a quella della valutazione globale prevista attualmente per il sistema ISIS.

Come previsto attualmente per il sistema ISIS (cfr. art. 25 cpv. 3 OSI-SIC), i dati contrassegnati come non attendibili possono continuare a essere utilizzati fino alla successiva verifica periodica soltanto a condizioni ben precise, enumerate esaustivamente nel disegno di ordinanza (cfr. cpv. 3). A richiesta dell'autorità di vigilanza in materia di attività informative, il termine di conservazione dei dati non attendibili è stato armonizzato con i ritmi della verifica periodica e ora è di cinque anni.

Gli oggetti contrassegnati come dati concernenti terzi devono anch'essi essere cancellati in occasione della prima verifica periodica (cfr. cpv. 4). Il termine massimo di conservazione è dunque di cinque anni. Anche questa armonizzazione con i ritmi della verifica periodica tiene conto di un suggerimento dell'autorità di vigilanza in materia di attività informative.

Art. 28 Durata di conservazione

I termini di conservazione previsti per i dati in IASA-GEX SIC corrispondono esattamente ai termini attualmente previsti per il sistema ISIS (cfr. art. 26 OSI-SIC).

Sezione 6: Disposizioni particolari relative a INDEX SIC

Art. 29 Struttura

INDEX SIC è ora disciplinato come sistema informativo a sé stante, con una propria base legale all'articolo 51 LAIn e costituito dalle seguenti tre sezioni:

- una sezione per determinare se in IASA SIC o IASA-GEX SIC il SIC tratta dati riguardanti una persona fisica o giuridica, una cosa o un evento (IASA INDEX; cfr. lett. a). Tale sezione contiene gli stessi oggetti su persone fisiche o giuridiche, cose ed eventi attualmente contenuti nell'indice ISIS e ISAS;
- ora è prevista anche una nuova sezione per l'archiviazione, la registrazione, il trattamento, la consultazione e la valutazione di dati provenienti da accertamenti preliminari delle autorità d'esecuzione cantonali (KND INDEX; cfr. lett. b). In questa sezione queste ultime possono trattare i dati prima di averli consolidati al punto da poterli trasmettere al SIC. Oggi questi dati sono gestiti dalle autorità d'esecuzione cantonali, ma sottostanno alle disposizioni della LMSI e devono essere tenuti rigorosamente separati dagli altri dati di tali autorità. D'ora in poi essi saranno gestiti in un sistema d'informazione del SIC e pertanto potranno essere consultati e verificati più facilmente dall'organo di controllo della qualità del SIC. Questa soluzione agevola anche il trattamento delle domande di accesso ai sensi dell'articolo 63 LAIn. Inoltre, tiene anche conto delle esigenze legate alla sicurezza dei dati (nella trasmissione dalle autorità d'esecuzione cantonali al SIC);
- infine, è prevista una sezione per la gestione dei mandati nonché per l'allestimento, la gestione e l'archiviazione dei rapporti delle autorità d'esecuzione cantonali e per l'archiviazione dei prodotti ottenuti dal SIC (cfr. lett. c). Il SIC accetterà dunque un rapporto se esso corrisponde al mandato da esso impartito o se è stato presentato spontaneamente in virtù del mandato informativo generale, esiste il nesso con i compiti di cui all'articolo 6 LAIn e le informazioni in esso contenute sono rilevanti ed esatte. Anche la gestione dei mandati è oggi affidata alle autorità d'esecuzione cantonali e sottostà alle disposizioni della LMSI. In questa sezione possono essere archiviate anche le informazioni che il SIC trasmette alle autorità d'esecuzione cantonali per l'adempimento dei loro compiti ufficiali.

Art. 30 Dati

Il contenuto di INDEX SIC è retto esaustivamente dall'articolo 51 capoverso 3 LAIn, sicché in questa sede si rinuncia a ulteriori commenti (cfr. cpv. 1).

Come già oggi previsto (cfr. art. 16 cpv. 5 e 22 cpv. 5 OSI-SIC), il capoverso 2 formula una riserva a favore della protezione delle fonti secondo l'articolo 35 LAIn. A titolo eccezionale, se necessario per motivi di protezione delle fonti, i dati riguardanti persone fisiche e giuridiche trattati in IASA SIC o in IASA-GEX SIC non vengono riversati in IASA INDEX. In passato questa prassi ha dato buone prove.

In virtù dell'articolo 44 capoverso 1 LAIn, anche le autorità d'esecuzione cantonali possono trattare dati personali degni di particolare protezione e profili della personalità. INDEX SIC può pertanto contenere anche questo tipo di dati (cfr. cpv. 3).

Secondo la prassi attuale, in INDEX SIC non vengono registrati dati (del sistema ISIS) concernenti terzi. Questa regola sarà applicata anche in futuro, poiché i terzi hanno una rilevanza per i settori di compiti del SIC ai sensi dell'articolo 6 LAIn soltanto attraverso il nesso con altre persone fisiche o giuridiche. Essa è ora espressamente prevista al capoverso 4.

Come oggi, anche i capoversi 5 e 6 prevedono che il catalogo dei dati personali figuri nell'allegato, e che i campi di dati vengano definiti dal DDPS.

Art. 31 Trattamento dei dati da parte delle autorità d'esecuzione cantonali

Le autorità d'esecuzione cantonali devono rispettare i limiti previsti dalla LAIn sia nel trattamento di mandati concreti del SIC sia nella presentazione spontanea di rapporti (cfr. cpv. 1). In altri termini, deve sempre esistere un nesso con un settore

di compiti del SIC ai sensi dell'articolo 6 LAIn (anche nella registrazione di dati personali nell'ambito degli accertamenti preliminari ai sensi dell'art. 29 lett. b OSIM-SIC) e i limiti posti al trattamento dei dati dall'articolo 5 capoverso 5 LAIn devono essere rispettati.

Nell'ambito della consultazione sulla LAIn, le autorità d'esecuzione cantonali avevano espresso il desiderio di poter accedere reciprocamente ai rispettivi accertamenti preliminari ai sensi dell'articolo 29 lettera b del disegno di ordinanza, per poter accertare se negli altri Cantoni un'altra autorità d'esecuzione cantonale avesse già effettuato accertamenti preliminari su una persona fisica o giuridica, una cosa o un evento. Il numero delle persone che vivono, lavorano o operano in diversi Cantoni è aumentato considerevolmente. Il coordinamento delle attività necessarie per gli accertamenti preliminari consente di operare in modo più mirato, facilitando il compito alle autorità d'esecuzione cantonali. Questa rivendicazione è stata recepita al capoverso 2. Quindi, se nel quadro di accertamenti preliminari vengono registrati oggetti, è possibile concedere ad altre autorità d'esecuzione cantonali l'accesso a quest'ultimi.

Variante dell'articolo 31 capoverso 2

La Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS) ha suggerito di consentire alle autorità d'esecuzione cantonali di accertare in qualsiasi momento se altre autorità d'esecuzione cantonali abbiano già trattato, nell'ambito delle loro competenze, informazioni su una determinata persona o organizzazione. Secondo la CCPCS, non basta una formulazione potestativa: i Cantoni devono poter procedere spontaneamente a un confronto dei settori riservati ai Cantoni in INDEX SIC.

Per l'articolo 31 capoverso 2 vengono dunque presentate due possibili varianti. La scelta dipenderà dalle preferenze espresse in sede di consultazione.

Art. 32 Diritti d'accesso

I diritti d'accesso ai dati in INDEX SIC sono retti dall'articolo 51 capoverso 4 LAIn e mantengono la stessa estensione prevista dal diritto vigente.

Come già evocato, l'articolo 31 OSIM-SIC prevede che, per evitare inutili ripetizioni, le autorità d'esecuzione cantonali possano accedere reciprocamente agli accertamenti preliminari delle corrispondenti autorità degli altri Cantoni secondo l'articolo 29 lettera b. Ai collaboratori del SIC è accordato unicamente un diritto di lettura nella sezione del KND INDEX riservata alla gestione dei mandati, mentre non sono autorizzati ad accedere agli accertamenti preliminari delle autorità cantonali. Soltanto l'organo di controllo della qualità del SIC è autorizzato, in virtù dell'articolo 33 lettera b, ad accedere ai dati sugli accertamenti preliminari contenuti nel KND INDEX ai fini della verifica periodica dei dati personali. Come già nel diritto vigente, il capoverso 2 rimanda all'allegato 4 per un catalogo dei diritti d'accesso individuali.

Art. 33 Verifica periodica dei dati personali

Secondo l'articolo 29 lettera a OSIM-SIC, in IASA INDEX vengono rispecchiati, e verificati (periodicamente) secondo le regole vigenti per questi sistemi d'informazione, soltanto i dati registrati in IASA SIC e IASA-GEX SIC. Di conseguenza, è inutile prevedere una verifica periodica anche in IASA INDEX. Conviene tuttavia che l'organo di controllo della qualità del SIC verifichi periodicamente il rispetto delle disposizioni sulla registrazione dei dati provenienti da IASA SIC e IASA-GEX SIC. Tale verifica è prevista una volta l'anno (cfr. cpv. 1 lett. a).

I dati secondo l'articolo 29 lettera b e c OSIM-SIC vengono registrati, se sono rilevanti e sufficientemente consolidati, in IASA SIC o IASA-GEX SIC e verificati periodicamente secondo le disposizioni determinanti per questi sistemi d'informazione. L'organo di controllo della qualità del SIC è inoltre incaricato di verificare una volta l'anno se il trattamento dei dati da parte delle autorità d'esecuzione cantonali avviene nell'ambito dell'esecuzione della LAIn, se sono rispettati i limiti posti al trattamento dei dati secondo l'articolo 5 capoverso 5 LAIn e se i dati non vengono conservati per più di cinque anni (cfr. cpv. 1 lett. b). Se necessario, il suddetto organo rettifica o cancella i dati non conformi e organizza corsi di formazione. In tale contesto esso si concentra, secondo il piano dei controlli, sui dati trattati da una o più autorità d'esecuzione cantonali.

Per meglio garantire la trasparenza, l'organo di controllo della qualità comunica l'esito della verifica in un rapporto all'attenzione del direttore del SIC (cfr. cpv. 2).

Art. 34 Durata di conservazione

La durata massima di conservazione dei dati in IASA INDEX secondo l'articolo 29 lettera a OSIM-SIC è retta dalle disposizioni applicabili ai sistemi d'informazione da cui provengono i dati (per i dati provenienti da IASA SIC secondo l'art. 21 e per i dati provenienti da IASA-GEX SIC secondo l'art. 28 OSIM-SIC). La cancellazione dei dati in questi sistemi d'informazione comporta automaticamente la cancellazione dei corrispondenti dati in IASA INDEX, poiché i dati contenuti in quest'ultimo sono semplicemente uno specchio dei dati originali (cfr. cpv. 1).

I dati delle autorità d'esecuzione cantonali secondo l'articolo 29 lettere b e c OSIM-SIC potranno essere conservati, come secondo il diritto vigente, per un massimo di cinque anni (cfr. cpv. 2).

Secondo il capoverso 3 in combinato disposto con l'articolo 45 capoverso 5 lettera d LAIn, l'organo di controllo della qualità del SIC è tenuto a cancellare i dati di cui all'articolo 29 lettere b e c OSIM-SIC su richiesta delle autorità d'esecuzione cantonali o allo scadere del periodo previsto al capoverso 2. Le registrazioni errate possono essere distrutte entro dieci giorni dalle stesse autorità d'esecuzione cantonali.

Sezione 7: Disposizioni particolari relative a GEVER SIC

Art. 35 Struttura

La struttura attuale di GEVER SIC viene mantenuta senza cambiamenti. Il sistema si compone di una sezione per l'archiviazione e il trattamento dei dati che servono a trattare e controllare gli affari nonché a garantire l'efficienza dei processi di lavoro del SIC (cfr. lett. a), una sezione che permette di consultare e trattare i mandati pendenti e conclusi dei collaboratori del SIC (cfr. lett. b) e un motore di ricerca che permette di eseguire ricerche a tutto testo all'interno del sistema (cfr. lett. c).

Art. 36 Dati

Il contenuto di GEVER SIC è retto dall'articolo 52 capoverso 2 LAIn e rispetto ad oggi non subisce modifiche, benché ad esempio il controllo degli affari del servizio di documentazione sul razzismo non venga più menzionato espressamente (cfr. cpv. 1 e art. 38 cpv. 1 OSI-SIC). Nel presente disegno di ordinanza, i dati per il controllo degli affari nell'ambito dell'esplorazione radio sono disciplinati nella sezione 11 concernente le disposizioni particolari relative al sistema d'informazione ISCO.

Il disciplinamento attualmente previsto all'articolo 38 capoverso 2 OSI-SIC essendosi rivelato concretamente impraticabile (i dati utilizzati per l'allestimento dei contenuti secondo l'art. 38 cpv. 1 lett. a-c OSI-SIC, non essendo contrassegnati, in GEVER non possono essere selezionati con un onere ragionevole), nel presente disegno di ordinanza è stato omesso. Questi dati saranno invece aggiornati nell'ambito di una sistematica verifica periodica (cfr. art. 38 OSIM-SIC).

Il capoverso 2 prevede, come secondo il diritto vigente, che in deroga all'articolo 12 capoversi 2 e 3 dell'ordinanza GEVER del 30 novembre 2012[13], in GEVER SIC possono essere archiviati dati del livello di classificazione CONFIDENZIALE e SEGRETO non criptati (cfr. art. 37 cpv. 2 OSI-SIC e le misure di sicurezza particolari previste per GEVER).

Il catalogo dei dati personali figura ancora in un allegato del presente disegno di ordinanza.

Art. 37 Diritti d'accesso

I diritti d'accesso sono retti dall'articolo 52 capoverso 3 LAIn e rispetto a oggi non subiscono modifiche (cfr. cpv. 1). Come secondo il diritto vigente, il capoverso 2 rimanda, per un catalogo dei diritti d'accesso individuali, al pertinente allegato.

Art. 38 Verifica periodica dei dati personali

Secondo il capoverso 1, l'organo di controllo della qualità del SIC è competente per la verifica periodica dei dati di GEVER prevista dalla nuova ordinanza. In particolare, verifica che i dati utilizzati per l'allestimento dei contenuti ai sensi dell'articolo 52 capoverso 2 lettere a e b LAIn non vengano conservati troppo a lungo. A tal fine verifica, almeno ogni dieci anni, le cartelle e sottocartelle del compendio e, tenendo conto della situazione attuale, valuta se i dati che contengono sono ancora necessari per il trattamento e il controllo degli affari nonché per garantire l'efficienza dei processi di lavoro in seno al SIC.

Se non lo sono, vengono cancellati e consegnati all'Archivio federale (cfr. cpv. 2). Per garantire meglio la trasparenza, l'organo di controllo della qualità comunica l'esito della verifica in un rapporto all'attenzione del direttore del SIC.

Art. 39 Blocco dell'utilizzazione

Secondo il numero 3 delle istruzioni del direttore del SIC del 9 settembre 2013 concernenti il trattamento dei dati nel Sistema d'informazione per la gestione degli affari del SIC (GEVER SIC), i rapporti ufficiali e i rapporti sulla situazione o le comunicazioni emanate non possono essere allestiti soltanto sulla base dei dati di GEVER. In altri termini, i dati provenienti da IASA SIC o IASA-GEX SIC allegati, in GEVER, a un mandato, possono essere utilizzati soltanto dopo aver verificato se i dati sono ancora gestiti nel corrispondente sistema d'informazione. Questa regola scaturisce dal fatto che l'organo di controllo della qualità potrebbe nel frattempo aver cancellato i dati da IASA SIC o IASA-GEX SIC. Questo blocco dell'utilizzazione è ora statuito al capoverso 1. Per utilizzazione si intende dunque l'inserimento dell'informazione in un prodotto.

PES non è toccato dal blocco. Per il monitoraggio della situazione vengono necessariamente utilizzati dati provenienti direttamente da PES e anche per l'allestimento di prodotti informativi è talvolta necessario poter utilizzare questi dati direttamente, se non sono stati registrati in altri sistemi d'informazione. Data la brevità del termine di conservazione previsto per i dati nella PES, non sorgono conflitti con gli altri sistemi.

Secondo il capoverso 2, l'organo di controllo della qualità del SIC effettua una volta l'anno una verifica a campione sul rispetto del blocco dell'utilizzazione.

Art. 40 Durata di conservazione

La durata di conservazione prevista per i dati registrati in GEVER SIC è di 45 anni al massimo (cfr. art. 40 cpv. b OSI-SIC).

Sezione 8: Disposizioni particolari relative a PES

Art. 41 Struttura

La struttura di PES rimane invariata rispetto ad oggi, nonostante la disposizione sia stata riformulata (cfr. art. 29 cpv. 2 OSI-SIC).

---

13 RS **172.010.441**

Art. 42 Dati

Il contenuto di PES è retto dall'articolo 53 capoverso 2 LAIn e rispetto ad oggi rimane anch'esso invariato (cfr. art. 30 cpv. 1 OSI-SIC). In PES vengono registrati dati personali soltanto nella misura assolutamente indispensabile per la presentazione e valutazione della situazione.

Art. 43 Diritti d'accesso

I diritti d'accesso a PES sono retti dall'articolo 53 capoversi 3 e 4 LAIn e rispetto ad oggi rimangono invariati (cfr. cpv. 1 e art. 32 OSI-SIC).

Come sinora, a determinate condizioni il SIC ha la possibilità di concedere a servizi privati nonché ad autorità di sicurezza e di polizia estere, in caso di eventi che comportano un aggravamento del pericolo per la sicurezza, un accesso a PES limitato nel tempo e nei contenuti (cfr. cpv. 3). L'utilizzazione da parte di tali servizi e autorità può essere verificata conformemente al capoverso 4. Un catalogo dei diritti d'accesso individuali figura nell'allegato 8 (cfr. cpv. 5). I capoversi 3-5 di questa disposizione del disegno di ordinanza sono stati ripresi senza modifiche dall'articolo 32 capoversi 2-4 OSI-SIC.

Art. 44 Verifica periodica

La verifica periodica dei dati di PES prevista dalla nuova ordinanza viene effettuata dai collaboratori del SIC competenti per l'archiviazione dei dati nel sistema (cfr. cpv. 1). Nell'ambito di tale verifica, tutte le informazioni che non sono più necessarie per il coordinamento e l'attuazione delle misure di polizia di sicurezza e registrate da più di tre anni vengono cancellate e consegnate all'Archivio federale (cfr. cpv. 2). L'organo di controllo della qualità del SIC esegue inoltre controlli a campione secondo l'articolo 11 capoverso 2 (cfr. cpv. 4).

Per meglio garantire la trasparenza, i collaboratori che hanno effettuato la verifica periodica comunicano l'esito della verifica in un rapporto all'attenzione dell'organo di controllo della qualità del SIC (cfr. cpv. 3).

Art. 45 Durata di conservazione

La durata di conservazione dei dati in PES corrisponde a tre anni al massimo, esattamente come già previsto dall'articolo 31 OSI-SIC.

Sezione 9: Disposizioni particolari relative al Portale OSINT

Art. 46 Struttura

Nella vigente OSI-SIC, la struttura del Portale OSINT non è precisata. Per ragioni di trasparenza, essa viene invece specificata nel presente disegno di ordinanza. Il Portale OSINT è costituito in particolare da un archivio dati, organizzato per fonte, destinato alla registrazione e alla valutazione di dati provenienti da fonti accessibili al pubblico.

Art. 47 Dati

Come nella Memoria intermedia OSINT prevista dal vigente diritto (cfr. art. 42 cpv. 1 OSI-SIC), anche nel Portale OSINT vengono archiviati dati provenienti da fonti accessibili al pubblico. Tuttavia, i dati contenuti nel nuovo portale non sono semplici copie di dati tratti in Internet. Nel Portale OSINT vengono raccolte informazioni della miglior qualità possibile, che devono sempre avere un nesso con un settore di compiti del SIC. I dati provengono in parte da fonti a pagamento (vari abbonamenti a media online) o possono essere il frutto di ricerche mirate (monitoraggio del jihadismo). Tutti i dati contenuti nel nuovo portale vengono organizzati per fonte e tematica e possono essere analizzati e utilizzati per mezzo di strumenti (tool) di analisi (cfr. cpv. 1).

Prima del loro utilizzo o della loro trasmissione, i dati contenuti nel Portale OSINT devono essere riversati in IASA SIC, IASA-GEX SIC o GEVER SIC secondo le pertinenti norme applicabili all'archiviazione e alla registrazione di informazioni (cfr. cpv. 2).

Se i dati vengono archiviati in modo automatico anziché essere smistati manualmente, la qualità della fonte va preliminarmente verificata (cfr. cpv. 3) seguendo procedure e direttive prestabilite. Nel Portale OSINT, ad esempio, vengono archiviati soltanto dati provenienti da fonti accessibili al pubblico, e la registrazione automatica riguarda in particolare i dispacci di agenzia e simili.

Il catalogo dei dati personali e dei diritti d'accesso individuali figura all'allegato 9 (cfr. cpv. 4).

Art. 48 Diritti d'accesso

Come già previsto dal vigente diritto, al Portale OSINT hanno accesso tutti i collaboratori del SIC. In futuro l'accesso potrà essere accordato anche ai collaboratori delle autorità d'esecuzione cantonali (cfr. cpv. 1 in combinato disposto con l'art. 54 cpv. 3 e 4 LAIn). Il catalogo dei diritti d'accesso individuali figura nell'allegato 10 (cfr. cpv. 2).

Art. 49 Verifica periodica

La verifica periodica del Portale OSINT prevista dalla nuova ordinanza viene effettuata dai collaboratori del SIC competenti per l'archiviazione dei dati nel portale (cfr. cpv. 1). Questi sono tenuti a verificare almeno ogni cinque anni, tenendo conto della situazione attuale, se i dati sono ancora necessari per l'adempimento dei compiti secondo l'articolo 6 LAIn nonché a cancellare e consegnare all'Archivio federale, tutti i dati archiviati da più di 15 anni (cfr. cpv. 2). L'organo di controllo della qualità del SIC esegue inoltre un controllo a campione secondo l'articolo 11 capoverso 2 (cfr. cpv. 4).

Per meglio garantire la trasparenza, i collaboratori che hanno effettuato la verifica periodica ne comunicano l'esito in un rapporto all'attenzione dell'organo di controllo della qualità del SIC (cfr. cpv. 3).

Art. 50 Durata di conservazione

Affinché i dati strutturati e di pregiata qualità contenuti nel Portale OSINT possano essere utilizzati per un periodo prolungato e analizzati utilmente per mezzo di strumenti (tool) di analisi (ad es. monitoraggio della nascita e dell'espansione dello Stato Islamico [IS] e delle sue attività nei settori di Internet accessibili al pubblico), il termine di conservazione è stato fissato a 20 anni.

Sezione 10: Disposizioni particolari relative a Quattro P

Art. 51 Struttura

Questa disposizione è stata ripresa senza cambiamenti dal vigente articolo 33 capoverso 2 OSI-SIC.

Art. 52 Dati

Il contenuto di Quattro P è rimasto invariato e corrisponde a quanto previsto attualmente al vigente articolo 34 capoverso 1 OSI-SIC (cfr. cpv. 1).

Prima del loro utilizzo o della loro comunicazione, i dati contenuti in Quattro P devono essere riversati in IASA SIC, IASA-GEX SIC o GEVER SIC secondo le regole previste per l'archiviazione e la registrazione di informazioni (cfr. cpv. 2).

Se i dati vengono archiviati in modo automatico anziché essere smistati manualmente, la qualità della fonte va preliminarmente verificata (cfr. cpv. 3) seguendo procedure e direttive prestabilite. L'archiviazione automatica di dati in Quattro P, ad esempio, si basa su un elenco confidenziale di Paesi approvato dal Consiglio federale. Se la ricerca dà dei risultati, viene effettuato un controllo manuale e l'organo di controllo della qualità del SIC verifica, per mezzo di controlli a campione, se sono stati registrati dati su Paesi non figuranti nel pertinente elenco.

Un catalogo dei dati personali e dei diritti d'accesso individuali figura nell'allegato 11 (cfr. cpv. 4).

Art. 53 Diritti d'accesso

I diritti d'accesso rimangono invariati e corrispondono al vigente articolo 35 OSI-SIC.

Art. 54 Verifica periodica

Il capoverso 1 stabilisce ora che i collaboratori del SIC competenti per la registrazione dei dati in Quattro P devono effettuare una verifica periodica. A tal fine verificano almeno ogni cinque anni se i dati trasmessi al SIC dagli organi di controllo alla frontiera corrispondono all'elenco stabilito dal Consiglio federale di cui all'articolo 55 capoverso 4 LAIn e se sono ancora necessari per l'adempimento dei compiti del SIC secondo l'articolo LAIn. Se l'elenco del Consiglio federale viene modificato, la collezione di dati deve essere opportunamente adeguata. L'organo di controllo della qualità del SIC esegue inoltre un controllo a campione secondo l'articolo 11 capoverso 2 (cfr. cpv. 3).

I dati non più necessari devono essere cancellati e consegnati all'Archivio federale (cfr. cpv. 2).

Art. 55 Durata di conservazione

La durata di conservazione dei dati in Quattro P è di cinque anni al massimo, come già previsto dal diritto vigente (cfr. art. 36 OSI-SIC).

Sezione 11: Disposizioni particolari relative a ISCO

Art. 56 Struttura

Per ragioni di trasparenza, ISCO è ora disciplinato nella nuova ordinanza come sistema d'informazione a sé stante, costituito da un archivio dati che consente di gestire e dirigere i mezzi di esplorazione, di procedere a verifiche e di redigere rapporti. L'archiviazione dei dati corrispondenti è retta attualmente dalle disposizioni relative a GEVER (cfr. spec. art. 38 cpv. 1 lett. e OSI-SIC).

Art. 57 Dati

Il contenuto di ISCO è retto dall'articolo 56 capoverso 2 LAIn (cfr. cpv. 1) e consiste in particolare in mandati di esplorazione effettuati insieme al Centro operazioni elettroniche della Base di aiuto alla condotta dell'Esercito Svizzero (COE-BAC). Tuttavia, i risultati dell'esplorazione radio e dei segnali via cavo non vengono archiviati in ISCO, bensì in IASA SIC o nella Memoria dei dati residui e possono essere registrati in ISCO per mezzo di un riferimento (esempio di procedura: un oggetto registrato in IASA SIC [numero telefonico] deve essere esplorato dal COE-BAC; il numero telefonico e il mandato assegnato al COE-BAC vengono registrati in ISCO per poter garantire in modo capillare il coordinamento e la compliance; dopodiché il numero telefonico viene trasmesso come target al COE-BAC; il risultato dell'esplorazione viene trasmesso al SIC sotto forma di rapporto COMINT e confluisce come documento originale in IASA SIC con il riferimento a ISCO).

Se i dati vengono archiviati in modo automatico anziché essere smistati manualmente, la qualità della fonte va preliminarmente verificata (cfr. cpv. 3) seguendo procedure e direttive prestabilite. Il mandato di prestazione (ad es. il numero telefonico) viene verificato dai collaboratori del SIC e caricato manualmente. I risultati (ad es. i dati di collegamento) vengono verificati dal «sensore» (ad es. dal collaboratore incaricato del COE-BAC) per quanto riguarda il nesso con i settori di compiti secondo l'articolo 6 LAIn, trasmessi al SIC e archiviati automaticamente in ISCO.

Art. 58 Diritti d'accesso

A ISCO hanno accesso soltanto i collaboratori del SIC che si occupano direttamente dell'esplorazione radio e dei segnali via cavo (attualmente meno di 10 persone).

Art. 59 Verifica periodica

Secondo il diritto vigente, i mandati di esplorazione e le collezioni di dati vengono già periodicamente verificati dal profilo dell'adeguatezza e proporzionalità tenendo conto della situazione attuale (cfr. cpv. 1). Ora questa verifica è espressamente disciplinata al capoverso 1. Essa compete ai collaboratori del SIC incaricati dell'archiviazione dei dati in ISCO.

Per meglio garantire la trasparenza, i collaboratori che hanno effettuato la verifica periodica ne comunicano il risultato in un rapporto all'attenzione dell'organo di controllo della qualità del SIC (cfr. cpv. 3).

Art. 60 Durata di conservazione

La durata di conservazione dei dati in ISCO è di cinque anni al massimo dalla conclusione del relativo mandato di esplorazione.

Sezione 12: Disposizioni particolari relativi alla Memoria dei dati residui

Art. 61 Struttura

Nella Memoria dei dati residui vengono memorizzate tutte le informazioni che in occasione dello smistamento dei dati ricevuti non hanno potuto essere assegnate a un altro sistema (cfr. cpv. 1 in combinato disposto con l'art. 57 LAIn). Nell'ambito della verifica dei dati ricevuti, le informazioni vengono verificate controllando se vi sono sufficienti indizi per riconoscere un nesso con i settori di compiti secondo l'articolo 6 LAIn (cfr. art. 3 cpv. 1 OSIM-SIC).

I dati necessari per l'adempimento dei compiti del SIC devono essere riversati in IASA SIC, IASA-GEX SIC o GEVER SIC e possono essere cancellati dalla Memoria dei dati residui, poiché essi verranno consegnati all'Archivio federale attraverso detti sistemi d'informazione (cfr. cpv. 2). L'archiviazione dei dati è retta dalle disposizioni dell'articolo 3 capoverso 1. Se devono essere utilizzati o comunicati dati personali, il loro riversamento soggiace alle disposizioni di cui all'articolo 4 capoverso 1. In altri termini, i dati personali devono essere preliminarmente verificati singolarmente per quanto riguarda il nesso con i compiti, la rilevanza, l'esattezza e il rispetto dei limiti posti al trattamento ai sensi dell'articolo 5 capoverso 5 LAIn, ed essere registrati in modo strutturato in IASA SIC (per IASA GEX SIC è già previsto un obbligo generale di registrazione strutturata).

Art. 62 Dati

Il contenuto della Memoria dei dati residui è retto dall'articolo 57 capoverso 2 LAIn. Esso è costituito soprattutto da comunicazioni delle autorità di sicurezza estere, da dati provenienti dall'esplorazione radio e di segnali via cavo, da informazioni di fonti umane e da informazioni acquisite passivamente dal SIC.

Art. 63 Diritti d'accesso

Ai dati della Memoria dei dati residui hanno accesso i collaboratori del SIC incaricati della registrazione, della ricerca, dell'analisi e del controllo della qualità dei dati (cfr. art. 57 cpv. 3 LAIn).

Art. 64 Verifica periodica

Secondo il capoverso 1, l'organo di controllo della qualità del SIC verifica almeno ogni dieci anni, tenendo conto della situazione attuale, se le collezioni di dati della Memoria dei dati residui sono ancora necessarie per l'adempimento dei compiti secondo l'articolo 6 LAIn e non sono archiviati da più di dieci anni. I dati non più necessari e quelli archiviati da più di dieci anni devono essere cancellati e consegnati all'Archivio federale (cfr. cpv. 2).

L'organo di controllo della qualità del SIC è inoltre tenuto a verificare che siano rispettate le condizioni per il riversamento dei dati e che i dati riversati vengano distrutti (cfr. cpv. 3). Per meglio garantire la trasparenza, comunica l'esito della verifica in un rapporto all'attenzione del direttore del SIC. Se in occasione della verifica constata l'esistenza di mancanze, formula raccomandazioni al riguardo nel proprio rapporto e l'attuazione delle raccomandazioni formulate viene inserita nell'elenco delle pendenze della direzione del SIC (questo principio si applica peraltro anche a GEVER SIC).

L'organo di controllo della qualità del SIC esegue inoltre un controllo a campione secondo l'articolo 11 capoverso 2 (cfr. cpv. 4).

Art. 65 Durata di conservazione

La durata di conservazione dei dati nella Memoria dei dati residui è di dieci anni al massimo.

Sezione 13: Dati provenienti da misure di acquisizione soggette ad autorizzazione e da acquisizioni all'estero

Art. 66 Struttura

I sistemi di memorizzazione servono all'archiviazione dei dati per la registrazione, il trattamento e la consultazione di dati con riferimento a casi specifici raccolti dal SIC nel quadro di misure di acquisizione soggette ad autorizzazione e da acquisizioni all'estero (cfr. cpv. 1).

L'articolo 58 capoverso 1 LAIn stabilisce che i dati provenienti da questo tipo di misure sono memorizzati in sistemi distinti dalla rete dei sistemi d'informazione e ivi visionati (cfr. cpv. 2).

Art. 67 Dati

Come previsto per IASA SIC e IASA-GEX SIC, anche nei sistemi di memorizzazione possono essere trattati dati su persone fisiche e giuridiche, cose ed eventi, dati personali degni di particolare protezione e profili della personalità.

Art. 68 Diritti d'accesso

I diritti d'accesso sono retti dall'articolo 58 capoverso 5 LAIn (cfr. cpv. 1).

Per ogni singola operazione devono essere disposti diritti d'accesso separati (cfr. cpv. 2), garantendo che l'accesso sia concesso soltanto alle persone che dirigono l'operazione o incaricate dell'esecuzione delle misure di acquisizione e dell'analisi dei risultati (cfr. art. 58 cpv. 5 LAIn).

I diritti d'accesso individuali devono essere approvati dal SIC per ogni misura d'acquisizione (cfr. cpv. 3).

Art. 69 Blocco dell'utilizzazione

Il SIC può utilizzare o trasmettere dati provenienti da misure di acquisizione soggette ad autorizzazione e da acquisizioni all'estero unicamente se li ha previamente riversati in IASA SIC nel rispetto delle condizioni prestabilite (cfr. cpv. 1). A differenza di quanto previsto per la Memoria dei dati residui, i dati in questione non devono essere distrutti, dato il breve periodo di conservazione nei sistemi di memorizzazione.

Per i dati di persone non implicate e i dati di persone che beneficiano della facoltà di non deporre secondo gli articoli 171–173 del codice di procedura penale del 5 ottobre 2007[14] (CPP) è previsto un blocco di utilizzazione assoluto; questi dati devono essere distrutti al più tardi entro 30 giorni dalla conclusione della misura (cfr. cpv. 2). Questa soluzione garantisce che i dati in questione non confluiscano in prodotti del SIC e che non vengano comunicati.

L'organo di controllo della qualità del SIC verifica a campione se il blocco dell'utilizzazione è rispettato (cfr. cpv. 3).

Art. 70 Durata di conservazione

I dati contenuti nei sistemi di memorizzazione possono essere molto voluminosi e contenere molte informazioni che non hanno nulla a che fare con l'obiettivo dell'esplorazione, poiché può trattarsi ad esempio di informazioni di carattere meramente privato. Occorre tener conto anche della protezione della personalità di terzi, ad esempio degli estranei che utilizzano la linea di telecomunicazione della persona sorvegliata. Spesso è impossibile constatare immediatamente se certe comunicazioni sono o non sono rilevanti, ad esempio perché la rete dei contatti della persona sorvegliata deve ancora essere identificata o perché questa ricorre per la comunicazione a elementi cospirativi per proteggere i suoi contatti. I dati che non sono necessari per un procedimento legale in corso devono pertanto essere rapidamente cancellati (cfr. cpv. 1).

Se una comunicazione viene differita, la cancellazione deve avvenire al più tardi sei mesi dopo la comunicazione della misura alla persona interessata (cfr. cpv. 2).

La vigilanza del Tribunale amministrativo federale prevista all'articolo 58 capoverso 3 LAIn in caso di distruzione dei dati è assicurata dall'obbligo di presentare, prima della distruzione dei dati, una domanda a detto tribunale in cui figurino indicazioni relative ai dati archiviati separatamente e destinati alla distruzione (cfr. cpv. 3).

La durata di conservazione dei dati acquisiti in virtù dell'articolo 36 capoverso 5 LAIn è di tre anni al massimo (cfr. cpv. 5).

Allegati 1, 3, 5, 7, 9, 11, 13, 15 e 17: cataloghi di dati personali

In virtù dell'articolo 47 capoverso 2 lettera a LAIn, negli allegati summenzionati figurano i dati che riguardano una persona fisica o giuridica o possono essere registrati in relazione ad essa.

Quando sarà disponibile la pertinente base legale formale, i cataloghi di dati personali saranno completati, nell'ambito della prossima revisione, con il NAVS13 (numero AVS a 13 cifre).

Allegati 2, 4, 6, 8, 10, 12, 14, 16 und 18: diritti d'accesso

In virtù dell'articolo 47 capoverso 2 lettera c LAIn, negli allegati summenzionati figurano i diritti d'accesso ai sistemi d'informazione del SIC.

14 RS **312.0**