



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Autorità di vigilanza indipendente sulle
attività informative**

Rapporto di attività 2021

dell'Autorità di vigilanza indipendente
sulle attività informative AVI-AIn



AVI-AIn

SIC

SIM

COE

SICant

1. Sintesi

Tre eventi hanno segnato le attività dell'Autorità di vigilanza indipendente sulle attività informative (AVI-AIn) nel 2021: la fine del rapporto di lavoro con il direttore del Servizio delle attività informative della Confederazione (SIC), il netto aumento del numero di indicazioni e informazioni concernenti collaboratrici e collaboratori del SIC insoddisfatti e i cambiamenti di personale all'interno dell'AVI-AIn stessa, che hanno riguardato anche la direzione. Thomas Fritschi lascia infatti l'AVI-AIn dopo quasi cinque anni di servizio. Nonostante questi sviluppi, l'AVI-AIn ha comunque adempiuto pienamente il suo compito principale, ossia la vigilanza sulle attività informative.

Nel 2021 l'AVI-AIn ha svolto verifiche nei seguenti ambiti:

- «Strategia e pianificazione»: 1 verifica;
- «Organizzazione»: 3 verifiche;
- «Collaborazione»: 8 verifiche;
- «Acquisizione»: 4 verifiche;
- «Trattamento dei dati/archiviazione»: 2 verifiche.

In totale sono state condotte e concluse 18 verifiche. Rispetto agli ultimi anni, il numero di raccomandazioni formulate è nettamente diminuito. Ciò è riconducibile, da un lato, ai miglioramenti già raggiunti attraverso l'attuazione delle raccomandazioni emesse dall'AVI-AIn negli anni scorsi e, dall'altro, al fatto che ora l'AVI-AIn controlla più in profondità, dopo aver ottenuto nei primi anni – con le sue verifiche – soprattutto una panoramica generale delle attività informative. Questo, infatti, rende più impegnativa la formulazione di raccomandazioni conformi al livello gerarchico.

In base alla sua valutazione dei rischi, l'AVI-AIn ha incentrato la propria attività sul SIC, presso il quale ha svolto complessivamente 17 verifiche.

La verifica della collaborazione tra il SIC e i servizi informazioni cantonali (SICant), la verifica della protezione delle infrastrutture critiche mediante la ciberdifesa e la verifica dell'acquisizione di informazioni per mezzo di fonti umane (Human Intelligence, HUMINT) hanno richiesto un grande dispiegamento di risorse da parte dell'AVI-AIn. Nell'ambito HUMINT, l'AVI-AIn ha anche svolto una verifica straordinaria e su larga scala che non

era indicata nel piano di controllo 2021. Il SIC si è confrontato con le possibilità di miglioramento constatate. Il lungo periodo di transizione dovuto al cambiamento in seno alla direzione e l'insoddisfazione del personale rappresentano un peso per il servizio. Per quanto riguarda la collaborazione con i SICant, il SIC ha ottenuto una buona valutazione. Il contributo che fornisce alla sicurezza interna della Svizzera è importante. In ambito ciber, il SIC ha invece rivisto la sua prassi per quanto concerne l'acquisizione di informazioni. L'AVI-AIn si è regolarmente informata in modo dettagliato in merito a questo tema, al fine di creare le basi decisionali necessarie per un'eventuale verifica.

L'AVI-AIn ha sottoposto il Centro operazioni elettroniche (COE) a una verifica nell'ambito della ciberdifesa. Ne è emerso che il SIC e il COE dispongono delle competenze necessarie per la protezione delle infrastrutture critiche e che la collaborazione funziona. Inoltre, l'AVI-AIn ha preso parte come osservatrice alle riunioni dell'Autorità di controllo indipendente per l'esplorazione radio e l'esplorazione dei segnali via cavo (ACI).

Nell'anno in esame il Servizio informazioni militare (SIM) è stato verificato dall'AVI-AIn in riferimento alla protezione dei dati. Sebbene il SIM tratti dati personali, questi ultimi non rappresentano il suo interesse principale. Conformemente al mandato legale, l'acquisizione di informazioni riguarda soprattutto l'estero. L'AVI-AIn non ha constatato la presenza di punti che potessero far sorgere dubbi in merito alla legalità del trattamento dei dati personali da parte del SIM.

Nell'ambito di una riunione sono stati inoltre curati e consolidati gli scambi tra l'AVI-AIn e gli organi di vigilanza cantonali.

Il Rapporto di attività 2021 è stato presentato per consultazione al Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) e alla Delegazione delle Commissioni della gestione delle Camere federali (DelCG) dal 14 al 27 febbraio 2022. Se i commenti menzionavano errori di forma o di sostanza in questo rapporto o interessi da tutelare che ostano alla pubblicazione di alcune parti, questi sono stati presi in considerazione.

Conclusione

L'AVI-AIn ha formulato 18 raccomandazioni nel quadro di 18 verifiche condotte. Attuando queste raccomandazioni permette di ridurre i rischi delle attività informative e garantire una maggiore efficacia.

Nell'anno in esame, le incertezze relative al personale del SIC hanno prevalso sulle attività informative svolte dal servizio. Il SIC stesso ha fatto i primi passi per cercare di risolvere i problemi, ma probabilmente questi sforzi non saranno sufficienti per smorzare le tensioni in modo duraturo e chiarire la situazione. Le strutture e le procedure esistenti nel servizio devono essere messe in discussione e, se necessario, adattate. Questo potrebbe garantire stabilità a lungo termine, il che ridurrebbe al minimo i rischi. Per raggiungere tale obiettivo, il SIC ha bisogno del sostegno del Dipartimento. Il minor numero di raccomandazioni indica che è stato possibile eliminare o perlomeno ridurre al minimo i rischi esistenti nel settore delle attività informative.

Le due organizzazioni militari nel settore delle attività informative, ossia il SIM e il COE, sono state sottoposte a un esame meno ampio tenendo conto della valutazione dei rischi su cui erano basate le verifiche. Non è stato necessario emettere raccomandazioni per queste organizzazioni. Resta da vedere come il COE si integrerà nel futuro Comando Ciber.



2. Contenuto

1	Sintesi	2
2	Contenuto	4
3	Nota personale	5
4	Sistemi d'informazione	6
4.1	Sistemi d'informazione verificati finora dall'AVI-AIn	7
4.2	In relazione ai sistemi d'informazione verificati, quali sono le sfide e le opportunità individuate dall'AVI-AIn?	9
4.3	Sviluppi futuri	11
4.4	Nuova gestione di dati: ripercussioni sulla LAIn	11
5	Attività di vigilanza	12
5.1	Piano di controllo	12
5.2	Verifiche nel 2021	12
5.3	Consenso	26
5.4	Controlling delle raccomandazioni	26
6	Vista interna	28
6.1	Personale e formazione continua	28
6.2	Revisione della LAIn	28
6.3	Legge federale sul principio di trasparenza dell'amministrazione (Legge sulla trasparenza, LTras)	28
6.4	Visite	28
6.5	Giurisprudenza	28
7	Coordinamento	29
7.1	Contatti nazionali	29
7.2	Contatti internazionali	31
8	Vista esterna	33
9	Cifre al 31 dicembre 2021	36
10	Allegato	37
10.1	Piano di controllo 2021	37
10.2	Elenco delle abbreviazioni	38

3. Nota personale

«L'AVI-AIn assicura «checks and balances» nel campo dei servizi informazioni.»

Thomas Fritschi



Thomas Fritschi, capo AVI-AIn

La pandemia di COVID-19, accompagnata da una tendenza alle divisioni sociali, le politiche egemoniche di singoli Stati o anche la nostra vulnerabilità ai ciberattacchi ci fanno capire quanto sia fragile la nostra sicurezza e quanto siano importanti la prevenzione e la valutazione della situazione per i decisori politici. In questi tempi sempre più incerti e difficili, il bisogno di informazioni e fatti sicuri è ancora maggiore. Per questo i servizi informazioni, e quindi anche la vigilanza su di essi, sono stati e sono tuttora sollecitati.

Anche nell'anno in esame abbiamo continuato a svolgere le nostre attività di vigilanza basandoci sui rischi e adeguandoci agli sviluppi attuali. Il numero delle nostre raccomandazioni è nettamente diminuito. Da un lato, perché alcuni miglioramenti sono già stati ottenuti negli anni passati; dall'altro, perché ci siamo concentrati maggiormente sulle sfide essenziali legate al lavoro di intelligence in uno Stato di diritto democratico e abbiamo controllato più in profondità, il che comporta requisiti più elevati per la formulazione di raccomandazioni conformi al livello gerarchico. Tra le attività particolarmente impegnative che abbiamo svolto figurano una verifica nel settore della gestione delle fonti umane e accertamenti approfonditi su eventi nell'dipartimento Ciber del SIC.

La nostra attenzione si è concentrata sull'organizzazione del SIC, che è stata messa alla prova dall'inaspettata partenza del direttore. A metà del 2021 le collaboratrici e i collaboratori insoddisfatti hanno fatto sentire la loro voce nei media. È quindi opportuno procedere a un cambiamento di cultura e a una revisione delle strutture e dei processi del SIC. Non è compito dell'autorità di vigilanza decidere in merito all'attuazione di tali misure. Si deve invece ritenere che questo sia il mandato del direttore del SIC designato.

Nel presente rapporto di attività, oltre a riferire sulle nostre attività di verifica e sugli sviluppi interni al SIC, vogliamo approfondire il tema dei sistemi d'informazione, a cui è legato

anche l'aspetto della protezione dei dati. A tale proposito, abbiamo affidato la redazione della rubrica «Vista esterna» a uno specialista qualificato: l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), il dr. iur. Adrian Lobsiger.

Si tratta dell'ultimo rapporto di attività dell'AVI-AIn redatto sotto la mia responsabilità e sono grato per questi quasi cinque anni di lavoro costruttivo in un ambiente altamente sensibile e impegnativo. L'AVI-AIn assicura il controllo e l'equilibrio («checks and balances») nel contesto dell'ampliamento delle competenze del SIC avvenuto nel 2017 e di un servizio in costante crescita. È strutturata e sviluppata in modo tale da poter soddisfare questa esigenza. La sua indipendenza viene rispettata e tenuta in considerazione e sono garantiti gli scambi e il coordinamento con gli altri organi di vigilanza a livello federale e cantonale. La speranza è che in futuro possa essere avviato anche un dialogo con l'alta vigilanza parlamentare.

È un bene che esista l'AVI-AIn, in quanto questa autorità può creare un clima di fiducia nei confronti delle attività informative. A tale proposito colgo anche l'occasione per ringraziarvi della fiducia che avete riposto in me negli ultimi anni e vi auguro buona lettura.

Thomas Fritschi, capo AVI-AIn

4. Sistemi d'informazione

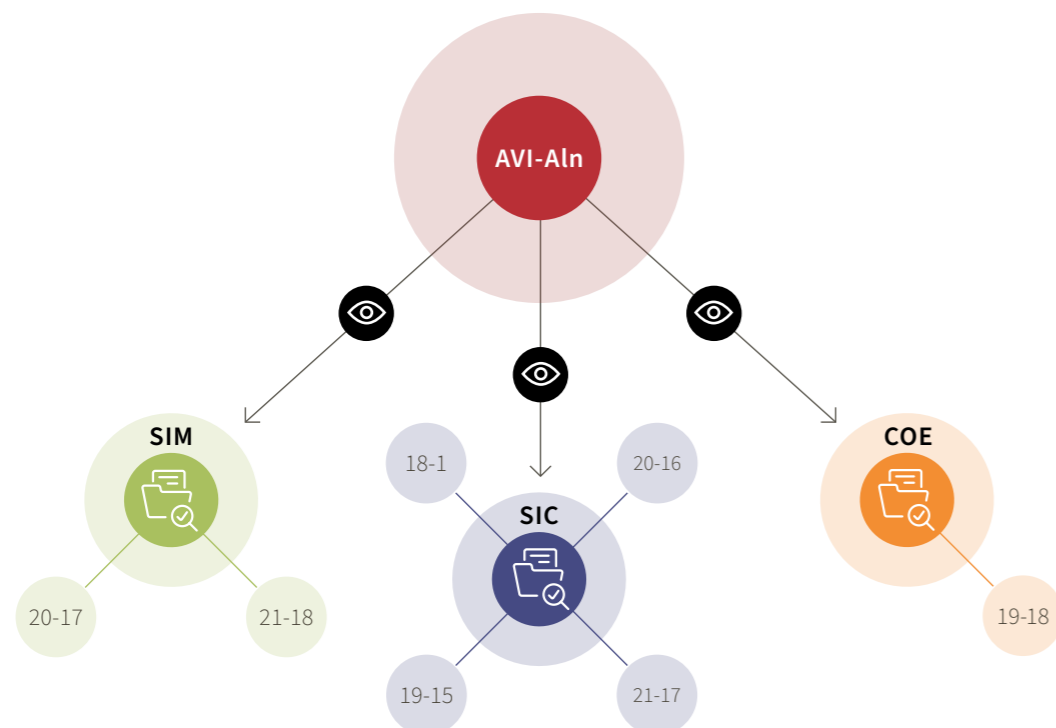
«Ogni anno, l'AVI-AIn verifica una serie di trattamenti di dati o di sistemi d'informazione.»

L'acquisizione di informazioni per l'adempimento dei compiti previsti dalla legge è uno dei compiti principali dei servizi informazioni svizzeri. Tali informazioni devono essere messe il più presto possibile a disposizione del personale competente al fine di consentirgli di svolgere i suoi compiti di servizio. Le informazioni vengono incorporate in prodotti di intelligence che sono messi a disposizione delle autorità di sicurezza nazionali ed estere nonché dei decisori militari e politici. Lo scopo dell'acquisizione di informazioni è quello di valutare la situazione di minaccia del momento ai fini della prevenzione sul piano nazionale e internazionale e all'attenzione dei decisori politici.

Le informazioni che non sono più necessarie per l'adempimento dei compiti dei servizi informazioni e il cui termine di conservazione è scaduto vengono offerte all'Archivio federale per

l'archiviazione. Le informazioni che l'Archivio federale considera prive di valore archivistico devono essere distrutte.

I servizi informazioni gestiscono una rete di sistemi d'informazione in cui le informazioni o i dati vengono trattati durante tutto il loro ciclo di vita, dall'acquisizione alla cancellazione. Le leggi applicabili contengono una serie di disposizioni sulla gestione dei dati. Poiché questo settore è importante per i servizi informazioni, l'AVI-AIn gli ha riservato uno specifico ambito nel suo piano di controllo: «Trattamento dei dati/archiviazione». Ogni anno, l'AVI-AIn verifica una serie di trattamenti di dati o di sistemi d'informazione. Considerata l'importanza dell'argomento, il presente rapporto di attività si concentra sul tema dei sistemi d'informazione.



4.1 Sistemi d'informazione verificati finora dall'AVI-AIn

Per quanto riguarda il SIC l'AVI-AIn ha sottoposto a verifica i sistemi d'informazione indicati qui di seguito.

Verifica	Scopo	Anno/fonte
18-1 Panoramica dei dati del SIC e contenuto dell'Archivio dei dati residui	La legge federale sulle attività informative (LAI) ¹ indica all'articolo 47 i sistemi d'informazione gestiti dal SIC. I sistemi d'informazione vengono poi ulteriormente disciplinati a livello di ordinanza ² . Questa verifica ha permesso all'AVI-AIn di ottenere una panoramica di tutti i sistemi d'informazione del SIC ed è servita come punto di partenza per ulteriori verifiche. Secondo la legge, la Memoria dei dati residui può contenere dati che non possono essere assegnati a nessun altro sistema d'informazione. L'AVI-AIn ha quindi sottoposto a verifica il contenuto di questo sistema per determinare il tipo di dati in esso trattati.	2018 (Rapporto di attività 2018, pagina 13)
19-15 Esercizio, contenuto e utilizzo dei sistemi d'informazione GEVER SIC ³ , memorizzazione dei file in BURAUT ⁴ , memorizzazione dei file in SiLAN ⁵ (valutazioni temporanee)	Nel 2012 il SIC ha introdotto un sistema di gestione degli affari. A tale sistema ha accesso tutto il personale del SIC. Vi vengono trattati dati amministrativi e informativi. Considerati i dati trattati e il grande numero di persone autorizzate ad accedervi, l'AVI-AIn ha scelto questo sistema per effettuare una prima verifica approfondita su un sistema d'informazione.	2019 (Rapporto di attività 2019, pag. 23 segg.)
20-16 Esercizio, contenuto e utilizzo dei sistemi di informazione IASA ⁶	IASA contiene i tre principali sistemi d'informazione per le attività informative ed è lo strumento di lavoro centrale del SIC. Per questo è stato oggetto di una verifica da parte dell'AVI-AIn.	2020 (Rapporto di attività 2020, pagina 23)

¹ RS 121

² Ordinanza sui sistemi d'informazione e di memorizzazione del Servizio delle attività informative della Confederazione (OSIME-SIC; RS 121.2)

³ Sistema per la gestione degli affari

⁴ Banca dati del SIC

⁵ Rete locale protetta del SIC

⁶ Sistema di analisi integrale del SIC

«Le basi legali rilevanti per il SIC per quanto concerne la gestione dei sistemi d'informazione sono più dettagliate e trasparenti di quelle relative al SIM e al COE. »

Verifica	Scopo	Anno/fonte
21-17 Servizio del SIC selezionato (Quattro P)	In questo sistema d'informazione viene registrato e trattato un grande numero di spostamenti di persone straniere. L'elevato numero di dati personali trattati con questo sistema e il fatto che i dati di Quattro P vengono utilizzati per il sistema di riconoscimento facciale del SIC hanno spinto l'AVI-AIn a sottoporre a verifica questo sistema.	2021 (Rapporto di attività 2021, pag. 22 segg.)

Per quanto riguarda il SIM, l'AVI-AIn ha sottoposto a verifica i sistemi d'informazione indicati nella tabella sottostante.

Verifica	Scopo	Anno/fonte
20-17 Sistemi d'informazione del SIM (gestione delle autorizzazioni)	I risultati della verifica sono serviti all'AVI-AIn per capire e pianificare ulteriori verifiche.	2020 (non è stato trattato specificamente nel rapporto di attività, ma sul sito Internet dell'AVI-AIn è disponibile un riassunto).
21-18 Protezione dei dati all'interno del SIM	Sebbene non si tratti della sua attività principale, il SIM tratta dati personali. L'AVI-AIn ha pertanto sottoposto a verifica gli aspetti dell'attività del SIM legati alla protezione dei dati in determinati sistemi d'informazione.	2021 (Rapporto di attività 2021, pag. 25 segg.)

Infine, per quanto concerne il COE, l'AVI-AIn ha sottoposto a verifica il sistema d'informazione riportato qui di seguito.

Verifica	Scopo	Anno/fonte
19-18 Ambiente informativo COE	Questa verifica ha fornito all'AVI-AIn una panoramica ed è servita come punto di partenza per ulteriori verifiche. Non esiste una base giuridica specifica che disciplini i sistemi informativi del COE. Le relative basi si trovano in diverse leggi e ordinanze.	2019 (Rapporto di attività 2019, pagina 26)

Oltre alle verifiche incentrate specificamente sui sistemi d'informazione, l'AVI-AIn ne ha condotte anche altre nel settore del trattamento e dell'archiviazione dei dati: più precisamente, nove verifiche supplementari dall'inizio della sua attività di vigilanza. Pertanto, dall'avvio delle proprie attività di verifica a oggi, nel quadro di 16 verifiche l'AVI-AIn si è occupata principalmente dei sistemi d'informazione dei servizi informativi nonché del trattamento dei dati in tali sistemi. I risultati di queste verifiche sono presentati qui di seguito.

4.2 In relazione ai sistemi d'informazione verificati, quali sono le sfide e le opportunità individuate dall'AVI-AIn?

4.2.1 Basi legali concernenti i sistemi d'informazione per le attività informative

Le basi legali riguardanti i sistemi d'informazione del SIC, del SIM e del COE non sono state tutte elaborate allo stesso modo. Le basi legali rilevanti per il SIC per quanto concerne la gestione dei sistemi d'informazione sono più dettagliate e trasparenti di quelle relative al SIM e al COE. La maggiore chiarezza delle disposizioni legali rende più facile per l'AVI-AIn controllare la legalità dei sistemi d'informazione gestiti dal SIC. Pertanto, l'AVI-AIn si adopera per garantire che, in futuro, anche le basi giuridiche riguardanti il SIM e il COE vengano elaborate in modo più chiaro e differenziato.

4.2.2 Accesso dell'AVI-AIn ai sistemi d'informazione per le attività informative

I responsabili delle verifiche dell'AVI-AIn ricevono, solo dal SIC, un accesso diretto e limitato nel tempo ai sistemi d'informazione da sottoporre a verifica. Dispongono inoltre di un accesso permanente al sistema per la gestione degli affari del SIC.

Questo facilita le verifiche, visto che l'AVI-AIn può procurarsi autonomamente la documentazione necessaria. Al SIM e al COE ciò risulta più complicato, in quanto l'AVI-AIn deve farsi mostrare i sistemi o organizzare un accesso sul posto, il che rende più difficile, per esempio, elaborare autonomamente i dati dei controlli a campione in questi sistemi d'informazione.

4.2.3 Destinatari e attuazione delle raccomandazioni

Il COE e il SIM sono unità organizzative dell'esercito relativamente piccole. Il loro margine di manovra per la configurazione specifica dei sistemi d'informazione secondo le proprie esigenze è quindi limitato. Per l'AVI-AIn ciò rende più complicata la formulazione di raccomandazioni attuabili, poiché simili raccomandazioni devono riguardare solo i servizi informazioni stessi e non altre componenti dell'esercito. Tuttavia, le eventuali raccomandazioni in questo settore non possono praticamente mai riguardare soltanto il SIM o il COE. Al contrario, spesso il loro campo d'applicazione si interseca con tutti gli ambiti dell'esercito.

4.2.4 Priorità dell'AVI-AIn nel verificare i sistemi d'informazione

Gestione degli accessi e cancellazione dei dati nei sistemi d'informazione del SIC

Nell'ambito delle verifiche dei sistemi d'informazione del SIC, l'AVI-AIn attribuisce particolare importanza al rispetto dei termini di conservazione dei dati nonché alla legalità e all'adeguatezza della gestione degli accessi. Per i dati dei suoi sistemi d'informazione, il SIC prevede più di dieci termini di conservazione, che vanno da sei mesi a 45 anni. Il rispetto di questi termini, conformemente alla legislazione, viene perlopiù garantito da programmi di cancellazione automatica. L'AVI-AIn verifica la cancellazione sulla base di controlli a campione nei sistemi d'informazione.

«Le nuove tecnologie non comportano solo rischi per la sicurezza del Paese, ma possono anche influire positivamente sul lavoro dei servizi informazioni.»

La gestione degli accessi comporta notevoli sfide per il SIC. Per ragioni di informazione e protezione dei dati, il personale può avere accesso solo ai dati di cui necessita per il proprio lavoro. In seguito a cambiamenti interni, ma anche in caso di arrivo o partenza di collaboratrici e collaboratori, le autorizzazioni devono essere adeguate tempestivamente. Il SIC ha creato appositi processi a tal fine e l'AVI-AIn verifica le autorizzazioni di accesso sulla base di controlli a campione nei sistemi d'informazione. Inoltre, può chiedere al personale di mostrarle le opzioni di accesso ai sistemi d'informazione nelle postazioni di lavoro.

Ritardo nel trattamento delle informazioni

Per i servizi informazioni è importante che le informazioni acquisite o ricevute siano inserite il più rapidamente possibile nei sistemi d'informazione previsti a tal fine. Per ragioni di protezione delle informazioni, a volte i dati acquisiti vengono dapprima memorizzati temporaneamente in file particolarmente protetti. Solo successivamente vengono riversati nei sistemi d'informazione ai quali il personale ha accesso per analizzare le informazioni e riutilizzarle nei prodotti di intelligence. Inoltre, talvolta le informazioni devono essere anonimizzate prima di essere inserite in un sistema d'informazione. L'AVI-AIn presta quindi molta attenzione alla verifica di questi processi.

4.3 Sviluppi futuri

I servizi informazioni devono essere in grado di anticipare i cambiamenti sociali e tecnologici che si rivelano negativi per la sicurezza della Svizzera. Tuttavia, le nuove tecnologie non comportano solo rischi per la sicurezza del Paese, ma possono anche influire positivamente sul lavoro dei servizi informazioni. Un motore di ricerca trasversale del SIC introdotto sei anni fa ha per esempio facilitato notevolmente il lavoro al personale.

Tutti e tre i servizi osservano gli sviluppi tecnologici e li impiegano per le loro attività informative. Un nuovo sistema di riconoscimento facciale permetterà al SIC di visualizzare le immagini memorizzate nei suoi sistemi in forma aggregata e in riferimento a specifiche persone (ne riportiamo le pagine 18 e seguenti).

Da parte sua, il SIM promuove in misura sempre maggiore l'analisi delle immagini satellitari, mentre il COE sta valutando in che modo sia possibile compensare con altri sensori tecnici la sorveglianza del ridotto traffico di radiocomunicazione a seguito dell'utilizzo di nuovi mezzi di comunicazione.

4.4 Nuova gestione di dati: ripercussioni sulla LAIn

Nella maggior parte dei casi, nelle leggi che trattano il tema della gestione dei dati viene utilizzata l'espressione «sistema d'informazione». La LAIn non fa eccezione. L'articolo 47 LAIn riporta i diversi sistemi d'informazione gestiti dal SIC. Nel messaggio concernente la legge sulle attività informative si precisa che le informazioni acquisite dal SIC o da esso ricevute vanno archiviate, in funzione della tematica, della fonte e del grado di sensibilità dei dati, in una rete integrata di sistemi d'informazione⁷.

È possibile che il collegamento – a livello di legge – tra l'espressione «sistema d'informazione» e gli scopi di trattamento previsti non corrisponda più ai moderni concetti di gestione dei dati. Nella nuova legge sulla protezione dei dati, per esempio, si rinuncia anche alla definizione di «collezione di dati». La motivazione addotta è che, grazie alle nuove tecnologie, i dati possono oggi essere gestiti come una collezione anche quando sono disseminati⁸.

Il progetto di revisione della LAIn prevede un adeguamento delle disposizioni legale riguardanti i sistemi d'informazione del SIC: il termine «informazioni» sarà sostituito con il termine «dati» e i dati saranno attribuiti a diverse categorie conformemente disposizioni di legge. Il contenuto di queste categorie corrisponderà approssimativamente a quello degli attuali sistemi d'informazione descritti nella LAIn.

⁷ FF 2014 1885, in particolare pag. 1887.

⁸ FF 2017 5939, in particolare pag. 6015.

5. Attività di vigilanza

Secondo la prassi introdotta lo scorso anno, anche nel presente rapporto di attività l'AVI-AIn non riferisce in merito a tutte le verifiche condotte. Abbiamo definito delle priorità, alcune verifiche sono trattate in un modo più dettagliato, mentre altre sono solo menzionate. Sul sito Internet dell'AVI-AIn è comunque disponibile un riassunto dei risultati di ogni verifica⁹.

5.1 Piano di controllo

L'AVI-AIn allestisce per ogni anno un piano di controllo orientato ai rischi¹⁰, che prevede verifiche nei seguenti ambiti:

- «Strategia e pianificazione»;
- «Organizzazione»;
- «Collaborazione»;
- «Acquisizione»;
- «Risorse»;
- «Trattamento dei dati/archiviazione».

Per il 2021 l'AVI-AIn aveva previsto in totale 18 verifiche. Oltre alle verifiche previste, ha svolto la verifica 20-3 «Responsabilità e sfere di competenza tra il settore SIC A¹¹ e il SIM», che era in programma per il 2020, nonché una verifica straordinaria nell'ambito HUMINT. Ha invece rinunciato completamente alle verifiche 20-1 «Gestione dei cambiamenti» e 21-3 «Sicurezza all'interno del SIC»: questo sia a causa di una mancanza temporanea di risorse umane sia perché, nel lasso di tempo intercorso tra la pianificazione e la realizzazione delle verifiche, le circostanze reali sono cambiate a tal punto da far venire meno la loro utilità. Singoli aspetti delle verifiche pianificate sono già stati inclusi in altre verifiche o saranno presi in considerazione nell'ambito di verifiche future. Lo svolgimento della verifica 21-16 «Servizi di telecomunicazione» è stato avviato nel 2022.

Nell'anno in esame, sulla base degli eventi e degli sviluppi del momento, l'AVI-AIn ha eseguito in tre casi accertamenti singoli

a breve termine in vista di una possibile verifica. Le conoscenze così acquisite sono in parte confluite in verifiche in corso di svolgimento oppure previste.

5.2 Verifiche nel 2021

5.2.1 Strategia e pianificazione

Nell'ambito «Strategia e pianificazione» vengono svolte verifiche su temi che riguardano la pianificazione strategica delle autorità di intelligence della Svizzera a breve, medio e lungo termine nonché la definizione dei loro obiettivi. Nel 2021 per questo ambito era prevista la seguente verifica:

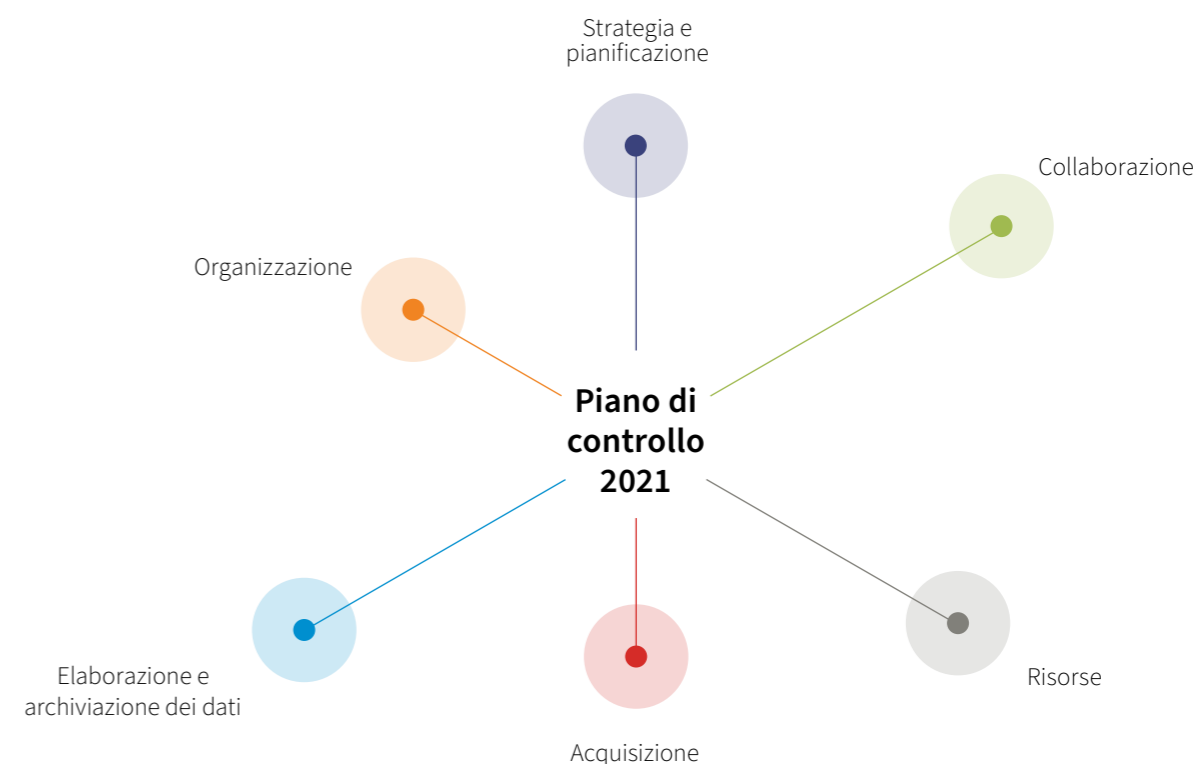
- **21-1 Impiego dei collaboratori del SIC nelle rappresentanze svizzere all'estero (SIC).**

Si trattava di un follow-up della verifica 19-2 «Gestione delle informazioni d'intelligence tra il sensore «addeito alla difesa» e il SIC» e l'obiettivo era, tra le altre cose, quello di controllare l'attuazione della raccomandazione. Per questo riferiamo in merito alla verifica 21-1 al numero 5.4 («Controlling») del presente rapporto.

5.2.2 Organizzazione

Nell'ambito «Organizzazione» l'AVI-AIn verifica che i servizi e i loro processi siano allestiti in maniera tale da adempiere il mandato legale in modo conforme alla legge, adeguato ed efficace.

Nel 2021 l'AVI-AIn ha condotto la verifica 20-3 «Responsabilità e sfere di competenza tra il settore SIC A e il SIM», che avrebbe dovuto svolgersi l'anno precedente. I risultati sono illustrati nel presente rapporto. Conformemente al piano di controllo 2021 erano inoltre previste le seguenti verifiche:



- **21-2 Protezione delle infrastrutture critiche/Cyber Defence (SIC/COE);**
- 21-3 Sicurezza all'interno del SIC (SIC);
- **21-4 Estremismo violento di destra (SIC).**

Tuttavia, la verifica 21-3 «Sicurezza all'interno del SIC» non è stata effettuata.

20-3 Responsabilità e sfere di competenza tra il settore SIC A e il SIM (SIC/SIM)

La verifica era volta soprattutto a stabilire se i prodotti del SIC e del SIM sono abbastanza distinti l'uno dall'altro. Inoltre, è stato esaminato se, dove tali prodotti si sovrappongono, le potenziali sinergie, come lo scambio reciproco di know-how tecnico, vengono sufficientemente sfruttate. Questa verifica era prevista per il 2020, ma è stata rimandata a causa di alcune riorganizzazioni nel settore analisi del SIC. Si è quindi svolta nel settembre del 2021. L'AVI-AIn ha effettuato analisi approfondite dei prodotti e delle forme di cooperazione dei servizi controllati, tenendo conto dei mandati di base e dell'accordo di cooperazione tra il SIC e il SIM, e ha constatato che sono pochi i temi per i quali è possibile una sovrapposizione di aree di interesse nelle attività di analisi del SIC e del SIM.

Per evitare doppioni, tra i rispettivi settori del SIC e del SIM ha luogo uno scambio regolare e in parte formalizzato. Tra le altre cose, i servizi si informano a vicenda sulla loro produzione prevista e mettono i loro prodotti a disposizione dell'altro

servizio. Questo scambio di informazioni si riflette anche nei prodotti stessi, che tendono a completarsi piuttosto che a ripetersi quando si tratta di aree di interesse comune. Spesso si trovano prodotti che, partendo dalla stessa situazione iniziale, trasmettono prospettive diverse a seconda dei casi. L'AVI-AIn è quindi giunta alla conclusione che la distinzione tra il settore analisi del SIC e quello del SIM è adeguata ed efficace.

21-2 Protezione delle infrastrutture critiche/Cyber Defence (SIC/COE)

Nel rapporto sulla situazione «La sicurezza della Svizzera 2021», il SIC fa notare che la pressione digitale accentuata dalle misure di protezione prese contro la pandemia ha allargato la superficie utile per i ciberattacchi. Le numerose imprese svizzere che offrono accessori e servizi ai gestori di infrastrutture critiche nel Paese e all'estero sono obiettivi interessanti anche per gli attori statali. I ciberattacchi classici, come pure il ciberspionaggio, il cibersabotaggio e il ciberterrorismo rivolti direttamente contro le infrastrutture critiche costituiscono solo una piccola parte delle minacce informatiche globali identificate. Secondo il SIC, finora le infrastrutture critiche in Svizzera non sono state un bersaglio diretto degli atti di sabotaggio. Tuttavia, il SIC ritiene che questo sia l'ambito con il potenziale di danno più elevato, poiché i servizi infrastrutturali corrispondenti, come la fornitura di elettricità o i servizi di telecomunicazione, sono considerati cruciali per il funzionamento della società.

⁹ <https://www.ab-nd.admin.ch/it/pruefplan-und-pruefberichte.html>

¹⁰ Cfr. Rapporto di attività 2020 dell'AVI-AIn, pagina 9.

¹¹ SIC, settore analisi

Vista l'indiscutibile presenza di questi rischi, l'AVI-AIn ha verificato se i servizi SIC e COE possiedono competenze e capacità qualitative e quantitative sufficienti per acquisire le informazioni necessarie¹² e per perturbare, impedire o rallentare eventuali attacchi alle infrastrutture critiche.¹³

L'unità Ciber del SIC, la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (OIC¹⁴ MELANI) e determinate componenti dell'esercito sono gli attori chiave nella lotta contro le cyberminacce e fanno parte di una struttura organizzativa complessa e interdipartimentale per la protezione delle infrastrutture critiche e la ciberdifesa. Il compito principale del SIC, con il coinvolgimento del COE, è quello di identificare e attribuire gli attacchi informatici utilizzando mezzi di intelligence. Inoltre, il SIC supporta i gestori di infrastrutture critiche con la presentazione della situazione informatica aggiornata. I mezzi del COE sono utilizzati dal SIC per l'analisi tecnica delle cyberminacce.

All'interno del SIC l'analisi tecnica e l'analisi operativa sono riunite nell'ambito Ciber. Parallelamente, anche il COE dispone di un'unità Cyber Threat Intelligence (CTI), integrata nel settore Cyber Network Operations (CNO), che si occupa delle analisi delle cyberminacce. L'unità Ciber del SIC si considera chiamato in causa nel relativo campo d'azione quando si verificano incidenti rilevanti sotto il profilo della politica di sicurezza che possono essere attribuiti a un altro Stato. Le semplici attività dei cybercriminali non rientrano nel suo settore di compiti.

In caso di approvazione di una richiesta del SIC di procedere contro gli autori di un attacco informatico conformemente all'articolo 37 capoverso 1 LAln, il SIC incaricherebbe il COE di eseguire il contrattacco, in quanto internamente non dispone

delle forze necessarie per sferrare un ciberattacco. Secondo la Strategia Ciber DDPS, infatti, tali contromisure sono di competenza dell'esercito. Una forma di cooperazione che va oltre il puro rapporto mandante/mandatario è rappresentata dal Joint Cyber Technical Analysis Centre (JCTAC): non si tratta di una nuova unità organizzativa, bensì dell'unione tra il personale del SIC e quello del COE per procedere congiuntamente all'analisi tecnica delle cyberminacce.

Dalla verifica è emerso che il SIC e il COE dispongono delle competenze necessarie e che l'interazione tra i due servizi funziona.

Accertamento singolo sull'ambito Ciber del SIC

Dal maggio del 2021 l'AVI-AIn è a conoscenza della presenza di irregolarità nell'ambito Ciber del SIC. Ha quindi seguito da vicino i conseguenti accertamenti interni del SIC, ponendo domande ove necessario. In linea di principio, siamo d'accordo con il modo di procedere del SIC e del DDPS. Per noi, il chiarimento della rilevanza penale è molto importante. Anche in futuro continueremo a seguire da vicino gli ulteriori sviluppi, intervenendo se necessario. Finora non abbiamo ritenuto che ulteriori accertamenti da parte nostra (p. es. una verifica) potessero apportare un valore aggiunto.

21-4 Estremismo violento di destra (SIC)

Il SIC è responsabile dell'acquisizione e del trattamento delle informazioni per l'individuazione tempestiva e la prevenzione delle minacce alla sicurezza interna ed esterna della Svizzera. Questo vale anche se le minacce derivano dall'estremismo violento (abbreviazione tedesca è GEX).¹⁵

«Il fatto di essere sempre in bilico tra il trattamento dei dati consentito e auspicato e quello vietato in quest'ambito è molto difficile per il personale del SIC.»

Il SIC e le sue attività nel campo dell'estremismo violento di destra (abbreviazione tedesca è REX) – come parte dell'ambito GEX – sono stati ripetutamente messi in discussione e criticati da più parti. Da un lato, si rimprovera al SIC di essere «cieco dall'occhio destro» e di non prendere abbastanza sul serio questa tematica¹⁶, dall'altro il SIC deve continuamente confrontarsi con le accuse di procurarsi illegalmente informazioni sulle attività politiche¹⁷.

Secondo il rapporto del SIC «La sicurezza della Svizzera 2020», le persone facenti parte degli ambienti di estrema destra sono restie a ricorrere alla violenza. In Svizzera il rischio maggiore di attentati ispirati all'estrema destra sarebbe quindi rappresentato da individui isolati con posizioni di estrema destra, ma senza una solida appartenenza ai gruppi estremisti violenti tradizionali. Nel rapporto del 2021 il SIC riferisce che gli ambienti di estrema destra hanno un potenziale di minaccia significativo. I gruppi esistenti sono stati sciolti più volte e nuovi gruppi hanno visto la luce. Tuttavia, nell'anno in esame si è constatato «solo» un evento connesso a violenza.

Uno degli obiettivi della verifica 21-4 dell'AVI-AIn era quello di controllare se, in seno al SIC, esistono concetti e processi adeguati per l'ambito REX, se questi vengono attuati in modo efficace e se le informazioni sono gestite in modo conforme alla legge. Durante le sue ispezioni, l'AVI-AIn ha constatato che il SIC dispone di numerosi concetti e processi per il trattamento dell'ambito REX da parte del servizio informazioni.

Il SIC non può né acquisire né trattare informazioni sull'attività politica e sull'esercizio della libertà di opinione, di riunione o

di associazione in Svizzera. Si tratta dei cosiddetti limiti posti al trattamento dei dati¹⁸.

Allo stesso tempo, tuttavia, il SIC deve individuare tempestivamente i pericoli provenienti dall'estremismo violento di destra che minacciano la sicurezza interna ed esterna della Svizzera. Il fatto di essere sempre in bilico tra il trattamento dei dati consentito e auspicato e quello vietato in quest'ambito è molto difficile per il personale del SIC, che nel suo lavoro quotidiano è chiamato a operare diverse distinzioni:

- In che modo l'estremismo differisce dall'estremismo violento e dal terrorismo?
- Qual è la definizione esatta di estremismo violento¹⁹ e in quali casi si parla di azioni di organizzazioni che commettono, incoraggiano o approvano atti violenti²⁰?
- In quali casi una determinata azione rientra nell'ambito GEX (e può quindi essere trattata dal SIC) e in quali, invece, è considerata attività politica ed esercizio della libertà di opinione, riunione o di associazione in Svizzera (e pertanto non può essere trattata dal SIC)?²¹
- In quali casi il SIC può comunque trattare informazioni sull'attività politica e sull'esercizio della libertà di opinione, di riunione o di associazione in Svizzera se sussistono indizi concreti che tali persone esercitano i propri diritti per preparare o eseguire attività di estremismo violento?²²

Partendo da queste domande e considerazioni, il SIC ha creato diversi strumenti per fornire supporto al personale nel lavoro quotidiano. Grazie a una raccolta di casi (casistica) su cui basarsi, per esempio, in futuro per le collaboratrici e i collaboratori sarà più facile prendere decisioni in casi analoghi.

¹² Art. 6 cpv. 1 lett. a n. 4 LAln

¹³ Art. 37 cpv. 1 LAln

¹⁴ Operation Information Center, settore di MELANI

¹⁵ Art. 6 cpv. 1 lett. a n. 5 LAln

¹⁶ P. es. postulato 02.3059; postulato 17.3831; ora delle domande/domanda 19.5677; ora delle domande/domanda 21.7312; «Die braune Gefahr – Die Schweiz ist keine Insel», SRF, 12 maggio 2019; «Wie neutral ist unsere Polizei?», Walliser Bote, 23 luglio 2020; «Geheimdienst soll Rechtsextreme ins Visier nehmen», Zeitung für die Region Basel, 25 maggio 2021.

¹⁷ P. es. interpellanza 19.3868; «Geheimdienst überwacht Menschenrechtsorganisation seit 15 Jahren», Netzpolitik.org, 10 agosto 2021

¹⁸ Art. 5 cpv. 5 LAln

¹⁹ Art. 6 cpv. 1 lett. a n. 5 LAln

²⁰ Art. 19 cpv. 2 lett. e LAln

²¹ Art. 5 cpv. 5 LAln

²² Art. 5 cpv. 6 LAln

«Il SIC deve far sì che la LAIn venga attuata conformemente alle disposizioni sia in seno al SIC che presso i SICant attraverso adeguate misure di garanzia della qualità e di controllo. »

Un metodo per rispettare i limiti posti al trattamento dei dati è l'anonimizzazione: secondo la legge, le informazioni non consentite ma acquisite sull'attività politica e sull'esercizio della libertà di opinione, di riunione o di associazione in Svizzera devono essere anonimizzate. Nell'ambito della verifica 21-4 l'AVI-AIn ha constatato la presenza di incoerenze interne per quanto riguarda l'anonimizzazione dei prodotti/delle informazioni in relazione ai limiti posti al trattamento dei dati.

Un altro riferimento importante per il lavoro quotidiano del personale del SIC è la lista d'osservazione. Si tratta di uno strumento di direzione politica del Consiglio federale, che approva la lista ogni anno. La lista d'osservazione elenca le organizzazioni e i gruppi che è fondato supporre minaccino la sicurezza interna o esterna della Svizzera²³ e consente, per tali organizzazioni e gruppi, di superare i limiti posti al trattamento dei dati²⁴.

Con la verifica 21-4 l'AVI-AIn ha controllato l'adeguatezza della procedura di verifica applicata dal SIC ai fini dell'inclusione, nella lista d'osservazione, di organizzazioni che operano nell'ambito REX²⁵. Ha analizzato la procedura del SIC sulla base di controlli a campione e l'ha giudicata adeguata.

Sempre nel quadro dei suoi controlli a campione, l'AVI-AIn non ha constatato irregolarità neanche per quanto concerne la legalità della gestione delle informazioni. Ha inoltre interpellato terzi per verificare se le informazioni sul fenomeno REX sono state riferite e trasmesse in modo efficace. I terzi interpellati hanno dichiarato di ritenere fundamentalmente efficaci le informazioni ricevute dal SIC.

5.2.3 Collaborazione

In questo ambito rientrano temi che riguardano la collaborazione nazionale e internazionale dei servizi. A tale proposito, una parte rilevante dell'attività di verifica annuale dell'AVI-AIn ha per oggetto i SICant. Quest'anno l'AVI-AIn riferisce in merito alle verifiche sotto forma di riassunti.

Nel 2021 l'AVI-AIn ha svolto le seguenti verifiche in questo ambito:

- **21-5 Garanzia della qualità del SIC con i servizi informazioni cantonali (SICant) (SIC);**
- **21-6 Controllo SICant BS (SIC/SICant);**
- **21-7 Controllo SICant BL (SIC/SICant);**
- **21-8 Controllo SICant AR (SIC/SICant);**
- **21-9 Controllo SICant AI (SIC/SICant);**
- **21-10 Controllo SICant AG (SIC/SICant);**
- **21-11 Controllo SICant VD (SIC/SICant);**
- **21-12 Controllo SICant NE (SIC/SICant).**

21-5 Garanzia della qualità del SIC con i servizi informazioni cantonali (SICant) (SIC)

La garanzia della qualità è una misura di riduzione dei rischi. Oltre a svolgere le verifiche periodiche nei SICant, l'AVI-AIn ha anche verificato l'efficacia di tale misura in seno a questi ultimi. Ciò consente di assicurare, in coordinamento con l'AVI-AIn, una corretta vigilanza sui SICant. Garantire in maniera affidabile e gestibile la qualità è importante ai fini della bontà dei dati e delle informazioni del SIC e dei SICant. Pertanto, il SIC deve far sì che la LAIn venga attuata conformemente alle disposizioni sia in seno al SIC che presso i SICant attraverso adeguate misure di garanzia della qualità e di controllo. Tale compito spetta all'organo di controllo della qualità del SIC (CQ SIC), integrato nella divisione Gestione delle informazioni/Ciber.

Il CQ controlla a campione almeno una volta l'anno la legalità, l'adeguatezza, l'efficacia e l'esattezza del trattamento dei dati in tutti i sistemi d'informazione del SIC. A tal fine allestisce un piano di controllo e, tra le altre cose, verifica periodicamente la rilevanza e l'esattezza dei rapporti dei SICant registrati nel sistema. Inoltre, cancella i dati risultanti da accertamenti preliminari dei SICant la cui registrazione risale a oltre cinque anni prima, nonché i dati che i SICant propongono di cancellare. Infine, provvede alla formazione interna in materia di protezione dei dati.

Il CQ SIC sceglie sempre la stessa procedura per effettuare i controlli a campione presso i SICant. Le singole fasi di questa procedura sono programmate con indicazione delle scadenze e attribuite in modo chiaro al personale competente del CQ SIC. Queste fasi comprendono, tra le altre cose, l'assegnazione del mandato, il rilevamento di dati statistici in base a criteri uniformi, un questionario basato sulle statistiche rilevate, il parere del SICant in merito al questionario e il rapporto finale. Tale rapporto viene presentato per consultazione alla direzione SIC e infine approvato dal direttore di quest'ultimo. Nell'ultima fase, i SICant ricevono il rapporto definitivo e il CQ SIC monitora l'attuazione delle sue eventuali raccomandazioni. Il coinvolgimento della direzione del SIC e l'approvazione definitiva da parte del direttore contribuiscono anche a garantire il necessario livello di considerazione di questi rapporti presso i SICant.

Il CQ SIC adempie adeguatamente ed efficacemente proprio mandato di controllo presso i SICant. Lo dimostra, per esempio, il processo sviluppato dallo stesso CQ SIC per i controlli a campione, il quale garantisce che i campioni vengano raccolti sempre nello stesso modo e sulla base di azioni identiche. L'AVI-AIn ne ha avuto la conferma in occasione di due controlli a campione eseguiti. Mandati interni chiari e l'applicazione costante del principio del doppio controllo assicurano che i controlli siano eseguiti in modo efficiente e che possano essere individuati i relativi rischi.

Garantendo un coordinamento interno al SIC e con i piani di controllo dell'AVI-AIn, nonché tenendo conto dei risultati di verifiche precedenti, il CQ SIC coordina le sue attività di controllo presso i SICant in modo adeguato ed efficace. Questo garantisce che lo stesso SICant non venga controllato due volte in un anno, sebbene ciò sia possibile all'occorrenza. Inoltre, i controlli interni al SIC sono distribuiti tra diverse persone. In questo modo si garantisce che, per quanto concerne i trattamenti di dati verificati, vengano presi in considerazione anche gli aspetti operativi e quelli legati alla sicurezza tecnica.

Da 21-6 a 21-12: verifiche dei SICant Basilea Città, Basilea Campagna, Appenzello Esterno, Appenzello Interno, Argovia, Vaud e Neuchâtel (SIC/SICant)

Nel 2021 l'AVI-AIn ha verificato le attività informative dei SICant dei Cantoni Argovia, Appenzello Esterno e Interno, Basilea Città e Campagna, Neuchâtel e Vaud nonché la loro collaborazione con il SIC. Pertanto, dall'inizio della sua attività di vigilanza a oggi, l'AVI-AIn ha complessivamente sottoposto a verifica 17 SICant²⁶. I nove SICant che ancora mancano saranno verificati nei prossimi due anni.

Da tutte le verifiche dei SICant effettuate nel corso del 2021 è risultato che la collaborazione tra il SIC e i SICant è in linea di principio buona in tutti gli ambiti dell'intelligence. Tuttavia, per quanto riguarda l'attuazione di azioni operative congiunte, entrambe le parti auspicano un migliore coordinamento. Le divergenze di opinioni tra il SIC e singoli SICant sulla valutazione annuale della prestazione sono state appianate nell'ambito di colloqui chiarificatori.

I SICant dispongono di buone o addirittura ottime conoscenze di intelligence ed eseguono i mandati del SIC in modo conforme alla legge e puntuale nonché con una qualità soddisfacente per il SIC. Il SIC mette a disposizione dei SICant, nella

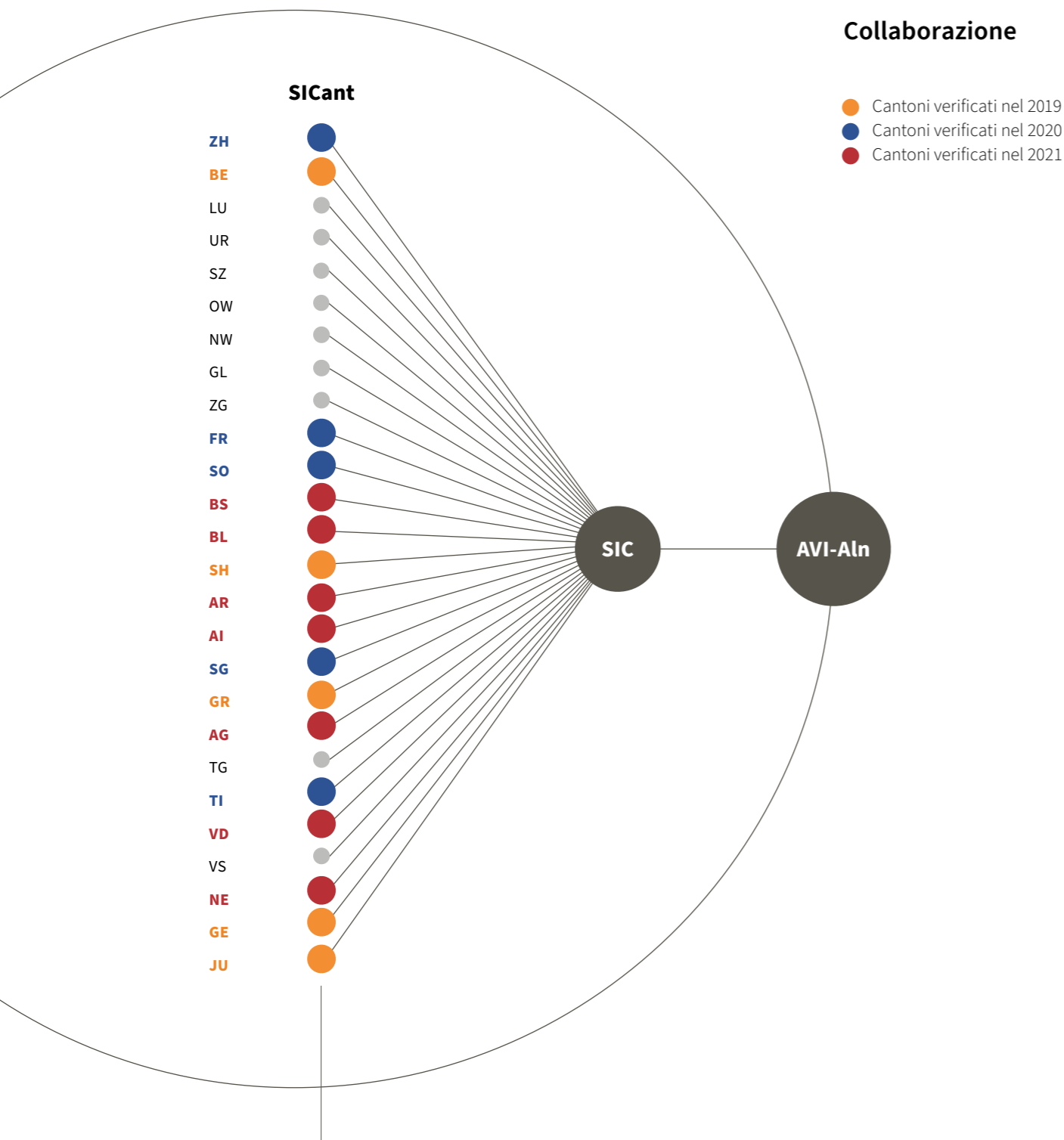
²³ Art. 70 cpv. 1 lett. b e art. 72 LAIn

²⁴ Art. 5 cpv. 8 LAIn

²⁵ Art. 72 LAIn

²⁶ Nel 2020 l'AVI-AIn ha verificato i SICant dei Cantoni San Gallo, Zurigo, Ticino, Soletta e Friburgo, mentre nel 2019 era stata la volta di Berna, Grigioni, Ginevra, Giura e Sciaffusa.

Collaborazione



150 Posti a tempo pieno



postazione di lavoro decentralizzata²⁷, diverse applicazioni e archivi di intelligence tra cui un sistema per la gestione dei mandati e un'applicazione specialistica (App Spec SICant) che consente ai Cantoni di registrare gli oggetti in modo strutturato²⁸. Presso i SICant l'AVI-AIn non ha constatato la presenza né di collezioni di dati proprie né di dati personali il cui trattamento non fosse disciplinato da una base legale. Nell'App Spec SICant sono stati invece trovati alcuni dati che non erano stati registrati in concomitanza con gli eventi/le constatazioni a essi riferiti. È quindi possibile che tali dati siano stati conservati nell'applicazione per un periodo più lungo dei cinque anni previsti. Questo errore nei dati di registrazione è dovuto presumibilmente a una precedente migrazione di dati (2017/2018) e dovrebbe essere eliminato nei prossimi due anni grazie al funzionamento del sistema di cancellazione automatica. L'AVI-AIn continuerà a seguire l'evolversi della situazione in coordinamento con il CQ SIC.

5.2.4 Acquisizione

L'acquisizione di informazioni è un compito fondamentale dei servizi informazioni. A tal fine questi ultimi possono ricorrere a diversi mezzi. Tra questi, gli strumenti che interferiscono in modo più invasivo nella sfera privata delle persone interessate sono oggetto di un'attenzione particolare da parte dell'AVI-AIn. Nel 2021 l'AVI-AIn ha svolto anche una verifica straordinaria nell'ambito HUMINT, che era stata previamente annunciata al SIC.

Nel 2021 l'AVI-AIn ha svolto le seguenti verifiche nell'ambito «Acquisizione»:

- **21-13 Gestione del rischio per gli impegni all'estero (SIC)**
- **21-14 Operazioni (SIC)**
- **21-15 HUMINT (SIC)**
- 21-19 Verifica straordinaria HUMINT (SIC)

21-13 Gestione del rischio per gli impegni all'estero (SIC)

Il SIC impiega personale per attività operative all'estero. Tra le destinazioni vi sono anche Paesi in cui i principi dello Stato di diritto sono solo parzialmente rispettati o non sono rispettati affatto oppure aree in cui la sicurezza può essere compromessa. In singoli casi il SIC si avvale del supporto di terzi. Per il personale impiegato, le acquisizioni all'estero comportano rischi, pertanto il SIC deve assicurarsi che questi ultimi non siano sproporzionati rispetto al valore atteso delle informazioni²⁹ e provvedere alla protezione delle sue collaboratrici e dei suoi collaboratori impiegati all'estero³⁰. Sono necessari controlli e processi interni per garantire che tali disposizioni possano essere rispettate. Di conseguenza, è importante una gestione dei rischi adeguata ed efficace.

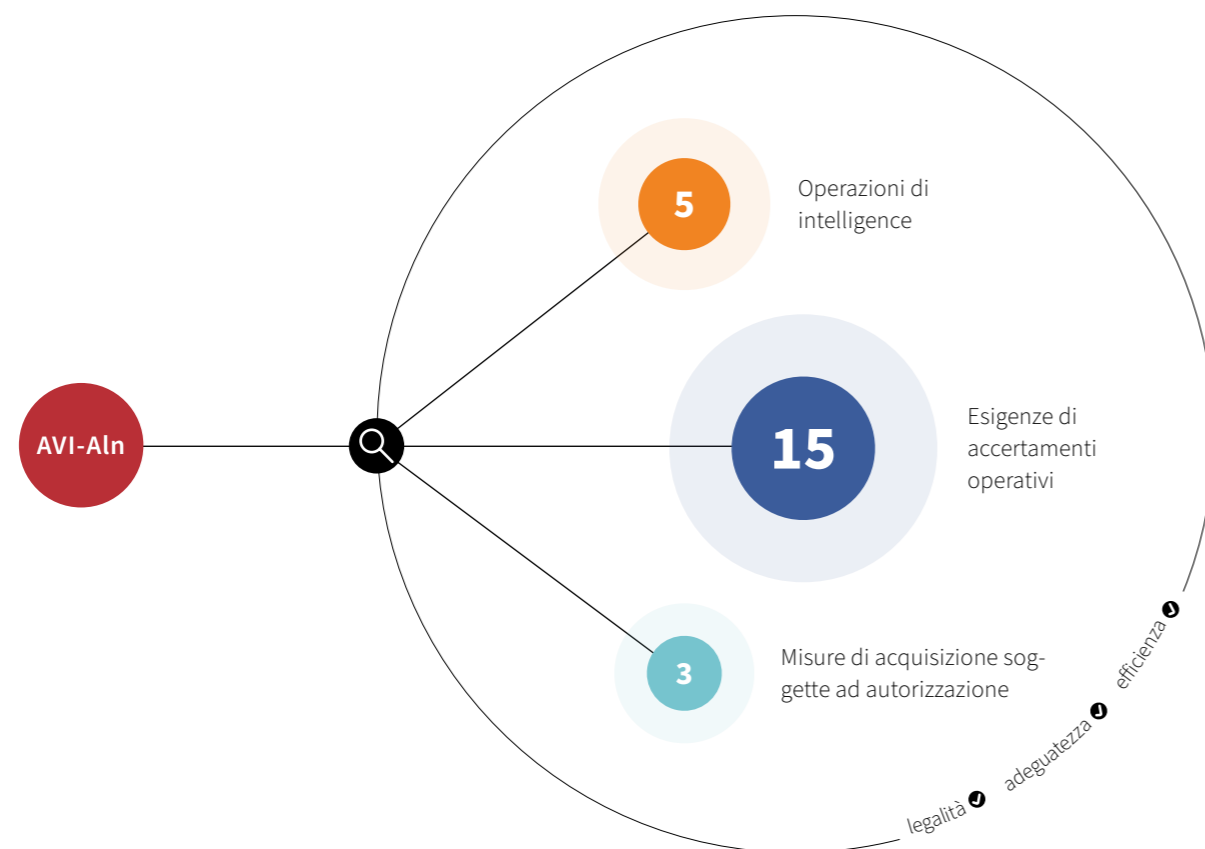
In questa verifica l'AVI-AIn si è concentrata in particolare su impieghi operativi in tre ambiti del SIC. Oltre a effettuare interviste e a esaminare i documenti, sono stati analizzati a titolo di confronto anche i modi di procedere del DFAE e di fedpol per quanto concerne gli impieghi all'estero.

²⁷ La postazione di lavoro decentralizzata è un segmento all'interno della rete protetta SiLAN del SIC che consente di accedere ai sistemi di quest'ultimo da una posizione decentralizzata. Sono postazioni di lavoro decentralizzate anche i computer portatili che permettono di lavorare in modo decentralizzato. La postazione di lavoro SICant è la variante di postazione di lavoro decentralizzata che viene messa a disposizione dei servizi informazioni cantonali.

²⁸ Gli oggetti dell'App Spec SICant più utilizzati sono persone, eventi e mezzi di comunicazione.

²⁹ Art. 36 cpv. 3 LAIn

³⁰ Art. 36 cpv. 7 LAIn



L'AVI-AIn ritiene che, nell'ambito degli impieghi all'estero, il SIC garantisca la gestione dei rischi a livello strategico. Tuttavia, è importante aumentare l'adeguatezza della gestione dei rischi per gli impieghi all'estero. L'obiettivo principale è quello di garantire la sicurezza fisica del personale. Inoltre, la direzione degli impieghi all'estero dovrebbe essere centralizzata nel SIC e i processi dovrebbero essere standardizzati. L'AVI-AIn può confermare che il coinvolgimento di terzi in impieghi all'estero rischiosi è conforme alla legge e chiaramente documentato.

21-14 Operazioni (SIC)

Il SIC conduce operazioni di intelligence utilizzando in parte misure di acquisizione soggette ad autorizzazione. I progetti meno critici dal punto di vista temporale e meno rilevanti per la sicurezza, e nel cui ambito vengono utilizzate soltanto misure di acquisizione non soggette ad autorizzazione, vengono attuati come accertamenti operativi. Il SIC riferisce annualmente al Consiglio federale in merito alle operazioni. Per quanto riguarda le esigenze di accertamenti operativi, invece, il capo del DDPS è informato del relativo contenuto solo in determinati casi e secondo necessità.

Nell'ambito di una verifica ripetuta a cadenza annuale, l'AVI-AIn ha analizzato cinque operazioni di intelligence selezionate e 15 esigenze di accertamenti operativi per verificarne la legalità, l'adeguatezza e l'efficacia. Inoltre, tre misure di acquisizione che avevano ottenuto l'autorizzazione e il nullaosta sono state esaminate per determinare se la loro attuazione fosse conforme alle decisioni del Tribunale amministrativo

federale. Negli anni precedenti questi tre ambiti erano stati controllati separatamente, ma viste le numerose interfacce e interdipendenze, l'AVI-AIn ha deciso di combinarle in un'unica verifica.

Negli atti di verifica sono stati inclusi l'esame di documenti e interviste con le specialiste e gli specialisti responsabili in seno al SIC. Sulla base dei risultati di questi atti di verifica, l'AVI-AIn può sostanzialmente confermare il rispetto dei requisiti di legalità, adeguatezza ed efficacia.

21-15 HUMINT (SIC)

L'uso di fonti umane rimane uno dei più importanti strumenti d'intelligence dei servizi informazioni nonostante il notevole ampliamento delle possibilità tecniche di sorveglianza e l'accesso a un numero pressoché infinito di informazioni accessibili al pubblico. Le persone che godono di un particolare accesso a informazioni specifiche sono quindi interessanti e importanti per ogni servizio informazioni.

Nel rapporto «Ispezione a seguito dell'arresto di un'ex fonte del SIC in Germania», la DelCG ha illustrato all'opinione pubblica in che modo il SIC impiega le fonti umane. Nel 2017 un'ex fonte del SIC è stata arrestata in Germania per sospetta attività di spionaggio. La DelCG ha quindi deciso di indagare, con un'apposita ispezione, sui retroscena del caso e sul ruolo del SIC, del Consiglio federale e del Ministero pubblico della Confederazione. L'attuazione delle raccomandazioni del rapporto è ancora oggi alla base del lavoro del SIC con le fonti umane.

«L'AVI-AIn verifica annualmente l'HUMINT nel SIC tramite controlli a campione e, nel quadro di tali verifiche, copre tutta la gestione delle fonti umane.»

L'HUMINT è spesso associata a elevati rischi personali sia per il personale del SIC che per le fonti. Ciò comporta una responsabilità e un obbligo particolari per il SIC, che devono essere presi molto sul serio da quest'ultimo e che sono di conseguenza tenuti particolarmente in considerazione nell'ambito della vigilanza da parte dell'AVI-AIn. I gestori delle fonti devono non solo disporre di conoscenze specialistiche nel rispettivo ambito nonché di una formazione completa nel campo dell'intelligence e conoscere diverse lingue, ma anche avere abilità sociali superiori alla media, tra cui soprattutto competenza interculturale e sensibilità psicologica, per poter affrontare sfide fuori dal comune.

In quanto gestori delle fonti, devono capire che cos'è che motiva le persone e guida i loro comportamenti, indipendentemente dalla loro provenienza o da cosa fanno. Il personale operativo riceve quindi una formazione specifica, per esempio nel campo delle lingue straniere, dell'uso della tecnologia o della gestione di persone. Va inoltre ricordato che il ruolo di gestore delle fonti comporta molte limitazioni nella vita privata.

L'AVI-AIn verifica annualmente l'HUMINT nel SIC tramite controlli a campione e, nel quadro di tali verifiche, copre tutta la gestione delle fonti, compresi i rischi per la sicurezza, le spese e l'impatto concreto dell'analisi delle informazioni ottenute da fonti umane. L'AVI-AIn sceglie quale gestione delle fonti verificare in base ai rischi e, tra le altre cose, conduce interviste con i gestori delle fonti, con la direzione HUMINT e con collaboratrici e collaboratori del settore analisi, che integrano infine le informazioni ottenute in prodotti di intelligence.

Queste verifiche pongono maggiori esigenze in termini di tutela del segreto. Per esempio, i nomi delle fonti e dei gestori delle fonti rimangono segreti, anche per l'AVI-AIn, a meno che non siano rilevanti per le verifiche stesse. Ciò corrisponde al cosiddetto principio della necessità di sapere (need-to-know). In termini concreti, significa che l'accesso ai dati personali viene limitato alle persone che ne hanno assolutamente bisogno per adempiere i loro compiti.

La protezione delle fonti è un bene prezioso che viene anche tutelato dalla legge³¹. Pertanto, in tutte le sue verifiche l'AVI-AIn deve soddisfare le stesse condizioni per garantire tale protezione. Per motivi di protezione dello Stato, l'AVI-AIn non può fornire informazioni sui risultati delle sue verifiche nell'ambito HUMINT nella stessa misura in cui lo fa per altri ambiti.

5.2.5 Risorse

Per poter garantire un'attività informativa efficace, è indispensabile un uso adeguato delle risorse.

Nel 2021 l'AVI-AIn non ha svolto verifiche in questo ambito.

5.2.6 Trattamento dei dati/archiviazione

I servizi trattano informazioni altamente sensibili. Inoltre, le disposizioni legali sono ampie e complesse. Per questo l'Autorità di vigilanza deve prestare particolare attenzione alla legalità del trattamento delle informazioni.

Nel 2021 l'AVI-AIn ha pianificato le seguenti verifiche in questo ambito:

- 21-16 Servizi di telecomunicazione (SIC)
- **21-17 Servizio del SIC selezionato (Quattro P)**
- **21-18 Protezione dei dati all'interno del SIM**

La verifica 21-16 «Servizi di telecomunicazione» è stata avviata soltanto nel quarto trimestre 2021. Alla chiusura redazionale del presente rapporto di attività non erano ancora disponibili risultati rilevanti.

³¹ Art. 35 LAln

21-17 Servizio del SIC selezionato (Quattro P)

Nel 2020 l'AVI-AIn ha deciso di inserire il sistema d'informazione Quattro P nel piano delle verifiche del 2021, poiché tale sistema è utilizzato per registrare ed elaborare un gran numero di viaggi di persone di determinate nazionalità. I dati personali inseriti nel sistema Quattro P servono anche come base per il sistema di riconoscimento facciale utilizzato dal SIC dal 2020 ma sinora soltanto per ricerche nei propri dati. In definitiva, la cerchia degli aventi diritto di accesso a Quattro P è vasta, dato che si tratta della metà dei collaboratori del SIC. Nell'ambito di questa verifica l'AVI-AIn ha analizzato la legalità e l'adeguatezza del funzionamento, dell'utilizzazione e dei contenuti del sistema d'informazione. Inoltre, una delle questioni da verificare riguardava la legalità del sistema utilizzato per il riconoscimento facciale.

Nell'ambito delle loro attività, i responsabili delle verifiche hanno potuto accedere ai sistemi d'informazione Quattro P e IASA SIC, SiLAN file storage e al sistema di riconoscimento facciale. L'AVI-AIn ha così potuto pianificare ed effettuare i suoi controlli a campione in modo indipendente.

Legalità della registrazione e del trattamento dei dati nel sistema Quattro

In un elenco non pubblico, il Consiglio federale enumera i viaggiatori i cui dati devono essere comunicati spontaneamente al SIC³². L'elenco è stilato in funzione della situazione di minaccia attuale. I dati di viaggio all'interno dello spazio Schengen non vengono registrati in Quattro P, non essendovi controlli alle frontiere.

A livello di contenuto, in Quattro P vengono registrati i dati personali seguenti:³³

- cognome, nome, data di nascita, nazionalità;
- numero del documento d'identità, numero del visto, data di validità;
- foto sul documento d'identità;
- luogo, data e descrizione del controllo alla frontiera;
- sesso;
- dati relativi al chip del documento d'identità;
- dati relativi al visto.

Questi dati sono forniti dalle autorità interessate (Corpo delle guardie di confine, servizi di polizia). La selezione dei dati da fornire è effettuata dalle stesse autorità, affinché il SIC riceva soltanto i dati che gli sono destinati in virtù delle disposizioni legali. I dati di minorenni di età inferiore a 16 anni non vengono registrati.

Dopo aver analizzato le disposizioni di legge e la documentazione del sistema d'informazione, per verificare la legalità l'AVI-AIn ha effettuato i seguenti controlli a campione:

- registrazione dei soli viaggi di cittadini di Stati figuranti nell'elenco allestito dal Consiglio federale;
- registrazione di dati di bambini;
- rispetto della durata di conservazione di cinque anni;³⁴
- verifica delle iscrizioni in Quattro P e della loro registrazione in IASA SIC.

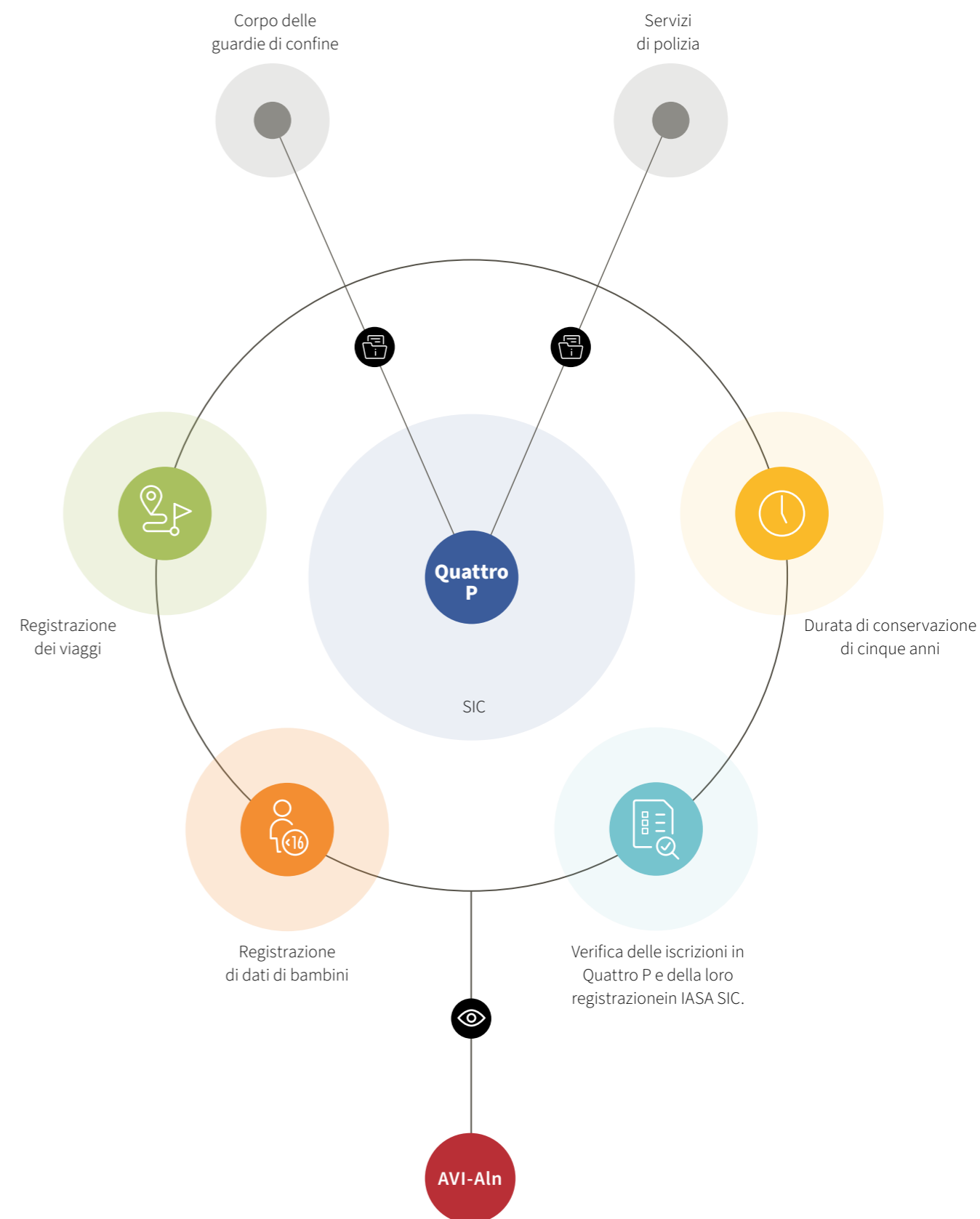
Nell'ambito di questi controlli a campione l'AVI-AIn ha scoperto casi in cui per singoli viaggi i documenti di viaggio erano stati registrati più volte. Per questa ragione ha raccomandato al SIC di studiare e introdurre misure per ridurre il numero di questi casi. Per il resto, alla luce delle verifiche effettuate, l'AVI-AIn ha considerato conforme alla legge il trattamento dei dati in Quattro P.

³² Art. 55 cpv. 4 LAln; l'elenco dei Paesi fa parte dell'elenco previsto all'art. 20 cpv. 4 LAln (fatti e constatazioni che devono essere comunicati spontaneamente).

³³ Allegato 8 OSIME-SIC

³⁴ Art. 55 OSIME-SIC

Quattro P



«Il riconoscimento facciale è un nuovo motore di ricerca la cui conformità alla legislazione sulla protezione dei dati è controversa. Siccome è utilizzato dal SIC, l'AVI-AIn ha deciso di esaminare la legalità del suo impiego.»

Adeguatezza della registrazione e del trattamento dei dati nel sistema Quattro P

Il concetto di adeguatezza comprende l'idoneità, la necessità e il carattere adeguato di un modo di procedere, ossia, nel caso presente, del trattamento dei dati in Quattro P. Se il trattamento è complesso e laborioso, il SIC potrebbe disporre troppo tardi delle informazioni rilevanti per l'adempimento dei suoi compiti.

Considerata la grande quantità di dati forniti, la trasmissione automatica dei dati da parte dei servizi esterni fornitori sembra essere una buona soluzione. Soltanto una piccola percentuale dei dati forniti viene trattata manualmente in seguito. Se la percentuale dei dati trasmessi in modo errato aumenta, il SIC contatta le autorità fornitrici e vengono adottate opportune misure per aumentare la qualità dei dati.

Nel quadro dei controlli a campione effettuati per verificare la legalità della registrazione dei dati, l'AVI-AIn ha constatato che all'incirca nel 25 per cento dei casi la destinazione era indicata come «non definita»³⁵. Pertanto, ha raccomandato al SIC di esaminare insieme agli organi di controllo quali misure potrebbero essere adottate per ridurre questa quota.

Legalità e adeguatezza della gestione degli accessi a Quattro P

Per motivi di sicurezza delle informazioni e protezione dei dati, possono accedere a Quattro P soltanto il personale del SIC che ne ha bisogno per adempiere i propri compiti. Se non sono aggiornate, le autorizzazioni d'accesso non soddisfano il principio del «need-to-know». Processi inadeguati nella gestione degli accessi causano ritardi nell'adeguamento delle autorizzazioni d'accesso. In caso di cambiamento di posto o di partenze di personale, tali autorizzazioni devono essere

tempestivamente adeguate per evitare accessi non conformi alla legge e conseguenti lacune a livello di sicurezza.

Sulla base dei controlli a campione effettuati e dell'analisi dei documenti rilevanti, l'AVI-AIn ha raccomandato di verificare regolarmente le autorizzazioni d'accesso e di cancellare gli accessi non necessari.³⁶

Legalità del sistema di riconoscimento facciale

I sistemi di riconoscimento facciale consentono di identificare persone in fotografie o filmati o in tempo reale. Le immagini presenti in un insieme di dati vengono analizzate in base alla geometria dei volti registrati. Gli elementi chiave caratteristici vengono trasformati in un'impronta facciale consistente in un set di dati digitali. L'impronta facciale è unica come un'impronta digitale. Questi dati sono denominati dati biometrici.³⁷

Il riconoscimento facciale è un nuovo motore di ricerca la cui conformità alla legislazione sulla protezione dei dati è controversa. Siccome è utilizzato dal SIC, l'AVI-AIn ha deciso di esaminare la legalità del suo impiego.

Ha constatato che all'inizio del progetto il SIC ha disposto diversi accertamenti per verificare se il sistema era conforme alla legge. Gli accertamenti condotti sono stati utilizzati per elaborare un regolamento sul trattamento di questi dati e un'analisi delle basi legali. In seguito il progetto è stato sviluppato senza ulteriori verifiche della legalità da parte del servizio giuridico o deli' organo di controllo della qualità del SIC.

Secondo l'AVI-AIn, il sistema di riconoscimento facciale è utilizzato per trattare dati biometrici. La riveduta legge federale sulla protezione dei dati³⁸ (non ancora entrata in vigore) classifica i dati di questo tipo come dati personali degni di particolare protezione. Secondo l'articolo 47 capoverso 2 LAIn, per

ogni sistema d'informazione del SIC il Consiglio federale disciplina il catalogo dei dati personali trattati. Questa materia è stata disciplinata nell'OSIME-SIC, ma il trattamento di dati biometrici non è previsto in nessuno dei sistemi d'informazione ivi menzionati.

Inoltre, il sistema di riconoscimento facciale consente di creare profili di immagini che possono essere completati con metadati. Secondo l'AVI-AIn, questa possibilità porta alla realizzazione di profili della personalità. Alla luce di queste riflessioni, l'Autorità di vigilanza ha formulato diverse raccomandazioni, che riguardavano in particolare anche il coinvolgimento dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) negli ulteriori accertamenti giuridici del SIC.

21-18 Protezione dei dati all'interno del SIM

Nell'ambito della verifica 20-17, l'AVI-AIn aveva esaminato i sistemi informatici rilevanti per le attività informative del SIM. Nell'anno in rassegna, nell'ambito della verifica 21-18, ha esaminato la legalità del trattamento di dati personali in due sistemi, basandosi su una serie di audizioni, sulla consultazione di documenti e su controlli a campione. Tra i vari sistemi d'informazione, sottosistemi e applicazioni speciali autorizzati, ha concentrato la propria attenzione sui sistemi informatici gestiti dal SIM sotto la propria responsabilità. Si tratta del principale strumento di lavoro di quest'ultimo, ossia del Sistema informatico Servizio informazioni militare (Sist Infm SIM), e del sistema BICES per lo scambio di informazioni con Stati esteri³⁹. Secondo la valutazione dell'AVI-AIn, questi sono i sistemi che comportano il maggior rischio potenziale in materia di protezione dei dati, a causa della quantità, del tipo di dati e dei loro destinatari, nonché delle possibili ripercussioni in termini di violazioni dei diritti della personalità degli interessati.

L'AVI-AIn ha constatato che nell'ambito dei propri compiti di legge il SIM tratta dati personali, e che in tale ambito può essere indispensabile anche trattare dati personali degni di particolare protezione o allestire profili della personalità. Tuttavia, nell'esame dei controlli a campione non è incappata in alcun caso del genere. Secondo quanto constatato dall'AVI-AIn, in determinati prodotti del SIM sono presenti dati personali, ma questi dati non sono al centro dell'interesse del servizio. Il SIM è invece concentrato sui propri compiti, e precisamente sull'acquisizione e analisi di informazioni sull'estero rilevanti per l'esercito (in particolare nell'ottica della difesa del Paese), per il servizio di promovimento della pace e per il servizio d'appoggio all'estero. L'acquisizione di informazioni è focalizzata soprattutto sull'estero. Essa non si concentra su persone in Svizzera e queste persone non vengono registrate in modo strutturato nei sistemi del SIM. I dati personali di cittadini svizzeri che vengono rilevati nell'ambito di un servizio d'appoggio in Svizzera (p. es. per il World Economic Forum) sono trasmessi alle autorità competenti svizzere e non possono essere utilizzati in relazione ad attività informative.

I dati personali eventualmente trattati sono i nomi di personalità politiche, di leader stranieri e di esponenti di reti o gruppi armati. Questi dati consentono al SIM di osservare e valutare gli sviluppi strategici militari e quelli delle forze armate. Il servizio concentra la sua attenzione su determinati Paesi o minacce militari e conflitti armati e sugli ambiti d'impiego dell'esercito svizzero all'estero.

Per ogni caso esaminato nell'ambito dei controlli a campione è stato possibile accertare l'esistenza di un collegamento con le attività del SIM. Inoltre, l'AVI-AIn ha chiesto spiegazioni sulle autorizzazioni d'accesso degli utenti e sui processi di archiviazione e cancellazione dei documenti e ha constatato che l'accesso è riservato al personale che ne ha bisogno per l'adempimento dei propri compiti. I prodotti contenuti nei sistemi esaminati ven-

³⁵ Le possibilità a disposizione sono le seguenti: «entrata», «uscita» e «non definita».

³⁶ Art. 5 cpv. 4 OSIME-SIC

³⁷ Fonte: www.kaspersky.de/resource-center/definitions/what-is-facial-recognition, consultato l'ultima volta il 22 novembre 2021

³⁸ RS 235.1

³⁹ Battlefield Information Collection and Exploitation System, piattaforma internazionale della NATO per lo scambio sicuro di informazioni

gono offerti all'Archivio federale e non vengono conservati oltre il termine previsto dalla legge. I sistemi utilizzati dal SIM sono ben documentati. Inoltre, non sono collegati gli uni con gli altri attraverso interfacce comuni che permettano uno scambio automatico dei dati. Questa soluzione limita il rischio di abusi.

Nell'ambito della sua verifica l'AVI-AIn non ha riscontrato in nessuna delle varie fasi l'esistenza di punti che possano mettere in dubbio la legalità del trattamento di dati personali da parte del SIM. Non ha nemmeno scoperto alcun impiego dei dati personali che possa essere considerato abusivo o sproporzionato ai sensi della legislazione o il diritto in materia di protezione dei dati.

Inoltre, ha constatato che per trasmettere dati personali all'estero il SIM può fondarsi su disposizioni specifiche. In generale, i prodotti trasmessi all'estero riguardano analisi della situazione (di carattere militare, politico o di politica militare). Benché non si possa escludere che nei prodotti del SIM compaiano occasionalmente dati personali, non vengono effettuati scambi di dati riguardanti una persona precisa. Inoltre, i prodotti del SIM sono trasmessi soltanto ai servizi di Paesi che condividono i valori occidentali e che possiedono una legislazione in materia di protezione dei dati.

5.3 Consenso

I responsabili delle verifiche dell'AVI-AIn sono stati ricevuti con atteggiamento costruttivo e professionalità dai servizi sottoposti alla vigilanza. Essi hanno potuto accedere senza complicazioni ai documenti e sistemi d'informazione necessari per poter adempiere il loro mandato di verifica. Le persone intervistate erano a loro disposizione. Nonostante le restrizioni dovute alla pandemia di COVID-19, le interviste sono state pianificate tempestivamente e hanno potuto svolgersi. Alle domande complementari è stata data risposta il più rapidamente possibile.

Nell'anno in rassegna l'AVI-AIn ha registrato un notevole aumento delle informazioni e indicazioni passate informalmente, riconducibili perlopiù all'insoddisfazione del personale del SIC. Le informazioni sono state analizzate nella misura di quanto necessario e possibile e integrate nelle attività di verifica o fatte oggetto di accertamenti specifici. Il 13 luglio e il 22 ottobre 2021 il capo del DDPS è stato informato per scritto in merito a tali sviluppi. La questione non è ancora stata trattata esaurientemente e occuperà l'AVI-AIn anche in futuro.

5.4 Controlling delle raccomandazioni

La verifica dell'attuazione delle raccomandazioni non è espressamente disciplinata dalle basi legali in materia di attività informative. D'intesa con il DDPS e con le autorità sottoposte a vigilanza si è convenuto che queste ultime avrebbero informato per scritto il Dipartimento in merito all'attuazione delle raccomandazioni, con copia all'AVI-AIn. Nel 2021 è stata comunicata l'attuazione di 66 raccomandazioni. A fine anno il SIM e il COE avevano attuato tutte le raccomandazioni formulate. A metà anno ha inoltre avuto luogo un incontro con tutti i servizi sottoposti a vigilanza e alla presenza del consulente del capo del DDPS in materia di attività informative per tracciare un bilancio della situazione riguardo alle raccomandazioni in via di attuazione e a quelle già attuate.

Verifica delle raccomandazioni: un esempio concreto

L'entrata in vigore della LAIn ha fornito al SIC una base legale esplicita che gli consente di impiegare i propri collaboratori presso le rappresentanze svizzere all'estero per promuovere i contatti internazionali.⁴⁰ Il SIC sfrutta questa possibilità e impiega persone di collegamento per il servizio informazioni. Perciò, nel 2019 l'AVI-AIn ha esaminato la gestione delle informazioni di intelligence tra gli addetti alla difesa in quanto sensori e il SIC.

⁴⁰ Art. 12 cpv. 2 LAIn

Per la Svizzera gli addetti alla difesa sono uno strumento d'appoggio per la realizzazione degli interessi del Paese in materia di politica estera e di sicurezza. Pur essendo militari, il loro impiego come sensori rientra prioritariamente nelle responsabilità del SIC, il quale è dunque responsabile della loro gestione per quanto riguarda le attività informative.

In seguito a questa verifica, l'AVI-AIn ha raccomandato al SIC di elaborare un piano strategico per definire meglio l'impiego dello strumento delle persone di collegamento per il servizio informazioni e i contatti del servizio con gli addetti alla difesa. A tal fine occorrerebbe migliorare l'adeguatezza ed efficacia in questo ambito delle attività informative.

Nell'anno in rassegna l'AVI-AIn ha effettuato la verifica 21-1 «Impiego dei collaboratori del SIC nelle rappresentanze svizzere all'estero». Un elemento essenziale di questa verifica

consisteva nel verificare l'attuazione della suddetta raccomandazione relativa all'elaborazione di un piano strategico per l'impiego delle persone di collegamento. L'AVI-AIn registra le raccomandazioni formulate in un sistema di monitoraggio e le confronta con le notifiche di esecuzione ricevute dal SIC. Infine, decide se l'attuazione descritta è sufficiente o se deve essere verificata più approfonditamente. In quest'ultimo caso l'attuazione da verificare viene integrata in una verifica già prevista o, come nel caso qui descritto, viene pianificata una verifica apposita.

«Nell'anno in rassegna l'AVI-AIn ha registrato un notevole aumento delle informazioni e indicazioni passate informalmente, riconducibili perlopiù all'insoddisfazione del personale del SIC.»

6. Vista interna

Nel presente capitolo l'AVI-AIn riferisce sempre in merito ad affari interni.

6.1 Personale e formazione continua

L'AVI-AIn continua ad avere un effettivo di dieci collaboratori (9,1 ETP). A fine 2021 due responsabili delle verifiche e un responsabile dell'ufficio hanno deciso di cogliere nuove sfide e di dimettersi dall'AVI-AIn. A fine novembre 2021 una parte dei subentranti era stata trovata e nel primo semestre 2022 l'AVI-AIn sarà di nuovo al completo.

Le possibilità di formazione continua offerte nel 2021 sono state sfruttate. I collaboratori hanno assolto formazioni impegnative a livello di Master e di CAS⁴¹ in ambito tecnico e gestionale. Lo stage già previsto nel 2020 presso il Comité R in Belgio ha dovuto essere rimandato.

Il telelavoro, al quale si è fatto intensamente ricorso a causa delle misure di lotta alla pandemia di COVID-19, è funzionato in modo sostanzialmente soddisfacente, ma questa forma di lavoro presenta dei limiti quando devono essere trattate informazioni classificate. Durante le settimane e i mesi di telelavoro, la mancanza di contatti e scambi diretti si è fatta sentire. Gli strumenti tecnici, infatti, non possono compensare la mancanza di scambi diretti di informazioni. Il telelavoro è una soluzione svantaggiosa per l'introduzione di nuovi collaboratori e potrebbe ritardare considerevolmente la possibilità di svolgere le attività di verifica previste.

6.2 Revisione della LAIn

Nel 2021 l'avamprogetto di revisione della LAIn è stato sottoposto alla consultazione degli uffici. L'AVI-AIn ha avuto la possibilità

di far valere i suoi interessi, segnatamente nella sezione 2 del capitolo 6, che la riguarda direttamente. Il progetto è condotto sotto l'egida del DDPS.

6.3 Legge federale sul principio di trasparenza dell'amministrazione (Legge sulla trasparenza, LTras)

Nell'anno in esame, l'AVI-AIn non ha ricevuto alcuna richiesta di consultare documenti ufficiali.

6.4 Visite

Nel mese di settembre il capo del DDPS si è recato in visita alla sede dell'AVI-AIn e si è informato presso tre postazioni di lavoro in merito alle attività svolte e alle possibilità di cui dispone l'autorità di vigilanza.

Inoltre, nel gennaio 2021, l'AVI-AIn ha invitato la Delegazione delle Commissioni della gestione (DelCG) a renderle visita presso i suoi uffici. Lo scopo dell'invito consisteva nel permettere alle DelCG di farsi un'idea delle attività concrete dell'AVI-AIn. La DelCG non ha dato seguito a questo invito.

6.5 Giurisprudenza

L'AVI-AIn ha seguito gli sviluppi della giurisprudenza a livello nazionale e internazionale. Nell'anno in rassegna ha analizzato internamente e discusso in gruppo alcune sentenze della Corte europea dei diritti dell'uomo. Inoltre, durante la European Oversight Conference tenutasi a Roma, ha ricevuto alcune indicazioni importanti sulla giurisprudenza a livello europeo.

⁴¹ Certificate of Advanced Studies, diplomi di formazione paraprofessionale a livello accademico

7. Coordinamento

L'AVI-AIn deve coordinare la sua attività con le attività di vigilanza parlamentare e con altre autorità di vigilanza della Confederazione e dei Cantoni.⁴² Tuttavia, anche nel 2021, questo coordinamento è stato influenzato dalla pandemia e dalle conseguenti misure e restrizioni di viaggio.

7.1 Contatti nazionali

Riunione con le autorità di vigilanza cantonali

Il 18 agosto 2021, presso la caserma della truppa di Berna, l'AVI-AIn ha tenuto la sua seconda riunione con le autorità di vigilanza cantonali. A questa riunione hanno partecipato 15 organi di vigilanza cantonali, rappresentanti del SIC e due capi di servizi informazioni cantonali. La riunione è servita per la formazione continua, per sviluppare i contatti tra i partecipanti e per lo scambio di informazioni.

Essa si è aperta con le relazioni dei rappresentanti di due organi di vigilanza cantonali (Soletta e Friburgo), che hanno parlato dei frutti della loro attività, delle loro sfide e delle loro aspettative. In seguito due rappresentanti del SIC hanno presentato la loro prospettiva riguardo al controllo della qualità e della sicurezza e al controllo dell'amministrazione generale. Hanno preso la parola anche i capi dei servizi informazioni cantonali di Basilea Città e Friburgo, che hanno illustrato il modo in cui la vigilanza influenza il loro lavoro. Nell'ultima relazione il capo dell'AVI-AIn ha illustrato le attività svolte dalla sua organizzazione dall'ultima riunione del 2018. Nel corso del pomeriggio un dibattito con quattro partecipanti ha permesso di affrontare questioni di principio e fornito spunti di riflessione per le future attività di vigilanza delle attività di servizi informazioni.

Da questa conferenza sono stati tratti i seguenti riscontri:

Per le autorità di vigilanza cantonali, l'attenzione deve essere concentrata principalmente sulla legalità delle attività dei servizi informazioni cantonali. In particolare l'impiego delle fonti, le liste di controllo, il quadro della situazione di minaccia e la delimitazione con il lavoro della polizia pongono sfide continue. A loro volta, la trasparenza, il dialogo e la prossimità sono gli elementi chiave della fiducia.

Il SIC pone in primo piano l'informazione reciproca e il coordinamento dei servizi informazioni cantonali. Inoltre, constata che da quando nel settembre 2017 è entrata in vigore la LAIn sono stati compiuti grandi progressi. Tra i vari servizi informazioni cantonali rimangono comunque opinioni divergenti riguardo al trattamento dei dati e alla collaborazione. Il SIC chiede insistentemente che le irregolarità a qualsiasi livello vengano comunicate il più rapidamente possibile. Secondo il SIC vige il motto «Uniti siamo forti e insieme garantiamo la sicurezza della Svizzera.»

Agli occhi dei servizi informazioni cantonali, la demistificazione delle attività informative è il primo obiettivo della vigilanza. Lo scambio con le autorità di vigilanza funziona generalmente in modo costruttivo. Dà la possibilità di comunicare i bisogni, rafforza la trasparenza e la fiducia e offre un potenziale concreto di sviluppo e miglioramento. Tuttavia, si è constatato che il numero di controlli che un servizio informazioni cantonale subisce da parte di tutte le autorità di vigilanza cantonali e nazionali è straordinariamente elevato (fino a una verifica al mese per un determinato servizio), e che sarebbe auspicabile una migliore pianificazione delle verifiche tra le varie autorità. Inoltre, si è sottolineato che per le misure d'acquisizione soggette ad autorizzazione esistono consistenti ostacoli giuridici. Di conseguenza viene sviluppata l'acquisizione mediante fonti umane.

A giudizio dell'AVI-AIn, le verifiche svolte dall'entrata in vigore della LAIn, la collaborazione con tutti gli attori del settore della vigilanza, il flusso di informazioni e l'impegno dei servizi informa-

⁴² Art. 78 cpv. 2 LAIn.

zioni cantonali sono tutti aspetti chiaramente positivi. Nondimeno, ravvisa un potenziale di miglioramento per quanto riguarda il trattamento dei dati, la gestione delle risorse e l'uso dei mezzi tecnici. L'obiettivo dichiarato è indubbiamente la valorizzazione delle attività informative e al tempo stesso anche della fiducia.

Dopo un lungo periodo di incertezza e i rinvii dovuti alla pandemia di COVID-19, questa riunione si è rivelata un successo. La prossima edizione è prevista nel 2023.

Tribunale amministrativo federale (TAF)

Il 10 settembre 2021 l'AVI-AIn si è incontrata con alcuni rappresentanti del TAF per uno scambio di opinioni su diversi temi, tra cui le misure d'acquisizione soggette ad autorizzazione, gli ultimi sviluppi della giurisprudenza e la revisione della LAIn.

Controllo federale delle finanze (CDF)

Il 21 maggio 2021 la direzione dell'AVI-AIn ha discusso e coordinato insieme a due rappresentanti del CDF in particolare i possibili temi delle verifiche.

Delegazione delle Commissioni della gestione (DelCG)

La direzione dell'AVI-AIn e un collaboratore sono stati invitati a un unico colloquio tenutosi il 20 gennaio 2021. In tale occasione l'AVI-AIn ha presentato il rapporto della verifica «20-13 Accertamenti operativi». A nostro giudizio il rapporto della DelCG sull'AVI-AIn è univoco e disequilibrato. L'AVI-AIn ha preso posizione sulla bozza di rapporto annuale della DelCG in un documento di quattro pagine. Le nostre proposte di modifica sono state per la maggior parte ignorate dalla DelCG senza darcene comunicazione. A nostro modo di vedere questo tipo di rapporto non è utile né alla causa né negli effetti esterni. Per quanto riguarda la vigilanza sulle attività informative deve finalmente poter nascere un dialogo sensato tra le autorità di vigilanza competenti.

Revisione interna DDPS (RI DDPS)

Il 22 gennaio 2021, in occasione di un contatto telefonico, la direzione dell'AVI-AIn e la RI DDPS hanno discusso in particolare

del modo in cui quest'ultima potrebbe eventualmente approfittare delle conoscenze pregresse della prima, di quanto l'attività di vigilanza generi un valore aggiunto per i servizi e dell'eventuale presa in considerazione di una forma di «peer review» per l'attività di controllo dell'AVI-AIn. In quest'ultima ipotesi, l'adeguatezza dei processi di un'autorità di vigilanza, per esempio, sarebbe verificata da un'altra autorità di vigilanza.

Organo di vigilanza cantonale di Basilea Città (OVC BS)

Il 15 luglio 2021 il capo dell'AVI-AIn si è incontrato insieme a due responsabili delle verifiche con i rappresentanti dell'OVC BS per discutere di temi relativi alle verifiche nel settore dell'estremismo violento di destra, dei rapporti d'attività dell'AVI-AIn e dell'OVC BS, delle ripercussioni della legge federale sulle misure di polizia per la lotta al terrorismo, dei metodi utilizzati per l'esercizio della vigilanza e del rapporto di verifica 21-6 «Servizio informazioni cantonale Basilea Città».

Autorità di controllo indipendente per l'esplorazione radio e l'esplorazione dei segnali via cavo (ACI)

Con la revisione della LAIn sarà attuata la fusione tra l'ACI e l'AVI-AIn, già discussa nell'ambito dell'elaborazione della legge. A tal fine il presidente dell'ACI e il capo dell'AVI-AIn hanno stabilito che quest'ultima avrebbe presenziato alle riunioni di verifica periodiche della prima. Perciò, un rappresentante dell'AVI-AIn ha partecipato, a turno, alle riunioni dell'ACI del 26 giugno, 17 settembre, 22 ottobre e 18 novembre 2021.

Lo scopo era di farsi un'idea delle attività di controllo e quindi di sviluppare le conoscenze tecniche e di intelligence necessarie per la ripresa delle attività dell'ACI da parte dell'AVI-AIn. Per motivi di competenza l'AVI-AIn ha rinunciato ad assumere un ruolo attivo nel processo di controllo dell'ACI. Dal canto suo, l'ACI fa rapporto alla DelCG, e l'AVI-AIn riceve sempre il rapporto per conoscenza.

Inoltre, l'AVI-AIn ha partecipato all'atelier K, al quale l'ACI invita regolarmente rappresentanti del SIC, del COE, del TAF e dell'AVI-AIn per un reciproco scambio di informazioni sull'esplorazione via cavo. Nel 2021 si è discusso del potenziamento dell'in-

frastruttura tecnica, delle sfide particolari che si pongono nella gestione del sensore «esplorazione via cavo» e degli ostacoli giuridici che si incontrano nel chiedere la proroga dei mandati di esplorazione via cavo.

Riunione dell'AVI-AIn con la direzione del SIC

In una raccomandazione della perizia Koller del marzo 2013 sulla verifica dell'organizzazione e delle prestazioni della vigilanza sulle attività informative del DDPS, si sottolinea in particolare che la riunione annuale tra la vigilanza e il SIC potrebbe dar vita allo sviluppo di una strategia a lungo termine e all'identificazione dei (grandi) rischi politici⁴³.

Dopo circa quattro anni di coesistenza tra il SIC e l'AVI-AIn, questa raccomandazione è sempre valida anche nel mutato contesto attuale ed è approvata anche dal SIC. Il 2 novembre 2021 la direzione allargata del SIC si è incontrata con l'AVI-AIn. Alla riunione ha partecipato anche il consulente del capo del DDPS in materia di attività informative. Lo scopo di questo primo incontro consisteva nel promuovere la reciproca comprensione e il consenso e nel discutere del seguito dei lavori. In conclusione i partecipanti hanno riconosciuto l'utilità dell'incontro e stabilito che potrebbe essere utile ripeterlo in presenza del nuovo direttore.

Nel 2021 la direzione dell'AVI-AIn si è trovata almeno una volta per uno scambio di opinioni con le persone seguenti:

- capo del DDPS;
- segretario generale del DDPS;
- direttore/direttore supplente del SIC;
- capo del SIM;
- capo del COE;
- collaboratori dell'IFPDT.

L'incontro con i referenti del DFAE, del DFGP e del DDPS (membri della DelSic) è stato rinviato e nel 2021 non ha avuto luogo.

Richieste dei cittadini

Nel 2021 l'AVI-AIn ha ricevuto, trattato ed evaso undici richieste da parte di cittadini.

7.2 Contatti internazionali

Come sinora, l'AVI-AIn può esercitare la vigilanza sulle attività informative della Svizzera soltanto fino al confine nazionale. Attualmente non esiste alcuna base legale che consenta uno scambio nel merito con le autorità partner. Tuttavia, lo scambio può avvenire su metodi, processi ed esperienze in materia di vigilanza.

Incontro virtuale del 20 settembre 2021: Intelligence Oversight Working Group (IOWG)

Prima della pandemia l'IOWG si incontrava due volte l'anno per uno scambio. A causa della pandemia di COVID-19, l'ultimo scambio di questo tipo si è tenuto nel gennaio 2020, e pertanto il gruppo di lavoro si è incontrato di nuovo una prima volta in forma virtuale per rinfrescare i contatti e chiarire questioni riguardanti la continuazione delle attività del gruppo.

Roma, 7 e 8 ottobre 2021: European Oversight Conference

La Procura generale della Repubblica Italiana ha organizzato uno scambio internazionale in merito a varie sentenze giudiziarie nazionali e internazionali, nell'ambito del quale si è discusso soprattutto delle ripercussioni di queste sentenze per i rispettivi servizi informazioni ma anche sui relativi organi di vigilanza. Oltre ai rappresentanti degli organi di vigilanza italiani, hanno partecipato anche delegati di Belgio, Bulgaria, Danimarca, Germania, Francia, Grecia, Regno Unito, Lussemburgo, Norvegia, Olanda, Austria, Portogallo e Svizzera.

⁴³ Perizia «Aufgaben-, Organisations- und Leistungsüberprüfung der Nachrichtendienstlichen Aufsicht des VBS», elaborata dal prof. dr. iur. e lic. oec. Heinrich Koller, pag. 55

Contatti internazionali

● Intelligence Oversight Working Group (IOWG)
Incontro virtuale del 20 settembre 2021

● European Oversight Conference Roma,
7 e 8 ottobre 2021



8. Vista esterna

Il rapporto di attività include anche una vista esterna in relazione al campo di attività dell'AVI-AIn. In linea con il tema «Sistemi d'informazione» scelto per il 2021, Adrian Lobsiger presenta la sua personale visione delle cose.

Opportunità e rischi del «ripensamento digitale»

Nel 1989, sulla scia dello «scandalo delle schedature», la popolazione svizzera aveva perso improvvisamente fiducia nei confronti degli organi preposti alla protezione dello Stato. Dopo aver digerito questo scandalo sul trattamento di dati dei cittadini da parte della Polizia federale, le istanze politiche chiesero che i molteplici compiti di questa autorità di sicurezza fossero separati. Nell'ambito del confronto con i promotori di un'iniziativa per la totale abolizione della protezione dello Stato, allora disciplinata soltanto sommariamente, il Consiglio federale e il Parlamento avviarono un processo per la codificazione di tale attività. Nel 1998 una prima votazione popolare permise di continuare un'attività di protezione dello Stato disciplinata da allora in poi da una legge formale. In seguito, con una seconda votazione del 2016, fu approvata l'attuale legge federale sulle attività informative della Confederazione (LAIn) e il Servizio delle attività informative della Confederazione (SIC) fu autorizzato a procedere all'acquisizione totalmente occulta di dati personali anche con l'impiego di mezzi coercitivi. Questo abbandono dell'originario divieto di usare mezzi coercitivi indusse il legislatore in particolare a creare un'autorità di vigilanza specializzata consacrata esclusivamente al SIC.

Sebbene la sorveglianza esercitata dai servizi informazioni sia un tema che ancora oggi divide le opinioni, anche le voci più critiche devono riconoscere che da quando è entrata in vigore la LAIn il trattamento di dati da parte degli organi preposti alla protezione dello Stato si fonda su una base legale trasparente dal punto di vista della sistemica legislativa e sufficientemente precisa. La codificazione chiara per il cittadino del trattamento di dati personali da parte di altre autorità di sicurezza della Confederazione, altro tema molto delicato, rimane per contro ancora una meta lontana. Il trattamento di dati da parte della Polizia federale e del Corpo delle guardie di confine, per esempio, si basa su una panoplia sempre più folta di disposizioni speciali organizzate in modo carente dal punto di vista sistematico. La presentazione trasparente del trattamento di dati personali nella legge è ulteriormente ostacolata da grandi progetti di trasformazione digitale avviati nel frattempo dalle autorità di sicurezza della Confederazione. Questi progetti possono indurre profondi cambiamenti nei processi di trattamento dei dati personali e per questa ragione la vigilanza della Confederazione sulla protezione dei dati si impegna affinché questi processi siano rilevati in modo completo sin dalla fase di pianificazione per mezzo di cosiddette valutazioni d'impatto sulla protezione dei dati e affinché le loro ripercussioni sulla sfera privata dei cittadini vengano analizzate.

Nella sua strategia per la trasformazione digitale dell'Amministrazione federale, il Consiglio federale chiede un «cambiamento di mentalità» che rimetta in discussione le forme tradizionali di convivenza e di economia e consenta lo sviluppo di competenze digitali e la messa in rete nonché la condivisione di dati tra tutti gli attori. Le parole creano immagini, e così alcuni promotori della trasformazione digitale immaginano un «cloud» a disposizione dei corpi di polizia, delle autorità preposte al controllo dei confini e dei servizi informazioni per il bene di tutte le persone che rispettano la legge e non hanno nulla da nascondere.



Adrian Lobsiger (*1959)

Dopo i suoi studi a Berna e Basilea, Adrian Lobsiger, nato nel 1959, ha ottenuto un Master in diritto europeo a Exeter (GB). Nel 1992, il giurista laureato ha cominciato a lavorare per l'Ufficio federale di giustizia (OFG) nell'ambito del diritto internazionale privato. Nel 1995 è passato all'Ufficio federale di polizia (fedpol), dove è diventato direttore supplente.

Adrian Lobsiger è stato eletto dal Consiglio federale nel novembre 2015 e confermato dal Parlamento nel marzo 2016. È in carica dal giugno 2016. Nella seduta del 10 aprile 2019 il Consiglio federale ha confermato la rielezione di Adrian Lobsiger quale Incaricato federale della protezione dei dati e della trasparenza (IFPDT) per un secondo mandato fino alla fine del 2023.

Agli antipodi di questa visione, gli avversari intravedono nella malvista accumulazione di dati in cosiddetti «silos» i resti di un pensiero superato, da alcuni di essi attribuita a una politica di protezione dei dati che favorisce i delinquenti invece di proteggere i cittadini. Questi visionari scuotono la testa di fronte al fatto che i Cantoni abbiano corpi di polizia che trattano autonomamente i dati personali conservati in questi contenitori e che li condividano – generalmente soltanto su richiesta – con altre autorità di sicurezza, come pure di fronte al fatto che la Confederazione ripartisca il suo potere di polizia tra tre diversi uffici. In quanti nemici giurati dei silos di dati, queste persone considerano irregolare questa realtà che a loro giudizio dovrebbe essere eliminata da tempo, e per questa ragione portano avanti la messa in rete di tutte le autorità di sicurezza in linea con le possibilità offerte dalla tecnica.

Chi dimentica gli avvenimenti storici che hanno spinto il legislatore a organizzare la collettività secondo una struttura federale e a suddividere la concentrazione del potere dello Stato può effettivamente faticare a interpretare in modo razionale la complessità dei flussi di dati trattati dalle autorità di sicurezza. Una riflessione storica può invece aiutare a capire che il sistema della sicurezza interna della Svizzera è la conseguenza di decisioni delle sue istituzioni politiche alle quali il Popolo partecipa direttamente. Nel 1978, per esempio, con la riuscita del referendum contro la creazione di una polizia di sicurezza federale, il Popolo ha decretato ciò che può essere inteso come un veto sino a oggi mai revocato all'istituzione di un'autorità centrale di sicurezza a livello di Confederazione.

Un «cambiamento di mentalità» che considera la messa a disposizione in forma digitale di dati personali come misura di tutte le cose e ignora i concetti politici che limitano il potere dello Stato sarebbe più retrogrado che progressista. Ci porterebbe indietro allo Stato di polizia, abolito con il superamento delle aristocrazie assolutistiche dalla rivoluzione civile del XVIII° e XIX° secolo. La divisione delle strutture dominanti onnipotenti dell'Ancien Régime in uffici con competenze tecniche specializzate ha notevolmente contribuito a trasformare lo Stato di polizia in servizio pubblico e i sudditi in cittadini consapevoli capaci di esigere da questi uffici prestazioni professionali e discrete in cambio delle imposte versate.

Da allora, la professionalità richiesta a un'amministrazione orientata alle prestazioni implica che gli uffici specializzati condividano con altri servizi i dati dei cittadini in loro possesso soltanto in virtù di procedure previste dalla legge. Può essere considerato come espressione di professionalità anche il fatto che oggi l'Amministrazione federale tratti dati fattuali per renderli leggibili da macchine e li metta a disposizione dei vari settori, e anche il fatto che registri dati di base e attributi personali secondo il cosiddetto principio «once only» e gestisca questi dati per mezzo di identificatori uniformi come il numero AVS. La protezione dei dati non si oppone a queste operazioni di digitalizzazione volte a incrementare l'efficienza del servizio pubblico, poiché esse possono contribuire anche a migliorare la qualità dei dati.

Chi tentasse invece, seguendo la via di messe in rete nebulose, di creare una sorta di cloud in cui le autorità di sicurezza, le autorità inquirenti tributarie e altri organi dell'amministrazione interventista potessero pescare qualsiasi dato derivante dai rapporti della popolazione con l'amministrazione orientata alle prestazioni, si troverebbe in rotta di collisione con la protezione dei dati. Una simile caccia ai dati fornirebbe ben presto motivi di scandalo e minerebbe la fiducia dei cittadini nel ruolo dello Stato come servizio pubblico e garante dello Stato di diritto. Per prevenire queste situazioni, le autorità federali preposte alla vigilanza sulla protezione dei dati chiedono ai responsabili dei progetti di trasformazione digitali di chiarire, nelle loro valutazioni d'impatto, la portata e l'intensità del futuro trattamento di dati nonché la cerchia dei servizi aventi diritto d'accesso, e di confrontare tali aspetti con lo status quo. L'estensione e l'intensificazione del trattamento di dati personali devono essere motivati.

Talvolta gli uffici federali rispondono all'IFPDT che i rapidi progressi della tecnica impongono di pianificare «agilmente» i processi di trasformazione digitale. Di conseguenza sarebbe impossibile delimitare in modo esaustivo i futuri trattamenti di dati o confrontarli con lo status quo. Simili ragionamenti sono inaccettabili. Essi implicano il conferimento di una licenza generale all'amministrazione, poiché né gli organi politici responsabili nei confronti della popolazione delle ingerenze dell'autorità nella sfera privata né il vasto pubblico sono in grado di stimare i rischi legati a tale «agilità». Nella sua prassi, infatti, l'IFPDT chiede spesso di precisare e completare le valutazioni d'impatto sulla protezione dei dati, ogni volta che i risultati di tali valutazioni confluiscono nei messaggi con cui il Consiglio federale propone al legislatore di adeguare gli atti normativi in materia di sicurezza.

Considerate le sfide illustrate, l'IFPDT si rallegra che il suo lavoro nel settore delle attività informative sia integrato efficacemente dal lavoro dell'AVI-AIn.

9. Cifre al 31 dicembre 2021



Collaboratori

1.1.2021
31.12.2021
Annunciate

10
9
4



Verifiche

Pianificate **18 (18)**
Verifiche senza preavviso **0 (1)**
Verifiche eseguite **18 (17)**

Interviste condotte 2021

90 (102)

Effettivo di personale preventivato

10

Raccomandazioni

18 (55)



10. Allegato

10.1 Piano di controllo 2021

N.	Titolo	Organo verificato
Strategia e pianificazione		
21-1	Impiego dei collaboratori del SIC ¹ nelle rappresentanze svizzere all'estero	SIC
Organizzazione		
21-2	Protezione delle infrastrutture critiche/Cyber Defence	SIC/COE ²
21-3	Sicurezza all'interno del SIC	SIC
21-4	Estremismo violento di destra	SIC
Collaborazione		
21-5	Garanzia della qualità del SIC con i servizi informazioni cantonali (SICant)	SIC
21-6	Controllo SICant BS	SIC/SICant
21-7	Controllo SICant BL	SIC/SICant
21-8	Controllo SICant AR	SIC/SICant
21-9	Controllo SICant AI	SIC/SICant
21-10	Controllo SICant AG	SIC/SICant
21-11	Controllo SICant VD	SIC/SICant
21-12	Controllo SICant NE	SIC/SICant
Acquisizione di informazioni		
21-13	Gestione del rischio per gli impegni con l'estero	SIC
21-14	Operazioni	SIC
21-15	HUMINT ³	SIC
Risorse		
Nessun controllo pianificato		
Trattamento dei dati/archiviazione		
21-16	Servizi di telecomunicazione	SIC
21-17	Servizio del SIC selezionato (Quattro P ⁴)	SIC
21-18	Protezione dei dati all'interno del SIM ⁵	SIC

¹ Servizio delle attività informative della Confederazione

² Centro operazioni elettroniche

³ Human Intelligence, acquisizione di informazioni tramite fonti umane

⁴ Art. 55 della legge federale sulle attività informative (Legge sulle attività informative, LAIn, RS 121)

⁵ Servizio informazioni militare

10.2 Elenco delle abbreviazioni

ACI Autorità di controllo indipendente per l'esplorazione radio e l'esplorazione dei segnali via cavo	fedpol Ufficio federale di polizia	OVC BS Organo di vigilanza cantonale di Basilea Città
AD addetto alla difesa	FF Foglio federale	p. es. per esempio
App spec SICant Applicazione specialistica Servizio informazioni cantonale	GEVER Sistema di trattamento e controllo degli affari	PLdec posto di lavoro decentralizzato
Archivio BURAUT banca dati del SIC	GEX estremismo violento	Quattro P Sistema d'informazione del SIC per identificare determinate categorie di stranieri che entrano in Svizzera
art. articolo	HUMINT Human Intelligence, acquisizione di informazioni per mezzo di fonti umane	REX estremismo violento
AVI-AIn Autorità di vigilanza indipendente sulle attività informative	IASA SIC Sistema di analisi integrale del SIC	RI DDPS Revisione interna DDPS
CDF Controllo federale delle finanze	IFPDT Incaricato federale della protezione dei dati e della trasparenza	risp. rispettivamente
CNO Cyber Network Operations, settore del COE	IOWG Intelligence Oversight Working Group	RS Raccolta sistematica delle leggi federali
COE Centro operazioni elettroniche	JCTAC Joint Cyber Technical Analysis Center	segg. e seguenti
cpv. capoverso	LAIIn Legge federale sulle attività informative	settore SIC A settore analisi del SIC
CQ SIC organo di controllo della qualità del SIC	LPD Legge federale sulla protezione dei dati (RS 235.1)	SIC Servizio delle attività informative della Confederazione
CTI Cyber Threat Intelligence (CTI), unità del COE	MASA misure d'acquisizione soggette ad autorizzazione	SICant Servizi informazioni cantonali
DDPS Dipartimento federale della difesa, della protezione della popolazione e dello sport	MELANI Centrale d'annuncio e d'analisi per la sicurezza dell'informazione	SiLAN rete protetta del SIC
DFAE Dipartimento federale degli affari esteri	n. numero	SIM Servizio informazioni militare
DFGP Dipartimento federale di giustizia e polizia	OIC MELANI Operation Information Center, settore di MELANI	Sist infm SIM Sistema informatico Servizio informazioni militare
DeICG Delegazione delle Commissioni della gestione delle Camere federali	OSINT «Open Source Intelligence», messa a disposizione di dati provenienti da fonti accessibili al pubblico	SQ SIC Servizio di controllo della qualità del SIC
DeSic Delegazione Sicurezza del Consiglio federale	OSI-SIC Ordinanza sui sistemi d'informazione del Servizio delle attività informative della Confederazione	TAF Tribunale amministrativo federale



**Autorità di vigilanza indipendente sulle
attività informative**

Maulbeerstrasse 9, 3003 Berna
Telefono +41 58 464 20 75
www.ab-nd.admin.ch