



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Autorità di vigilanza indipendente
sulle attività informative AVI-AIn**

Rapporto di attività 2023

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

1 Sintesi

Il rapido mutare della situazione riguardante la sicurezza impone all'Autorità di vigilanza indipendente sulle attività informative (AVI-AIn) di adeguare continuamente le proprie attività di verifica. La guerra in Ucraina e i recenti sviluppi in Medio Oriente per esempio hanno condizionato le attività dei servizi sottoposti a vigilanza e di conseguenza l'AVI-AIn ha dovuto adeguare con flessibilità le sue attività di vigilanza.

Anche la trasformazione del Servizio delle attività informative della Confederazione (SIC) ha richiesto flessibilità e agilità da parte dell'AVI-AIn. Inoltre, l'AVI-AIn deve monitorare, analizzare e integrare nelle sue attività di verifica anche gli sviluppi tecnologici, per esempio l'utilizzo dell'intelligenza artificiale. Di riflesso, l'adeguamento alle mutevoli condizioni quadro è un tema affrontato e discusso anche a livello internazionale negli scambi con altre autorità di vigilanza.

Guardando all'anno in rassegna, la verifica 22-15 OSINT svolta presso il SIC si rivela come uno degli elementi centrali delle attività di verifica svolte dall'AVI-AIn nel 2023. L'Open Source Intelligence (OSINT) è un settore in rapido sviluppo dell'attività di acquisizione di informazioni di intelligence. Il collegamento di una quantità inesauribile di dati accessibili pubblicamente offre ai servizi informativi possibilità quasi infinite di acquisire informazioni. Le questioni che si pongono sono di natura giuridica ed etica, per esempio quella della delimitazione dell'OSINT rispetto alle misure di acquisizione soggette ad autorizzazione o quella di sapere se l'acquisizione o l'utilizzo di dati sottratti da terzi rientri ancora in questo ambito. Questa modalità di acquisizione di informazioni da parte dei servizi informazioni viene seguita da vicino e discussa dalle autorità di vigilanza anche a livello internazionale. L'AVI-AIn ha verificato le acquisizioni di questo tipo svolte dal SIC e ha formulato diverse raccomandazioni.

Per il 2023 l'AVI-AIn aveva programmato 16 verifiche, quattro delle quali sono state cancellate nel corso dell'anno. Una verifica avviata nel 2021 è stata portata a termine. Nel 2023 sono stati trasmessi sette rapporti di verifica definitivi riguardanti verifiche avviate nel 2022. Sempre nel 2023, l'AVI-AIn ha concluso gli atti di controllo relativi a un totale di sette verifiche previste nello stesso anno e ha trasmesso al Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) tre rapporti definitivi riguardanti le verifiche programmate nell'anno in corso.

Oltre alle verifiche effettuate presso il SIC una verifica ha riguardato il Centro operazioni elettroniche (COE; dal 1.1.2024 "Servizio delle attività ciber ed elettromagnetiche (ACE)"). Per quanto riguarda il Servizio informazioni militare (SIM), l'AVI-AIn ha condotto a livello di direzione vari colloqui relativi alle sue competenze in materia di vigilanza nel settore del Servizio di protezione preventiva dell'esercito (SPPEs) e ha inserito una corrispondente verifica nel proprio piano di controllo per il 2024.

2 Cifre al 31. dicembre 2023

Collaboratori	01.01.2023	10
	31.12.2023	10
Verifiche pianificate		16
Verifiche senza preavviso		0
Verifiche eseguite		11
Interviste realizzate	Oralmente e per iscritto	109
Raccomandazioni		10

3 Indice

1	Sintesi	2
2	Cifre al 31. dicembre 2023	3
3	Indice	4
4	Nota personale	4
5	Attività di vigilanza	6
5.1	Piano di controllo.....	6
5.2	Verifiche nel 2023.....	6
5.2.1	Strategia e pianificazione	6
5.2.2	Organizzazione	7
5.2.3	Collaborazione	9
5.2.4	Acquisizione	10
5.2.5	Risorse	12
5.2.6	Trattamento dei dati / archiviazione	14
5.3	Atteggiamento cooperativo	17
5.4	Controlling delle raccomandazioni	17
6	Sguardo all'interno dell'AVI-AIn	18
6.1	Personale	18
6.2	Formazioni e formazioni continue	18
6.3	Verifica condotta sull'AVI-AIn dal Controllo federale delle finanze (CDF)	20
6.4	Accesso a documenti e informazioni ufficiali	21
7	Coordinamento	21
7.1	Contatti nazionali.....	21
7.2	Contatti internazionali.....	22
8	Allegato	26
8.1	Piano di controllo 2023.....	26
8.2	Elenco delle abbreviazioni	27

4 Nota personale

La questione della fiducia

Come giurista, so che lo Stato può fare solo quello che la legge gli chiede di fare, rispettivamente, so che posso consultare una legge e capire (più o meno) tutto quello che un'autorità pubblica fa e perché lo fa. Ma se fossi un ingegnere, probabilmente capirei meglio perché oggi posso continuare a transitare nel tunnel autostradale del San Gottardo malgrado il fatto che il 10 settembre 2023 parti di calcestruzzo sono cadute sulla strada. Come semplice persona, devo fidarmi di chi ne sa più di me, come l'Ufficio federale delle strade.

Con lo Stato è così, alcune cose le capisco e altre no, ma c'è sempre qualcuno che, se lo chiedo, me lo deve spiegare. Poi ci sono i servizi informativi... A volte è stato rimproverato a questi servizi di essere come "uno Stato nello Stato", perché certe attività proprio non si possono conoscere, come se essi avessero un potere che nessun altro ha. Difatti, il potere della segretezza non è poca cosa.

Guardando concretamente cosa fanno i servizi informativi, in realtà, si capisce subito che la segretezza è prima di tutto uno strumento di lavoro. Se i servizi informativi non potessero agire in alcuni contesti con mezzi e metodi dissimulati, non servirebbero a niente.

Ovviamente a questo potere s'accompagna una grande responsabilità. Chi mi assicura che qualcuno non abusi della segretezza per scopi truffaldini o egoistici, come l'avidità e la smania di potere?

Il legislatore svizzero, da tempo, sa che quel potere va sottoposto a un controllo molto forte. In particolare, la Delegazione della gestione del nostro Parlamento si occupa di alta sorveglianza parlamentare dei servizi informativi già dal 1992. Nel 2015, con l'adozione della nuova legge sui servizi informativi, approvata dal popolo nel 2016, il legislatore ha voluto sviluppare ulteriormente la sorveglianza istituendo un'Autorità di vigilanza indipendente composta da specialisti.

Questo sistema, che coniuga un organo parlamentare con un'autorità indipendente, corrisponde alla scelta fatta da praticamente tutte le democrazie occidentali. Si tratta di una legittimazione importante per i servizi informativi, in quanto oramai essi vengono controllati sia da un organo parlamentare che rappresenta le varie sensibilità politiche in cui ogni cittadino può riconoscersi, sia da esperti come quelli che ho il piacere di dirigere e che vi presentano il loro lavoro in questo rapporto.

I servizi informativi non sono paragonabili all'Ufficio federale delle strade in quasi nessun punto, se non quello della fiducia. Essi necessitano della fiducia dei cittadini per funzionare, così come il cittadino ha bisogno dei servizi informativi per godere di una certa sicurezza.

La sorveglianza che svolge l'Autorità che rappresento consiste nel saper vigilare su delle attività particolarmente complesse e delicate, riconoscendone i rischi o le inadempienze, e presentando i correttivi che si rendono necessari. Non possiamo, come autorità di vigilanza, svelare tutti i segreti dei servizi informativi, ma possiamo accedervi.

L'Autorità indipendente di vigilanza sulle attività informative presenta quindi il proprio rapporto d'attività al fine di permettere a ogni cittadino di decidere da solo se può fidarsi.

Buona lettura!

Prisca Fischer, Capo AVI-Aln

5 Attività di vigilanza

5.1 Piano di controllo

L'AVI-AIn svolge verifiche in base a una propria valutazione dei rischi nei seguenti ambiti:

- Strategia e pianificazione
- Organizzazione
- Collaborazione
- Acquisizione
- Risorse
- Trattamento dei dati / archiviazione

Il piano di controllo è programmato in modo tale che vi sia almeno una verifica per ogni ambito. Il piano pubblicato per il 2023 è stato modificato nel corso dell'anno. Quattro verifiche sono state cancellate per i seguenti motivi:

- “23-1 Produzione ed efficacia dei prodotti informativi del Servizio delle attività informative della Confederazione (SIC)”: dato che il SIC vive una fase di trasformazione, vanno previsti cambiamenti non solo nei vari settori organizzativi, bensì anche a livello di produzione.
- “23-3 Protezione e sicurezza presso il SIC”: determinati aspetti legati alla sicurezza sono già stati esaminati nell'ambito delle scorse verifiche. Nell'ambito della verifica “22-14 Processo di reclutamento, di assistenza e di uscita” per esempio sono stati affrontati determinati aspetti riguardanti la sicurezza dei collaboratori. Per tale ragione, si è rinunciato a eseguire questa verifica per dare la precedenza ad altre. Nondimeno, la sicurezza del personale rimane sempre al centro dell'attenzione dell'AVI-AIn.
- “23-14 Attuazione delle raccomandazioni dell'AVI-AIn”: l'AVI-AIn ha lanciato un progetto interno per migliorare la qualità delle sue raccomandazioni. Due collaboratori hanno seguito un corso di perfezionamento e hanno elaborato un testo professionale su questo tema. Su questa base, l'AVI-AIn adeguerà il manuale per le verifiche. Inoltre, rafforzerà il monitoraggio delle raccomandazioni. Per tale ragione si è rinunciato a eseguire questa verifica per dare la precedenza ad altre verifiche.
- “23-15 Attuazione del diritto d'accesso nel SIC”: il 1° settembre 2023 è entrata in vigore la revisione della legge federale del 25 settembre 2020 sulla protezione dei dati (LPD; RS 235.1). Il SIC deve disporre di tempo a sufficienza per integrare le modifiche necessarie nei suoi processi. Per questo aspetto, l'AVI-AIn rimane in contatto non solo con il SIC, ma anche con l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).

5.2 Verifiche nel 2023

A partire dal rapporto di attività del 2023, l'AB-ND cambierà il modo di redigere i rapporti per riflettere lo stato più aggiornato possibile. Nei precedenti rapporti aveva sempre riferito soltanto in merito alle verifiche ultimate nell'anno appena concluso. D'ora in poi riferirà in merito a ogni verifica per la quale ha svolto tutte le attività pertinenti nell'anno in rassegna. Nel rapporto potranno essere trattate anche verifiche non ancora formalmente ultimate nel 2023.

5.2.1 Strategia e pianificazione

Nell'ambito «Strategia e pianificazione» l'AVI-AIn svolge verifiche su temi che riguardano la pianificazione strategica a breve, medio o lungo termine delle autorità di intelligence della Svizzera nonché la definizione dei loro obiettivi. Nel 2023 l'AVI-AIn si è occupata della seguente verifica:

22-1 Anticipazione e individuazione tempestiva

Questa verifica era incentrata sulla questione di sapere in che modo il SIC può adempiere il proprio mandato legale primario di individuazione tempestiva e anticipazione. L'acquisizione e il trattamento delle informazioni da parte del SIC servono all'individuazione tempestiva e alla prevenzione delle minacce rivolte alla sicurezza interna ed esterna. A tal fine il SIC deve disporre di capacità che gli

permettano di identificare e valutare tempestivamente una situazione e le minacce che ne derivano. A causa della crescente complessità del sistema geopolitico internazionale, le imponderabilità riguardanti la futura evoluzione delle minacce sono fortemente aumentate. **Gli sviluppi sociali e tecnologici nonché le attuali minacce ibride aventi dimensioni globali impongono al SIC di saper riconoscere queste minacce e reagire di fronte ad esse in modo rapido ed efficace.**

L'anticipazione delle minacce rilevanti nonché delle opportunità e degli sviluppi strategici riveste dunque un'importanza cruciale. Sotto questo aspetto il SIC svolge un ruolo importante per i suoi clienti per quanto riguarda l'individuazione tempestiva di minacce e crisi.

L'AVI-AIn ha constatato che l'individuazione tempestiva e l'anticipazione sono un obiettivo strategico del DDPS che il SIC persegue già da diverso tempo e per il quale ha adottato misure sul piano operativo che in parte sono già a buon punto e in parte devono essere ulteriormente intensificate. Per l'AVI-AIn, al tema viene attribuita la necessaria importanza sul piano strategico. Se prendiamo come metro di misura l'importanza attribuita al tema dell'individuazione tempestiva e dell'anticipazione all'interno delle rispettive strategie del DDPS e del SIC nonché le dichiarazioni dei collaboratori interessati, constatiamo che questi ultimi sono tutti unanimi nell'attribuire enorme importanza al tema.

Ma l'AVI-AIn ha anche constatato che le riflessioni (teoretiche) del SIC trovano approdo soltanto molto lentamente nei settori del servizio che si occupano di analisi. Gli strumenti disponibili si coniugano ancora in modo poco ottimale con i prodotti. Quindi, il SIC non riesce ancora a trasferire gli sforzi concettuali nei prodotti in modo sufficientemente concreto e a trarne utilità. L'AVI-AIn ha pertanto raccomandato al SIC di continuare a portare avanti con costanza le singole misure di attuazione della strategia 2020-2025 del SIC per quanto concerne l'individuazione tempestiva e l'anticipazione e di verificare almeno una volta all'anno il loro stato di attuazione.

L'AVI-AIn è persuasa che il SIC saprà sfruttare la trasformazione attualmente in corso come base per creare un futuro servizio agile, innovativo e capace di adattarsi. Occorre però tener conto del fatto che questo compito non si conclude semplicemente con una riorganizzazione. Il compito di mantenere aggiornate le strutture, le modalità operative e gli strumenti tecnologici del servizio, e quindi di fare in modo che esso sia in grado di reagire tempestivamente e in modo adeguato a minacce in continuo divenire, è un compito gestionale permanente che spetta in particolare alla direzione del SIC.

5.2.2 Organizzazione

Nell'ambito «Organizzazione», l'AVI-AIn verifica l'idoneità della struttura e dei processi dei servizi informazioni, interrogandosi sul fatto se possano consentire un adempimento conforme alla legge, adeguato ed efficace del mandato legale di queste autorità. Nel 2023 l'AVI-AIn ha svolto le seguenti verifiche in questo ambito:

23-2 Servizi giuridici nel SIC

L'osservanza della legge riveste grande importanza nelle attività di intelligence. Se il SIC non agisce in modo conforme alla legge, ossia nel quadro del suo mandato legale, ne deriva un danno di reputazione e ne esce danneggiata anche la fiducia della popolazione svizzera nel servizio. Inoltre, possono essere violati diritti della personalità in base alle prescrizioni in materia di protezione dei dati, il diritto alla protezione della sfera privata o segreti d'affari. Ma un rischio rilevante per la sicurezza della Svizzera può sorgere anche se il SIC per incertezza non sfrutta appieno le possibilità che la legge gli concede, non svolgendo quindi appieno il proprio mandato.

Basandosi su queste premesse, l'AVI-AIn ha verificato l'adeguatezza e l'efficacia di compiti, competenze e responsabilità dei fornitori di servizi giuridici in seno al SIC. Nell'ambito di tale verifica, si intendevano per servizi giuridici le attività del SIC che includono per esempio la risposta a una domanda concreta, accertamenti generali su contesti giuridici, progetti legislativi e sentenze giudiziarie, l'invocazione di pretese contestate e la partecipazione a progetti o alla conclusione di contratti. L'AVI-AIn non ha verificato la qualità dei servizi giuridici forniti dal punto di vista del contenuto (legalità).

L'AVI-AIn ha condotto otto interviste, in particolare con persone in posizione dirigenziale. Inoltre, per mezzo di un questionario, ha interrogato 30 collaboratori in merito al loro giudizio sui servizi forniti. Per di più, ha consultato e in seguito analizzato e valutato vari documenti presenti nel sistema di gestione degli affari del SIC e riguardanti compiti, responsabilità e servizi giuridici forniti.

Questa verifica è iniziata nel 2023 e alla chiusura di redazione del presente rapporto non era ancora stata ultimata. Per tale ragione non è ancora possibile esprimersi in merito ai risultati in questa sede. L'AVI-AIn prevede di pubblicare sul proprio sito web la sintesi della verifica nel 2024.

23-4 Business Continuity Management dell'informatica (IT) e Disaster Recovery-IT nel SIC

Nell'ambito di questa verifica, l'AVI-AIn ha esaminato se il SIC disponesse di processi efficaci e adeguati per continuare a garantire, in uno scenario di crisi o catastrofe, il funzionamento del suo sistema informatico e dunque il proseguimento della sua attività principale e per ripristinare i suoi dati.

Eventi imprevisti importanti, quali incendi, inondazioni o attività criminali, rappresentano una minaccia per qualsiasi organizzazione. Questo tipo di eventi può per sua natura causare potenzialmente danni più gravi di un semplice guasto, in particolare all'infrastruttura delle tecnologie dell'informazione e della comunicazione (TIC). Pertanto, le organizzazioni devono preoccuparsi di garantire la continuità della loro attività (Business Continuity Management [BCM]). Il BCM, dunque, si concentra su un evento e si sforza di ridurre l'impatto di un rischio sulle prestazioni e sui processi operativi essenziali.

Un sistema informatico affidabile e ad alta disponibilità è indispensabile per la sopravvivenza di un'impresa la cui attività principale è fortemente dipendente dalle tecnologie dell'informazione. L'IT Service continuity management (ITSCM), che deriva dal BCM, ha lo scopo di garantire la fornitura delle prestazioni informatiche critiche identificate dall'impresa in modo corrispondente alle esigenze anche in caso di evento importante. A tal fine, si valutano e si mettono in atto misure preventive (rafforzamento della resilienza) e misure predisposte in caso di evento (rafforzamento della risposta). L'ITSCM deve garantire che i servizi e l'infrastruttura TIC siano disponibili in caso di perturbazione o che possano essere ripristinati entro un termine stabilito. Il disaster recovery dell'infrastruttura informatica (Disaster Recovery-IT) invece ha l'obiettivo di ripristinare i servizi e l'infrastruttura TIC in caso di perturbazione.

Il tema dell'ITSCM consiste dunque nel rispondere a rischi molto attuali e concreti. **Con la digitalizzazione che avanza e data l'importanza del trattamento di dati per le attività del SIC, il servizio dipende sempre più dal funzionamento continuo e affidabile della sua infrastruttura informatica, il tutto in un contesto caratterizzato dal rischio di penuria di energia elettrica, dal moltiplicarsi dei ciberattacchi e da una guerra alle porte del continente europeo.** Allo stesso modo, perdite di dati rischierebbero di compromettere la capacità del SIC di compiere la propria missione.

La parte BCM di questa verifica era già stata oggetto di un rapporto dell'organo di revisione interna del DDPS, il quale invitava le unità amministrative del dipartimento ad aggiornare la propria documentazione su questo tema. Il SIC si sta adoperando per attuare questa raccomandazione. Per di più, la direzione del servizio ha deciso di approvare e attuare un nuovo BCM soltanto dopo che sarà stata ultimata la trasformazione attualmente in corso. L'AVI-AIn non ha insistito ulteriormente per quanto riguarda il BCM.

Quanto all'ITSCM, il SIC ha invece constatato che manca una documentazione. Questa mancanza è dovuta a un errore di governance TIC all'interno del servizio. In realtà esistono delle misure, ma soltanto a livello tecnico. L'unità TIC ha pertanto adottato numerose misure per garantire la continuità dell'attività in caso di evento importante. Le misure adottate sono efficaci e adeguate. Esse permettono di limitare i rischi in modo coerente. In particolare, la ridondanza dell'infrastruttura TIC e la strategia di salvataggio dei dati si dimostrano adeguate ed efficaci. Peraltro, il SIC non dispone di una strategia di test, sicché, anche se i servizi TIC sono molto stabili, non è certo che lo sarebbero anche in caso di evento importante. Inoltre, la mancanza di test variati e regolari impedisce di aggiornare l'ITSCM. L'AVI-AIn ha formulato raccomandazioni riguardanti la documentazione dell'ITSCM e l'organizzazione di test.

5.2.3 Collaborazione

Nell'ambito «Collaborazione» l'AVI-AIn verifica la collaborazione dei servizi con le autorità nazionali e internazionali. L'AVI-AIn verifica ogni anno la collaborazione con alcuni servizi informazioni cantonali (SICant). Per quanto riguarda le verifiche dei SICant di Nidvaldo e Obvaldo, un primo incontro è avvenuto ancora prima della fine del 2023, ma gli atti di controllo si svolgeranno nel 2024. Per questo motivo, l'AVI-Ain pubblicherà le sintesi dei risultati di queste verifiche sulla propria pagina Internet dopo che saranno completate.

Nel 2023 ha portato avanti le seguenti verifiche:

23-5 Servizio informazioni cantonale Lucerna

L'AVI-AIn ha verificato se la collaborazione tra SIC e SICant Lucerna si svolge in modo conforme alla legge, adeguato ed efficace. Essa è giunta alla conclusione che la collaborazione tra i due servizi è assidua e, in molti ambiti tematici, può essere considerata da buona a ottima. Il SICant Lucerna esegue i mandati del SIC in maniera tempestiva e in modo appropriato dal punto di vista del contenuto. In base alle attività di verifica svolte, l'AVI-AIn ha potuto constatare che il SICant Lucerna dispone di un'eccellente rete e di buone conoscenze in materia di intelligence e che i presupposti per l'adempimento dei compiti di intelligence sono soddisfatti e che i collaboratori sono motivati.

L'AVI-AIn ha verificato in particolare se i dati salvati e quelli registrati come dati personali rispettano le disposizioni legali per quanto riguarda il legame con il compito, il rispetto dei limiti di trattamento e la correttezza e rilevanza delle informazioni. A questo riguardo non ha constatato gravi anomalie, ma ha comunque suggerito di effettuare una verifica sistematica in tutti gli archivi.

23-8 Servizio informazioni cantonale Uri

L'AVI-AIn ha verificato se la collaborazione tra SIC e SICant Uri si svolge in modo conforme alla legge, adeguato ed efficace. Essa è giunta alla conclusione che la collaborazione tra i due servizi è assidua e, in molti ambiti tematici, può essere considerata buona. Il SICant Uri ha eseguito i mandati del SIC in maniera tempestiva e in modo appropriato dal punto di vista del contenuto. L'AVI-AIn ha avuto l'impressione che il SICant Uri disponga di una rete di contatti molto buona così come di buone conoscenze in materia di intelligence. Inoltre l'AVI-Ain ha potuto constatare che i presupposti per l'adempimento dei compiti sono soddisfatti e che i collaboratori sono motivati.

L'AVI-AIn ha verificato se i dati salvati e quelli registrati come dati personali rispettano le disposizioni legali per quanto riguarda il legame con il compito, il rispetto dei limiti di trattamento e la correttezza e rilevanza delle informazioni. A questo riguardo non sono state constatate anomalie.

23-9 Elaborazione dei mandati per mezzo di sensori tecnici in seno al Centro operazioni elettroniche (COE; dal 1.1.2024 "Servizio delle attività ciber ed elettromagnetiche (ACE)")

I sensori tecnici sono una fonte importante per l'acquisizione di informazioni di intelligence. Dato che in questa disciplina dell'acquisizione di informazioni la tecnica soggiacente evolve continuamente e di conseguenza l'efficacia di questa attività di intelligence tende a migliorare con gli sviluppi della tecnica, gli organi d'esecuzione devono per forza interessarsi costantemente degli ulteriori sviluppi delle loro possibilità nel campo dell'acquisizione di informazioni rilevanti per l'intelligence. Se le condizioni quadro giuridiche stabilite non fossero debitamente considerate in queste riflessioni, potrebbe derivarne un rischio.

Perciò, l'AVI-AIn ha verificato l'elaborazione dei mandati del SIC per mezzo di sensori tecnici in seno all'ACE. Nell'ambito di tale verifica ha constatato che è necessario che i mandati impartiti dai servizi siano sempre dettagliati e che siano redatti in forma scritta. La registrazione di questi mandati in un sistema amministrativo centrale di gestione dei mandati garantisce in qualsiasi momento la tracciabilità, il rispetto dei termini legali e l'assegnazione dei risultati al mandato corrispondente.

A livello di attività operative, l'ACE studia in che modo utilizzare strumenti intelligenti per sgravare le scarse risorse umane da compiti di routine e anche per sfruttare meglio i dati ottenuti con l'esplorazione radio e dei segnali via cavo, in particolare nell'ottica di future cyberminacce.

Per quanto riguarda il rispetto delle basi legali nelle attività operative, l'AVI-AIn ha avuto modo di constatare che non solo i collaboratori dell'ACE vengono regolarmente resi attenti alla rilevanza delle basi legali per le loro attività correnti, ma esistono anche misure organizzative, quali ad esempio *peer review* o istruzioni interne emanate dai responsabili del Servizio.

Nell'insieme l'AVI-AIn non ha trovato indizi atti a far credere che nell'impiego di sensori tecnici per l'elaborazione dei mandati dei servizi, l'ACE violi le basi legali o che i sensori non siano impiegati in modo efficace e adeguato.

23-10 Collaborazione del SIC con privati

Il SIC svolge una parte delle sue attività di acquisizione in modo dissimulato. Ciò è necessario perché altrimenti l'acquisizione delle informazioni potrebbe essere scoperta e impedita dagli Stati interessati o da altri attori. In tal modo si proteggono inoltre collaboratori, installazioni e fonti d'informazione del SIC.

Per nascondere il legame di una persona o della sua attività con il SIC è necessario creare e mantenere coperture efficaci. A tal fine il SIC deve potersi avvalere in particolare dell'aiuto di privati. Nell'ambito di questa verifica, il termine «privati» è stato sostanzialmente utilizzato per tutto quanto non deve essere considerato come ente pubblico svizzero o estero.

Secondo la LAIn, il SIC può collaborare con privati, aziende o organizzazioni. Questi possono fornire al SIC prestazioni utili per l'adempimento dei compiti previsti dalla LAIn o sostenere il SIC nell'acquisizione di informazioni. Inoltre, il SIC può assegnare a privati mandati di acquisizione se è necessario per motivi tecnici o di accesso all'oggetto dell'acquisizione. Ciò solleva questioni di legittimità del mandato e di organizzazione. Occorrerebbe per esempio pensare all'eventuale aggiramento di misure soggette ad autorizzazione, a comportamenti illeciti dei privati, a pagamenti senza controprestazione o alla collaborazione con persone poco raccomandabili. L'importante è avere una panoramica del reclutamento, delle verifiche della sicurezza e dell'indennizzo delle persone private impiegate, della documentazione ecc.

Le attività svolte in modo imprudente, specialmente da parte di privati, potrebbero consentire a terzi di risalire contrariamente a quanto auspicato a collaboratori e infrastrutture del SIC nonché alle fonti, mettendoli in pericolo. Inoltre, nel fornire le loro prestazioni, i privati che collaborano con il SIC potrebbero comportarsi in modo illecito, consapevolmente o inconsapevolmente. Il sorgere di questi rischi avrebbe non solo ripercussioni a livello operativo, per esempio ostacolando o addirittura rendendo impossibile l'acquisizione di informazioni, ma inevitabilmente avrebbe anche conseguenze per la reputazione e la credibilità del SIC.

Perciò l'AVI-AIn verifica se la collaborazione del SIC con privati e l'assegnazione di mandati a questi ultimi avviene lecitamente. Inoltre, verifica se i rischi e l'utilità della collaborazione con privati vengono controllati sistematicamente, se tale collaborazione e i relativi mandati sono organizzati e coordinati in modo efficace e adeguato e se sono documentati in modo comprensibile e significativo.

Questa verifica è iniziata nel settembre 2023 e alla chiusura di redazione del presente rapporto non era ancora stata ultimata. Per tale ragione non è ancora possibile esprimersi in merito ai risultati in questa sede. L'AVI-AIn prevede di pubblicare sul proprio sito web la sintesi della verifica nel 2024.

5.2.4 Acquisizione

L'acquisizione di informazioni è un compito fondamentale dei servizi di intelligence, che a tal fine possono utilizzare vari mezzi. Quelli che incidono in modo più invasivo nella sfera privata delle persone interessate sono oggetto di un'attenzione particolare da parte dell'AVI-AIn. Nel 2023 l'AVI-AIn ha portato avanti le seguenti verifiche:

22-10 Acquisizione di informazioni per mezzo di misure di acquisizione non soggette ad autorizzazione

Il SIC può applicare autonomamente e senza una specifica autorizzazione esterna talune misure atte all'acquisizione di informazioni poiché l'intensità della loro ingerenza nei diritti fondamentali è relativamente esigua. Se queste misure non sono sufficienti per ottenere informazioni essenziali per salvaguardare la sicurezza della Svizzera, il SIC ha il diritto di incidere maggiormente sui diritti fondamentali delle persone interessate adottando misure soggette ad autorizzazione. Più è profonda l'ingerenza, maggiore è la necessità di controllo. Per questa ragione, prima di poter essere applicate dal SIC, le misure di acquisizione soggette ad autorizzazione devono essere autorizzate dal Tribunale amministrativo federale (TAF) e ottenere il benestare del capo del DDPS previa consultazione della Delegazione Sicurezza del Consiglio federale. Per le misure di acquisizione non soggette ad autorizzazione invece non sono previsti controlli esterni. Esiste dunque il rischio che queste misure siano attuate illecitamente, per esempio quando riguardano fatti e installazioni appartenenti alla sfera privata protetta.

Perciò l'AVI-AIn ha verificato se l'impiego di misure di acquisizione non soggette ad autorizzazione in seno al SIC avviene in modo conforme alla legge. Nell'ambito di tale verifica ha constatato che il SIC dispone sostanzialmente di mezzi d'intervento adeguati e delle capacità necessarie per impiegare tutte le misure di acquisizione non soggette ad autorizzazione in funzione della situazione e in modo proporzionale, conformemente a quanto previsto dagli articoli 14 e 16 LAIn.

L'AVI-AIn ha anche constatato che il processo definito dal SIC per disporre l'adozione di una misura di acquisizione non soggetta ad autorizzazione ai sensi delle citate disposizioni crea i presupposti necessari per l'attuazione conforme alla legge di queste misure. Di principio, le misure di acquisizione non soggette ad autorizzazione attuate dal SIC vengono impiegate in modo conforme alla legge.

Per tutte le misure di acquisizione vige il principio secondo cui le informazioni acquisite sono inutili se non possono essere analizzate nell'immediato e in modo sistematico (in modo efficace e adeguato). Per delle videoregistrazioni, ad esempio, il SIC si affida a un software di analisi. In questo caso concreto l'AVI-AIn giunge alla conclusione che l'impiego di un tale software per favorire l'attività di analisi sia conforme alla legge.

Per quanto concerne l'utilizzo del sistema di ricerca informatizzato di polizia (RIPOL) e della parte nazionale del Sistema d'informazione di Schengen (N-SIS), l'AVI-AIn ha analizzato i processi necessari a effettuare segnalazioni nonché le autorizzazioni d'accesso e le consultazioni di dati in entrambi i sistemi. L'AVI-AIn constata che il processo legato alle segnalazioni in RIPOL e N-SIS di principio avviene in modo conforme alla legge. L'AVI-AIn ha invece constatato che non tutte le consultazioni in RIPOL e N-SIS effettuate dal SIC sono state documentate in maniera tale da dimostrare che erano dovute a motivi di servizio. Per questa ragione l'AVI-AIn raccomanda al SIC di sottoporre le consultazioni in RIPOL e N-SIS effettuate da collaboratori a controlli regolari e di documentare tali controlli.

Il SIC può adottare misure di acquisizione che secondo l'articolo 26 LAIn richiedono un'autorizzazione del Tribunale amministrativo federale nonché il nullaosta secondo l'articolo 30 LAIn (per esempio apparecchiature tecniche particolari per la sorveglianza del traffico delle telecomunicazioni, apparecchi di localizzazione, dispositivi di chiusura o di apertura ecc.). Nonostante tali misure richiedano un'autorizzazione e un nullaosta, potrebbero essere utilizzate dal SIC senza che gli organi preposti all'interno del SIC ne siano a conoscenza o ne abbiano autorizzato l'impiego. Nel quadro delle sue verifiche, l'AVI-AIn non ha riscontrato elementi che indicano che il SIC impieghi misure di acquisizione secondo l'articolo 26 LAIn senza la relativa autorizzazione e il relativo nullaosta.

23-11 Operazioni, necessità di accertamenti operativi e misure di acquisizione soggette ad autorizzazione del SIC

Le operazioni di intelligence (OP) e le necessità di accertamenti operativi (OPAB) rientrano tra i compiti fondamentali del SIC. Esse sono caratterizzate dal fatto che rispetto alle attività correnti sono più complesse e necessitano di una condotta operativa. Inoltre, nell'ambito delle OP, possono essere richieste anche misure di acquisizione soggette ad autorizzazione. La complessità delle OP e delle OPAB comporta regolarmente dei rischi sul piano dell'efficacia e dell'adeguatezza. Le misure soggette ad autorizzazione, dato che incidono nella sfera privata protetta, implicano sempre un rischio giuridico. Per questi motivi l'AVI-AIn verifica regolarmente queste attività del SIC.

Nell'ambito di questa verifica annuale, l'AVI-AIn ha analizzato la legalità, l'adeguatezza e l'efficacia di cinque OP e di tredici OPAB. Inoltre, per dodici misure di acquisizione autorizzate e approvate ha esaminato se l'attuazione corrispondeva alle decisioni del TAF. Le attività di verifica includevano lo studio della documentazione e interviste con gli specialisti competenti.

Questa verifica è iniziata nel 2023 e si è chiusa con il relativo rapporto a febbraio 2024. L'AVI-AIn ha pubblicato sul proprio sito web all'inizio dell'anno il riassunto delle risultanze di questa verifica.

23- 12 Fonti umane (HUMINT) presso il SIC

Per adempiere i propri compiti, il SIC acquisisce informazioni sia da fonti accessibili pubblicamente, sia da fonti non accessibili pubblicamente. A tal fine si avvale di misure di acquisizione soggette e non soggette ad autorizzazione. L'acquisizione di informazioni da fonti umane (HUMINT) costituisce una misura di acquisizione non soggetta ad autorizzazione. Per fonti umane si intendono informatori, nel senso di persone che comunicano al SIC informazioni o riscontri, che gli forniscono prestazioni utili per l'adempimento dei compiti secondo la LAIn o sostengono il SIC nell'acquisizione di informazioni. L'impiego di fonti umane comporta spesso rischi personali elevati, tanto per i collaboratori del SIC quanto per le fonti stesse. Ciò comporta per il SIC una responsabilità e un impegno particolari, che devono essere presi sul serio e che assumono una corrispondente importanza nell'attività di vigilanza svolta dall'AVI-AIn.

L'AVI-AIn verifica in che modo il SIC gestisce concretamente il proprio portafoglio di informatori e in che modo tale portafoglio evolve. Effettua controlli a campione e nell'ambito di questi controlli verifica la legalità, l'adeguatezza e l'efficacia delle relative attività. In questo campo, la protezione delle fonti e delle persone impone un particolare livello di riservatezza; di conseguenza, le verifiche HUMINT dell'AVI-AIn sono classificate SEGRETO.

Questa verifica è iniziata nell'agosto 2023 e alla chiusura di redazione del presente rapporto non era ancora stata ultimata. Per tale ragione non è ancora possibile esprimersi in merito ai risultati in questa sede. L'AVI-AIn prevede di pubblicare sul proprio sito web la sintesi della verifica nel 2024.

5.2.5 Risorse

Nell'ambito «Risorse» l'AVI-AIn verifica se vi è un uso adeguato delle risorse da parte dei servizi e se è garantita un'attività informativa efficace. La verifica 23-14 «Attuazione delle raccomandazioni dell'AVI-AIn» è stata cancellata. Nel 2023 l'AVI-AIn ha portato avanti le seguenti verifiche nell'ambito «Risorse»:

22-13 Flussi finanziari dissimulati

L'AVI-AIn ha verificato se il SIC dispone di metodi leciti, adeguati ed efficaci per generare flussi finanziari in modo da non comparire come mittente. Inoltre, ha verificato se le risorse finanziarie trasferite in tal modo sono impiegate esclusivamente per l'adempimento dei compiti previsti all'articolo 6 LAIn.

Nell'ambito di tale verifica, ha accertato che il SIC dispone di vari metodi collaudati e pronti per l'uso per far pervenire denaro ai destinatari senza comparire come mittente.

Il SIC designa come «supporter» le persone private che gli offrono sostegno per trasferire denaro in modo dissimulato e classifica queste persone tra le cosiddette «fonti umane». Anche la LAIn classifica tra le «fonti umane» le persone che offrono il loro sostegno al SIC nelle sue attività e gli forniscono prestazioni utili per l'adempimento dei suoi compiti. L'AVI-AIn è dello stesso parere e perciò raccomanda al SIC di assimilare la gestione dei supporter alla gestione delle «fonti umane» in senso stretto e di disciplinare tale gestione in modo vincolante. Tale disciplinamento deve comprendere in particolare un esame sistematico e ragionato dei rischi, dell'utilità, del potenziale e dei costi per supporter. Inoltre, i supporter devono essere elencati sommariamente come «fonti umane» nel rapporto annuale previsto dall'articolo 19 dell'ordinanza del 16 agosto 2017 sulle attività informative (OAI; RS 121.1).

Ai fini dell'esecuzione della LAIn, il SIC può collaborare con servizi di intelligence esteri svolgendo attività congiunte per l'acquisizione e l'analisi di informazioni e per la valutazione della situazione di minaccia. In relazione a due attività concrete svolte congiuntamente con servizi partner esteri, l'AVI-AIn ha constatato che il SIC, pur avendo riflettuto sulla legalità, sul rischio di reputazione assunto e sull'utilità prevista, non ha documentato in misura sufficiente tali riflessioni. Perciò, invita il SIC a consacrare in futuro maggiore attenzione a una documentazione accurata ed esaustiva di queste riflessioni e delle conseguenti decisioni.

22-14 Processo di reclutamento, di assistenza e di uscita

Per il SIC, dai collaboratori possono derivare rischi per la sicurezza quali tradimento, furto di dati o spionaggio. Potenzialmente è più probabile che collaboratori insoddisfatti si sentano indotti a lasciare il servizio e la fluttuazione che ne deriva comporta una serie di sfide. Possono andare perse preziose conoscenze e il reclutamento di nuovi collaboratori assorbe a sua volta risorse importanti.

A giudizio dell'AVI-AIn, negli ultimi anni questi rischi in seno al SIC sono cresciuti. Il notevole aumento del numero di indizi e informazioni sull'insoddisfazione dei collaboratori del SIC, gli avvicendamenti ai vertici del servizio, i risultati dell'ultimo sondaggio tra i collaboratori realizzato nel 2020 e l'alto tasso di fluttuazione in tutto il servizio hanno corroborato questa impressione.

L'AVI-AIn ha condotto un gran numero di interviste con i collaboratori ed eseguito controlli a campione nei dossier del personale. Queste attività di verifica si sono svolte da luglio a metà novembre 2022. Al momento della verifica il SIC era impegnato a preparare e realizzare una trasformazione nell'ambito della quale si è deciso di rivedere importanti documenti e processi nel settore del reclutamento, dell'assistenza e dell'uscita di collaboratori. Nel suo rapporto di verifica l'AVI-AIn ha tenuto conto di questo stadio particolare nello sviluppo dell'organizzazione. In sintesi, l'AVI-AIn ha constatato che nella sua strategia in materia di personale il SIC ha formulato i giusti obiettivi. Tali obiettivi trovano riscontro anche negli obiettivi della trasformazione.

L'AVI-AIn ha però constatato anche la presenza di gravi carenze nella gestione e conduzione del personale del SIC. Le carenze constatate riguardavano la documentazione nei dossier del personale, la conduzione dei colloqui con i collaboratori, le valutazioni dei collaboratori e la definizione della procedura da seguire in caso di accertamenti riguardanti collaboratori in situazioni particolarmente critiche. A questo riguardo l'AVI-AIn ha formulato varie raccomandazioni.

In particolare, le risorse dei servizi di supporto in seno al SIC, quali il settore del personale, devono essere potenziati, affinché sia possibile adempiere in modo corretto i compiti connessi con i processi di reclutamento, assistenza e uscita dei collaboratori. Al momento attuale questo aspetto è ancora più importante, poiché il SIC deve essere in grado di attuare in modo corretto la trasformazione in atto.

5.2.6 Trattamento dei dati / archiviazione

Nell'ambito «Trattamento dei dati / archiviazione» l'AVI-AIn verifica in particolare la legalità del trattamento delle informazioni, poiché le informazioni trattate dai servizi sono altamente sensibili e le disposizioni legali sono tanto ampie quanto complesse. Nel 2023 l'AVI-AIn ha svolto le seguenti verifiche nel suddetto ambito:

21-16 Servizi di telecomunicazione

Il SIC ha accesso alle informazioni riguardanti i fornitori svizzeri di servizi di comunicazione derivati (FSCD). L'acquisizione di metadati, quali per esempio le informazioni sul titolare di un conto utente, rappresentano una misura di acquisizione non soggetta ad autorizzazione. Tuttavia, se vengono acquisiti anche i contenuti di conversazioni e messaggi di testo, la misura è soggetta ad autorizzazione. Dunque, secondo l'AVI-AIn sussisteva il rischio che con riferimento a FSCD venissero eseguite misure di acquisizione di informazioni soggette ad autorizzazione senza il coinvolgimento e la necessaria autorizzazione del TAF. Di conseguenza, l'AVI-AIn ha deciso di esaminare questo rischio legato all'acquisizione di informazioni presso i FSCD da parte del SIC.

L'AVI-AIn ha quindi verificato se le informazioni del SIC sui servizi di una serie di operatori di telecomunicazioni fossero richieste in modo lecito e adeguato.

Le piattaforme dei FSCD al centro della verifica sono gestite in Svizzera e pertanto soggiacciono alle disposizioni della legge federale del 30 aprile 1997 sulle telecomunicazioni (LTC; RS 784.10). In virtù della LAIn¹, il SIC può richiedere informazioni secondo la legge federale del 18 marzo 2016 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT). Al fine di eseguire i compiti secondo la LAIn, il competente Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Servizio SCPT) del Dipartimento federale di giustizia e polizia (DFGP) su richiesta fornisce informazioni sui dati² al SIC.

Riguardo alle applicazioni che funzionano con la crittografia end-to-end, la legge permette al SIC di richiedere informazioni senza autorizzazione o di effettuare sorveglianze soggette ad autorizzazione.

La verifica ha evidenziato che il SIC ha trattato soltanto richieste legate al suo mandato di base. L'AVI-AIn ritiene che il processo per il trattamento centralizzato delle richieste sia adeguato. Il SIC però non sempre ha documentato integralmente le richieste verificate dall'AVI-AIn. In un caso, inoltre, nell'ambito di un'acquisizione di informazioni peraltro conforme alla legge, il SIC ha trattato informazioni supplementari che gli erano state trasmesse senza essere state richieste e in questa circostanza anche senza valida base legale. In entrambi i casi l'AVI-AIn ha emanato una raccomandazione.

22-15 Open Source Intelligence (OSINT)

L'Open Source Intelligence (OSINT) è un settore in rapido sviluppo dell'attività di acquisizione di informazioni svolta dai servizi di intelligence. Il collegamento di una quantità inesauribile di dati accessibili pubblicamente (Open Source Information, OSINF) offre ai servizi di intelligence possibilità quasi illimitate di acquisire informazioni. L'analisi delle OSINF, finalizzata a ottenere informazioni utili, è denominata OSINT. L'OSINT è una misura di acquisizione non soggetta ad autorizzazione ai sensi dell'articolo 13 LAIn e permette al SIC di procurarsi una grossa quantità d'informazioni rilevanti per l'adempimento del proprio scopo legale. L'OSINT è in costante sviluppo e solleva questioni di natura giuridica ed etica tra gli addetti ai lavori a livello internazionale, per esempio quella della delimitazione dell'OSINT rispetto alla ricerca d'informazioni tramite informatori (HUMINT), o tramite l'impiego d'identità fittizie per relazionarsi a degli obiettivi su internet, o ancora l'acquisizione e l'utilizzo di banche dati trafugate da terzi (*leaks*). Di conseguenza, l'AVI-AIn ha deciso di esaminare in che modo il SIC affronta i rischi legati a questo strumento.

¹ Art. 25 cpv. 2 LAIn

² Art. 21 e 22 LSCPT

Secondo l'articolo 13 LAIn, sono considerate fonti d'informazione pubbliche segnatamente i media accessibili al pubblico, i registri accessibili al pubblico di autorità della Confederazione e dei Cantoni, i dati personali che privati rendono accessibili al pubblico o le dichiarazioni rese in pubblico. Il limite tra OSINT e misure di acquisizione soggette ad autorizzazione non è sempre netto ed è tema di discussione anche presso i servizi partner del SIC e le autorità di vigilanza estere. Senza una concezione comune di questi limiti, si corre il rischio di acquisire dati illecitamente. Dalle interviste condotte con collaboratori del settore OSINT del SIC è emerso che essi sono consapevoli del fatto che operano in un contesto giuridico complesso. Tuttavia, non esistono criteri o una direttiva strutturata per determinare ciò che è realmente l'OSINT e quali sono i limiti del quadro giuridico di questa attività. Quindi, l'impiego delle varie misure di acquisizione in ambito OSINT non è disciplinato in modo chiaro e uniforme in seno al SIC. L'AVI-AIn ha formulato una raccomandazione con cui chiede di delimitare il quadro giuridico per le attività operative concrete del SIC che si fondano sull'OSINT e di stabilire norme uniformi per l'impiego dell'OSINT.

L'AVI-AIn ha verificato una serie di acquisizioni OSINT senza trovare elementi che indicano un'acquisizione illecita di informazioni. Secondo l'articolo 22 capoverso 1 dell'ordinanza del 25 novembre 1998 sull'organizzazione del Governo e dell'Amministrazione (OLOGA) in combinato disposto con l'articolo 52 LAIn, alle unità amministrative viene imposto di documentare la loro attività con una gestione degli affari sistematica. Inoltre, il capitolo 2 delle Istruzioni del 7 luglio 2022 concernenti la conservazione e l'archiviazione di documenti in seno al SIC prescrive, in virtù dell'articolo 2 dell'ordinanza del 3 aprile 2019 sulla gestione elettronica degli affari nell'Amministrazione federale (ordinanza GEVER), che tutti i documenti rilevanti per gli affari devono essere registrati e archiviati nel GEVER SIC. In singoli casi la documentazione degli accertamenti OSINT era lacunosa e non rispettava le vigenti prescrizioni nell'Amministrazione federale, ciò che ha reso impossibile una valutazione della conformità alla legge da parte dell'AVI-AIn. L'AVI-AIn ha formulato una raccomandazione in proposito.

Per poter raccogliere in modo adeguato ed efficace informazioni rilevanti per l'intelligence partendo dall'enorme quantità di dati disponibili nell'ambito pubblico di Internet, si utilizzano i cosiddetti «tool OSINT». Il SIC utilizza sia prodotti standard reperibili in commercio sia prodotti sviluppati in proprio. Con questi tool e avvalendosi tra l'altro di identità virtuali fittizie (IVF) conduce sia un monitoraggio permanente sia ricerche mirate. Dato che servono per attività di intelligence, le IVF utilizzate presentano anomalie e perciò potrebbero essere considerate come potenziali bersagli da altri servizi e attirare l'attenzione per esempio di servizi partner esteri. Per contrastare questo rischio, l'AVI-AIn ha suggerito al SIC di assicurare con i SICant un'informazione reciproca sulle IVF utilizzate.

Per l'acquisizione di informazioni OSINT anonimizzata, il SIC utilizza un'infrastruttura informatica speciale. Questa infrastruttura è affetta da lacune di sicurezza e dovrebbe essere sostituita al più presto. L'AVI-AIn ha formulato una raccomandazione in proposito.

La verifica delle informazioni tratte da ricerche OSINT non è sempre cosa semplice, in particolare se le informazioni provengono dal *darknet*. Secondo il SIC, le attività di intelligence implicano una sana diffidenza nei confronti delle informazioni acquisite. Se un'informazione non può essere verificata e il grado di veridicità del suo contenuto non può essere quantificato, nei rapporti OSINT questo aspetto viene indicato. Il problema della verifica delle fonti, che assume un ruolo importante per esempio per identificare e svelare le fake news, è noto in particolare nell'impiego di tool OSINT commerciali complessi e se ne discute regolarmente anche all'interno della comunità dei servizi di intelligence.

Oltre al SIC, anche i SICant svolgono accertamenti legati all'OSINT. L'AVI-AIn ha esaminato se esistono ridondanze e inefficienze. È giunta alla conclusione che tutti i servizi sono sensibilizzati in merito ai rischi e ha constatato per esempio che discutono regolarmente la questione dell'OSINT in un contesto creato appositamente.

Il contenuto del sistema d'informazione Portale OSINT (risultati di ricerche e materiale grezzo tratto da fonti pubbliche) è disciplinato dall'articolo 54 capoverso 2 LAIn e dagli articoli 46 e seguenti dell'OSIME-SIC. Il SIC utilizza questo sistema d'informazione per mettere a disposizione al suo

interno dati provenienti da fonti accessibili al pubblico. Le attività di controllo dell'AVI-AIn, e in particolare i controlli a campione, non hanno fatto emergere indizi di violazione dei principi di adeguatezza o efficacia nella gestione dei dati sul portale OSINT. Il rischio di prolungamento illecito del termine di conservazione, legato a un'etichettatura sbagliata dei dati come dati OSINT generata da altri sensori, è risultato inesistente, poiché i dati OSINT hanno un termine di conservazione più breve.

22-17 Follow-up 20-19: archivi SIC

La verifica 22-17 è un follow-up della verifica 20-19 «Archivi SIC e in particolare archivi segreti». Questa verifica era stata organizzata dopo che i media, in relazione al caso della Crypto AG, avevano riportato che il SIC possedeva «archivi segreti». Nell'ambito della verifica 20-19 l'AVI-AIn aveva constatato tra l'altro che documenti analogici classificati SEGRETI venivano conservati in un luogo anch'esso classificato SEGRETO. A quel momento, il SIC e l'Archivio federale svizzero (AFS) stavano discutendo in merito alla consegna di documenti da archiviare, tra cui anche alcuni di quelli citati dai media. La documentazione in questione riguardava soprattutto documenti delle organizzazioni precedenti al SIC risalenti agli anni precedenti al 2010. Pertanto, l'AVI-AIn ha rinunciato a emanare raccomandazioni e ha annunciato un follow-up.

Oltre ai rischi di reputazione, nell'ambito della verifica 22-17 l'AVI-AIn ha esaminato anche i rischi relativi alla legalità, all'adeguatezza ed all'efficacia dell'archiviazione e della conservazione di documenti. Per quanto riguarda l'archiviazione, occorre chiarire se i documenti fossero stati consegnati in modo legalmente e contrattualmente conforme, se fossero stati sottratti o distrutti documenti prima o dopo averli offerti o dopo che ne era stato riconosciuto il valore archivistico. Quanto alla conservazione di documenti, la verifica era volta a esaminare se i documenti conservati avrebbero dovuto essere archiviati e se le norme in materia di conservazione venivano rispettate.

Nell'ambito della verifica 22-17, l'AVI-AIn ha visitato i luoghi di conservazione dei documenti ed effettuato controlli a campione. In tale contesto ha constatato che nelle varie sedi in cui il SIC conserva documenti le attività di archiviazione dei documenti analogici (principalmente documenti cartacei e *microfiche*) sono decisamente avanzate. Nel complesso, l'AVI-AIn ha potuto accertare che la situazione si è concretizzata e sviluppata positivamente e che gli impegni assunti nell'ambito della verifica 20-19 riguardanti principalmente l'attuazione dell'accordo con l'AFS sono stati onorati. I lavori eseguiti rispettano tale accordo. Termini di consegna non sono stati rispettati per ragioni comprensibili, plausibili e ascrivibili soltanto in parte al SIC. Diverse migliaia di documenti (circa 200 metri lineari) e milioni di microfiche, che riguardavano principalmente le organizzazioni precedenti al SIC, sono stati repertoriati e consegnati all'AFS. I documenti consegnati riguardano il periodo tra il 1938 e il 2021.

I documenti delle organizzazioni precedenti non erano repertoriati, perciò l'AVI-AIn non ha potuto analizzare i rischi identificati, e in particolare non ha potuto esaminare se tutti i documenti fossero stati effettivamente offerti e consegnati all'AFS, o se alcuni fossero stati distrutti, per errore o intenzionalmente. L'AVI-AIn non ha scoperto segni di un'eventuale realizzazione di questi rischi.

I lavori di presa in visione e archiviazione dei documenti non sono ancora terminati. Sotto questo aspetto l'accordo non è ancora stato completamente attuato. Il SIC è stato invitato a far evolvere questa situazione. L'AVI-AIn ha constatato che i documenti conservati non sono repertoriati e ha pertanto emesso una raccomandazione che chiede al SIC di allestire un inventario dei documenti che non vengono consegnati all'AFS ma conservati dal servizio stesso.

22-18 Acquisizione di dati da parte del settore cyber del SIC

L'acquisizione illecita di informazioni da parte del settore cyber del SIC, di cui hanno parlato vari media, è stata trattata sia con un'indagine interna del SIC stesso sia nell'ambito di un'inchiesta amministrativa condotta da persone esterne. L'AVI-AIn ritiene che da entrambi i rapporti emergano ancora questioni irrisolte e pertanto ha avviato una verifica propria su questi fatti non ancora completamente chiariti. L'analisi dei voluminosi insiemi di dati, che sinora non erano stati visionati o valutati né dal SIC stesso né nell'ambito della suddetta inchiesta amministrativa, si è rivelata impegnativa anche in termini di dispendio di tempo e al momento della chiusura di redazione del presente rapporto di attività non

era ancora conclusa. Per tale ragione non è ancora possibile esprimersi in merito ai risultati in questa sede. L'AVI-AIn prevede di pubblicare sul proprio sito web la sintesi della verifica nel 2024.

23-16 Sistemi d'informazione, sistemi di memorizzazione e memorie di dati al di fuori dell'articolo 47 della legge federale sulle attività informative

La LAIn contiene una serie di norme sul trattamento dei dati e al suo articolo 47 fornisce un elenco dei sistemi d'informazione gestiti dal SIC. Il carattere esaustivo di questo elenco era già stato oggetto di discussioni al momento dell'elaborazione della nuova legge sulle attività informative. L'AVI-AIn ha voluto chiarire tale questione giuridica e anche valutare quali altri sistemi sono utilizzati e le ragioni del loro utilizzo. Sono state analizzate anche le pertinenti basi legali.

La verifica 23-16 è iniziata nell'agosto 2023 e alla chiusura di redazione del presente rapporto non era ancora stata ultimata. Pertanto, a questo punto non è possibile fare ulteriori dichiarazioni sui risultati dell'audit. L'AVI-AIn prevede di pubblicare sul proprio sito web la sintesi della verifica nel 2024.

Accertamenti riguardanti il ciberattacco contro la ditta Xplain AG

In seguito al ciberattacco sferrato contro la ditta Xplain AG, l'AVI-AIn ha condotto accertamenti non previsti dal suo consueto piano annuale di controllo. Tali accertamenti erano volti a esaminare se e quanto l'attacco riguardasse anche dati del SIC e in che modo il SIC stesse trattando l'incidente nell'ambito del suo mandato di base. Le informazioni tratte in questo contesto sono in parte confluite nella verifica 23-10 «Collaborazione del SIC con privati».

5.3 Atteggiamento cooperativo

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 ai sistemi d'informazione necessari per poter adempiere il loro mandato di verifica. Le persone intervistate erano a loro disposizione. Alle domande complementari è stata data risposta il più rapidamente possibile.

5.4 Controlling delle raccomandazioni

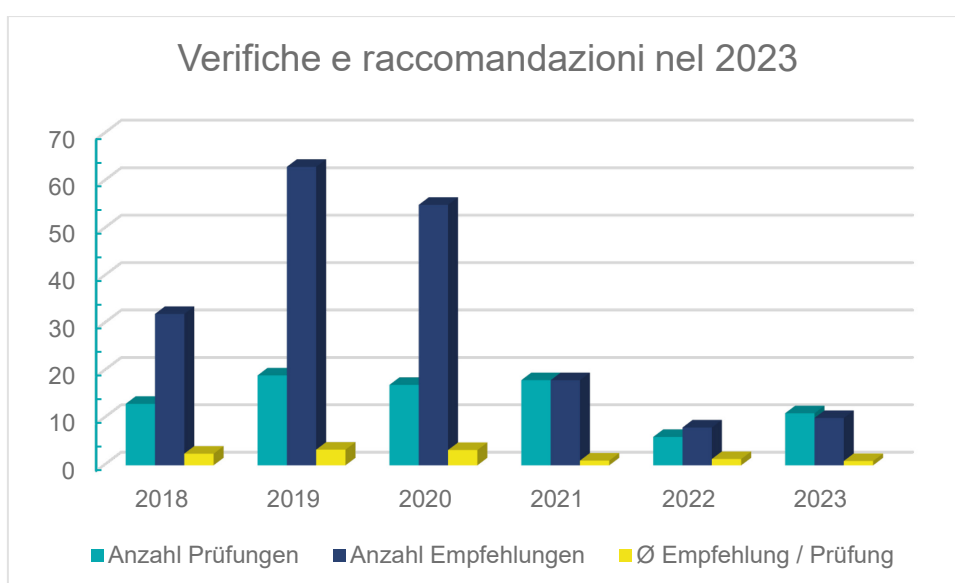
In seguito alle sue attività di verifica, l'AVI-AIn può formulare raccomandazioni. Esse vengono indirizzate al capo del DDPS. In seguito, il DDPS provvede alla loro concreta attuazione. Se respinge una raccomandazione, la sottopone al Consiglio federale per decisione, ma sinora ciò non è mai successo.

Secondo le basi legali applicabili, l'AVI-AIn formula le raccomandazioni e il DDPS le attua. Le basi legali in materia di intelligence dispongono che l'AVI-AIn ha facoltà di emanare raccomandazioni, ma non si esprimono né sulla qualità della loro attuazione né sul relativo controllo.

Tuttavia, una vigilanza efficace e credibile implica non solo che le raccomandazioni emanate vengano attuate, ma anche che la loro attuazione venga verificata. Insieme ai servizi sottoposti a vigilanza e al DDPS, l'AVI-AIn si sta occupando di perfezionare questa parte complessa della vigilanza.

Il grafico seguente illustra il rapporto tra il numero di verifiche e le conseguenti raccomandazioni negli ultimi sei anni. Dopo una fase iniziale di tre anni con in media due o tre raccomandazioni per verifica, nei tre anni successivi è stata formulata in media una sola raccomandazione per ogni verifica. L'AVI-AIn vuole che le sue raccomandazioni abbiano un'utilità concreta per la riduzione o la soppressione dei rischi e procede coerentemente in tal senso; questo approccio si rispecchia nelle cifre. Pertanto, con l'andar del tempo vengono emanate meno raccomandazioni, che però sono più mirate ed efficaci. Il numero di raccomandazioni non è indice né dei miglioramenti ottenuti né di un peggioramento della situazione, poiché nessuna verifica viene ripetuta tale e quale ad oggi.

	2018	2019	2020	2021	2022	2023
Numero di verifiche concluse nell'anno indicato	13	19	17	18	6	11 ³
Numero di raccomandazioni	32	63	55	18	8	10
∅ Raccomandazione/verifica	2,46	3,32	3,24	1,00	1,33	0,91



6 Sguardo all'interno dell'AVI-AIn

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

6.1 Personale

Nel 2023 l'AVI-AIn disponeva di un effettivo di 10 collaboratori. Nel 2023 sono partiti due collaboratori ed è stato dato il benvenuto a due nuovi colleghi.

6.2 Formazioni e formazioni continue

Formazione continua presso armasuisse in materia di scienza dei dati

Anche nel 2023 l'AVI-AIn ha sfruttato la possibilità di informarsi presso armasuisse in merito allo stato di avanzamento dei progetti di ricerca attuali. Come nel 2022, era interessata principalmente al programma di ricerca sulla scienza dei dati. Mentre nel 2022 i relatori si erano concentrati sulla questione di sapere come si può riuscire a stabilire l'autenticità delle immagini e dei contenuti pubblicati sui media, il simposio organizzato nel 2023 è stato consacrato all'impiego dell'intelligenza artificiale (IA) per l'analisi dei dati, e precisamente sugli strumenti che funzionano grazie all'IA, poiché l'intelligenza artificiale sta progredendo molto rapidamente. Ad oggi, l'IA è in grado di trarre dai dati informazioni che servono a loro volta per creare conoscenza. Gli strumenti IA disponibili

³ 21-16 (2)/22-1 (1)/22-5 (0)/22-8 (0)/22-10 (1)/22-13 (1)/22-14 (4)/22-17 (1)/23-5 (0)/23-8 (0)/23-9 (0).

attualmente vengono impiegati per riconoscere modelli e ripetizioni nelle serie di dati. Attualmente la ricerca si propone di sviluppare l'IA fino al punto di poter trarre da essa previsioni fondate per il futuro. A questo riguardo svolgono un ruolo importante sia la possibilità di comprendere le correlazioni e le correlazioni apparenti tra i dati, sia i metodi che permettono di garantire la solidità delle induzioni.

Formazione continua «Come effettuare un audit»

Due collaboratori dell'AVI-AIn hanno assolto una formazione continua offerta dal Centro di formazione dell'Amministrazione federale su come effettuare un audit. Questo corso è stato scelto perché trattava delle buone pratiche in materia di audit, consentiva di aggiornare determinate competenze e di confrontare la propria prassi con quella di altri servizi dell'Amministrazione federale che effettuano audit.

Il corso illustrava le varie fasi di un audit, dalla preparazione fino alla finalizzazione. Inoltre, trattava anche il ruolo degli auditor e i principi da seguire nel realizzare un audit. I vari lavori di gruppo hanno consentito ai partecipanti di confrontare le loro esperienze. Infine, è stato trattato anche il tema della formulazione di raccomandazioni e conclusioni alla fine di un audit.

Quest'ultimo tema è stato particolarmente utile per i collaboratori dell'AVI-AIn. Infatti, la formulazione di raccomandazioni è una questione che attualmente viene discussa anche internamente con l'intenzione di migliorare in questo campo. Redigendo un lavoro di transfer, i partecipanti dell'AVI-AIn al corso hanno potuto trattare nei dettagli il tema. Il documento da loro redatto servirà in futuro come base di riflessione per poi introdurre le ottimizzazioni auspiccate in seno all'AVI-AIn. Esso ha permesso di stabilire che nel formulare raccomandazioni occorre trovare un equilibrio tra una formulazione esaustiva e dettagliata e il mantenimento di un certo margine di manovra per l'autorità sottoposta a vigilanza. Tale margine di manovra consente all'autorità sottoposta a vigilanza di assumersi la propria responsabilità nell'attuare la raccomandazione. Una raccomandazione «ben formulata» indica al servizio sottoposto a vigilanza anche il rischio che occorre ridurre al minimo. Ciò consente di comprendere e di attuare la raccomandazione stessa in modo migliore.

Certificate of Advanced Studies (CAS) Digital Forensics and Cyber-Investigation-Fundamentals

Nell'anno in rassegna, un collaboratore dell'AVI-AIn ha assolto un CAS sul tema della scienza forense digitale e delle inchieste in ambito ciber, composto da quattro moduli: «Basi della scienza digitale forense», «Fondamenti delle inchieste in ambito ciber», «Panoramica della cibercriminalità» e «Acquisizione nell'ambito della scienza digitale forense». Le nozioni apprese durante questo corso di formazione continua sono direttamente confluite nella verifica 22-18 e nella conseguente analisi di dati. Per esempio, una procedura nota nell'ambito della scienza forense ciber è stata applicata per analizzare una serie di dati voluminosa.

CAS Comunicazione

L'AVI-AIn crea autonomamente i contenuti che pubblica sul proprio sito web e ogni anno allestisce e pubblica per proprio conto anche il rapporto di attività. Per approfondire le conoscenze specialistiche in materia di comunicazione, una collaboratrice si è iscritta a un CAS in comunicazione, che concluderà nel 2024.

Information Systems Audit and Control Association (ISACA) Conferenza Europa: «Digital Trust World», 18-19 ottobre 2023, Dublino

L'ISACA è un'associazione di categoria indipendente di revisori dei conti, revisori informatici e professionisti operanti nel settore della governance informatica e della sicurezza delle informazioni. Un collaboratore dell'AVI-AIn titolare di una certificazione ISACA come revisore informatico ha partecipato alle due giornate della conferenza europea annuale dell'associazione.

Diverse relazioni specialistiche su temi attuali riguardanti un ecosistema digitale sicuro e affidabile hanno permesso di approfondire le conoscenze specialistiche e di discutere e confrontarsi in merito a nuove conoscenze, tendenze e procedure collaudate. La conferenza era incentrata anche sulla questione del possibile influsso dell'intelligenza digitale e del «machine learning» sulla situazione in materia di sicurezza, ma anche sulle attività di revisione in ambito ciber. Le conoscenze acquisite sono state messe a frutto sia nella gestione dei rischi propria all'AVI-AIn sia nelle attività di verifica.

Evento informativo dell'IFPDT sulla protezione dei dati, 17 agosto 2023

In vista dell'entrata in vigore della nuova legge sulla protezione dei dati (LPD), l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) ha organizzato un evento informativo per gli incaricati della protezione dei dati degli organi della Confederazione. L'evento si è tenuto il 17 agosto 2023 all'Università di Friburgo e si è rivelato un pieno successo. Due collaboratori dell'AVI-AIn vi hanno partecipato e all'evento hanno incontrato in particolare anche collaboratori dei servizi sottoposti a vigilanza.

I temi riguardanti le novità introdotte nella LPD sono stati presentati dall'IFPDT e da alcuni suoi collaboratori nonché da rappresentanti dell'Ufficio federale della cibersicurezza (UFCS) e dell'Ufficio federale di polizia (fedpol); tra i temi trattati vi erano in particolare le valutazioni d'impatto sulla protezione dei dati (VIPD), l'impiego del nuovo registro delle attività di trattamento, la nuova competenza dell'IFPDT di aprire inchieste per violazioni delle disposizioni sulla protezione dei dati, la verbalizzazione e altro ancora. Le presentazioni sono state molto istruttive e avranno un'utilità sia per l'attività amministrativa dell'AVI-AIn sia nell'ambito delle attività di vigilanza.

6.3 Verifica condotta sull'AVI-AIn dal Controllo federale delle finanze (CDF)

Il CDF è l'organo supremo di controllo finanziario della Confederazione e nei limiti delle disposizioni di legge è un'entità autonoma e indipendente. La stessa indipendenza istituzionale iscritta nella legge è garantita anche all'AVI-AIn.

Il CDF esercita la vigilanza finanziaria secondo i criteri della regolarità, della legalità e della redditività. In particolare, verifica i sistemi di controllo interni o effettua controlli a campione degli ordini di pagamento emessi dalle unità amministrative. Il CDF è responsabile della revisione delle unità amministrative, contabilità ed effettivi compresi. L'AVI-AIn non effettua le sue verifiche secondo gli stessi criteri. Il suo mandato legale è molto diverso rispetto a quello del CDF.

Nel suo programma annuale per il 2023 il CDF ha annunciato una verifica presso l'AVI-AIn. Tale verifica si è svolta dal 14 agosto al 1° settembre 2023 e ha riguardato l'attività di vigilanza esercitata dall'AVI-AIn. La verifica è servita a valutare l'efficacia e l'economicità della vigilanza esercitata dall'AVI-AIn sulle attività di intelligence. Il 12 giugno 2023 il CDF ha presentato all'AVI-AIn i suoi quesiti:

1. La vigilanza esercitata dall'AVI-AIn sulle attività di intelligence è conforme alle basi legali?
2. Le risorse di cui dispone l'AVI-AIn bastano per garantire una vigilanza adeguata su tutti gli attori che operano nel campo delle attività di intelligence?
3. L'infrastruttura informatica in quanto strumento di lavoro consente di esercitare la vigilanza in modo efficiente?

Già nella primavera del 2023 l'AVI-AIn aveva fornito al CDF sei dossier completi del 2021 e del 2022 come campione per la verifica e altri documenti, tra cui per esempio concetti e manuali. Il CDF ha intervistato numerosi collaboratori dell'AVI-AIn, dei vari servizi sottoposti a vigilanza e della Segreteria generale del DDPS (SG-DDPS).

Nel formulare il loro giudizio, i revisori del CDF si sono dovuti impegnare a non confrontare eccessivamente le due autorità (CDF e AVI-AIn). **Dal punto di vista dell'AVI-AIn era importante che il CDF capisse il fatto che essa esercita un'attività di vigilanza diversa e quindi funziona diversamente rispetto al CDF.** Nell'incontro finale, queste differenze fondamentali sono state discusse ancora una volta, in modo da raggiungere una sintonia tra le diverse competenze delle

due autorità. Il CDF continua a esercitare la sua vigilanza secondo criteri propri e la creazione dell'AVI-Aln non ha comportato cambiamenti nella sua sfera di competenza.

6.4 Accesso a documenti e informazioni ufficiali

L'AVI-Aln, in quanto parte dell'Amministrazione federale decentralizzata, opera su mandato dei cittadini. I cittadini hanno il diritto di sapere cosa fanno le autorità e in che modo adempiono il loro mandato. Per derivazione da questo principio, essi hanno da un lato il diritto di accedere alle informazioni e dall'altro le autorità hanno l'obbligo di informare.

La legge federale del 17 dicembre 2004 sul principio di trasparenza dell'amministrazione (legge sulla trasparenza, LTras, RS 152.3) disciplina la portata e i limiti dell'informazione passiva. Ogni persona può chiedere di accedere a documenti ufficiali senza dover invocare un interesse particolare. Nell'anno in esame, l'AVI-Aln ha ricevuto una richiesta di visionare documenti ufficiali.

7 Coordinamento

Conformemente all'articolo 78 capoverso 2 LAln, l'AVI-Aln deve coordinare la sua attività con le attività di vigilanza parlamentare e con altre autorità di vigilanza della Confederazione e dei Cantoni.

7.1 Contatti nazionali

Delegazione delle Commissioni della gestione (DeICG)

La DeICG ha invitato l'AVI-Aln a due consultazioni, in occasione delle quali si è discusso in particolare del rapporto relativo alla verifica 22-13 «Flussi finanziari clandestini», delle esperienze del capo nel primo anno nella sua funzione, dell'ulteriore sviluppo della prassi dell'AVI-Aln in materia di raccomandazioni e del piano di controllo 2024.

Tribunale amministrativo federale (TAF)

Come già negli anni scorsi, anche nell'anno in esame l'AVI-Aln ha avuto un colloquio con il TAF. Le due autorità hanno discusso delle attuali operazioni del SIC per le quali sono state sottoposte al TAF misure di acquisizione soggette ad autorizzazione nonché degli attuali sviluppi in materia di esplorazione di segnali via cavo.

Dalle discussioni è emerso che la giurisprudenza si sviluppa costantemente e che il TAF è confrontato più spesso con questioni tecniche in ambito ciber. Con questa sfida è confrontata anche l'AVI-Aln, poiché con l'avanzare della digitalizzazione le attività di verifica si concentrano sempre più sui sistemi d'informazione. Tanto il TAF quanto l'AVI-Aln sono giunti alla conclusione che se i servizi di intelligence non illustrano le implicazioni tecniche non è possibile né decidere in merito a una richiesta né esercitare una vigilanza sufficiente.

Controllo federale delle finanze (CDF)

Nell'ambito del coordinamento con il CDF si sono svolti i seguenti incontri:

- 20 febbraio 2023: in occasione di questo incontro è stata presentata all'AVI-Aln l'IIA (Institute of Internal Auditors) e sono stati discussi vantaggi e svantaggi di un'eventuale adesione.
- 13 marzo 2023: in questa occasione sono stati discussi i criteri di protezione dei collaboratori in caso di segnalazioni su comportamenti scorretti all'interno dell'amministrazione federale (whistleblowing).
- 6 dicembre 2023: il nuovo responsabile del mandato per il DDPS si è presentato. Sono stati discussi diversi aspetti relativi al coordinamento, eventualmente occorrerà elaborare un accordo di coordinamento per definire gli aspetti comuni o diversi delle rispettive competenze

in materia di verifica ed evitare così che alcuni elementi specifici delle attività di verifica non vengano mai verificati.

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

L'AVI-AIn ha partecipato a tutte le cinque sedute dell'ACI.

L'integrazione delle attività di vigilanza in seno all'AVI-AIn, prevista dalla revisione della LAIn, ha subito un rallentamento. Perciò, nell'ambito del coordinamento, l'AVI-AIn continua a seguire i lavori dell'ACI e rinuncia per ora ad altre attività preparatorie.

Incaricato federale della protezione dei dati e della trasparenza (IFPDT)

Nell'ambito delle sue attività di verifica, l'AVI-AIn controlla i sistemi d'informazione utilizzati dai servizi sottoposti a vigilanza e il trattamento dei relativi dati. Inoltre, può verificare le ricerche effettuate da questi servizi nei dati il cui trattamento incombe ad altre autorità federali non sottoposte a vigilanza. L'autorità responsabile della vigilanza sul trattamento dei dati da parte delle autorità federali è l'IFPDT. Le competenze di quest'ultimo e dell'AVI-AIn, due autorità indipendenti dall'Amministrazione federale nell'adempimento dei rispettivi compiti, in parte si sovrappongono. Per evitare confusioni sulle competenze o accavallamenti tra le autorità di vigilanza, l'AVI-AIn e l'IFPDT concordano reciprocamente le loro attività e coltivano contatti regolari.

Nel febbraio 2023, nell'ambito di un incontro di coordinamento l'IFPDT e il capo dell'AVI-AIn hanno deciso di formalizzare la prassi attuale, che appare funzionale e adeguata. Nel maggio 2023 le due autorità hanno sottoscritto un accordo di coordinamento.

Richieste dei cittadini

Nel 2023 l'AVI-AIn ha ricevuto 20 richieste da parte di cittadini.

Ulteriori incontri

Nel 2023 la direzione dell'AVI-AIn si è trovata almeno una volta per uno scambio di opinioni con le seguenti persone:

- capo del DDPS;
- capo dell'esercito;
- segretario generale del DDPS;
- direttore e direttore supplente del SIC;
- capo del SIM;
- capo del COE;
- capo della Revisione interna DDPS;
- capo del Comando Operazioni;
- capo del Comando Ciber;
- consulente del DDPS in materia di intelligence;
- i membri dell'ACI.

7.2 Contatti internazionali

Riguardo a metodi, processi ed esperienze di vigilanza, l'AVI-AIn ha modo di confrontarsi con autorità di vigilanza di altri Paesi che operano nello stesso campo di attività. Ciò si rivela essere un valore aggiunto costante per le attività di verifica. Diversamente dai servizi informazioni, per l'AVI-AIn non esiste alcuna base legale che consenta un confronto con le autorità partner straniere su questioni di contenuto. Nel 2023 si sono tenuti i seguenti incontri internazionali.

Incontro virtuale con l'autorità di vigilanza canadese (National Security and Intelligence Review Agency [NSIRA]), 27 aprile 2023

Dopo la visita di una delegazione della NSIRA, che si era tenuta a Berna il 17 novembre 2022, il 27 aprile 2023 le due autorità di vigilanza si sono incontrate in forma virtuale.

In occasione di questo incontro la NSIRA ha presentato in particolare la sua storia, il suo mandato e la sua struttura. È stata istituita nel 2019 ed è un servizio indipendente che rende conto al Parlamento. I suoi compiti consistono essenzialmente nell'effettuare verifiche ed esaminare ricorsi. Essa verifica la legalità, l'idoneità, la necessità e l'efficacia delle attività del Servizio della sicurezza nazionale e delle attività di intelligence di tutti i ministeri e servizi del governo canadese. Sulla base dei risultati delle sue verifiche vengono emanate raccomandazioni. L'attività della NSIRA è simile a quella dell'AVI-AIn. Tuttavia, il segretariato dell'autorità di vigilanza canadese è composto da più di 70 persone e il settore di competenza è molto più ampio di quello dell'AVI-AIn. Dal punto di vista organizzativo, la NSIRA può contare sull'appoggio di un'unità specializzata che si occupa dell'evoluzione delle tecnologie e del loro impiego nelle attività di intelligence.

Intelligence Oversight Working Group (IOWG)

L'IOWG è un gruppo di lavoro internazionale composto di rappresentanti del Belgio, della Danimarca, dei Paesi Bassi, della Norvegia, dell'Inghilterra, della Svezia e della Svizzera. Da novembre 2023 l'autorità canadese NSIRA ha ottenuto lo statuto di osservatore per il 2024 presso questo gruppo di lavoro.

IOWG, incontro tra collaboratori delle autorità, 25 e 26 maggio 2023, L'Aia

All'inizio dell'incontro, i partecipanti hanno presentato vari sviluppi subentrati nei rispettivi Stati dopo l'ultimo incontro tenutosi nel 2022. In futuro i Paesi Bassi metteranno a disposizione dei membri dell'IOWG una piattaforma digitale per i loro incontri, sulla quale potranno essere caricate le loro presentazioni. La Norvegia ha presentato i suoi metodi e le sue modalità operative in materia di comunicazione. Un altro tema riguardava l'impiego di agenti virtuali e le varie normative degli Stati membri, con particolare riguardo alla delimitazione rispetto all'OSINT. Infine, un tecnico dell'autorità di vigilanza olandese ha presentato le proprie riflessioni sull'intelligenza artificiale e sulle decisioni automatizzate. Tutti hanno convenuto che i servizi e le autorità di vigilanza devono occuparsi maggiormente di questo tema.

IOWG, incontro tra collaboratori delle autorità, 8 e 9 novembre 2023, Oslo

L'8 novembre 2023 i collaboratori dell'IOWG si sono riuniti per preparare un incontro della direzione previsto il giorno successivo. In particolare, hanno elaborato una proposta di agenda per gli incontri del 2024 e proposto i seguenti temi:

- insiemi di dati acquistati sul mercato e utilizzati dai servizi sottoposti a vigilanza;
- organizzazione di uno scambio online su determinati temi tra un incontro e l'altro dell'IOWG;
- controlli di sicurezza relativi alle persone; scambio sulle normative e prassi in materia di controlli di sicurezza nei vari Stati membri dell'IOWG;
- discussione in merito alle possibili forme di cooperazione internazionale tra autorità di vigilanza;
- vigilanza in generale: presentazione dei vari metodi di vigilanza applicati dai diversi Paesi.

IOWG, incontro a livello direttivo, 9 novembre 2023, Oslo

Il 9 novembre 2023 si sono riuniti i capi delle varie autorità di vigilanza. L'agenda proposta dallo staff è stata approvata e tutti hanno apprezzato in particolare l'idea di una discussione approfondita sui metodi. All'autorità di vigilanza canadese è stato conferito su sua richiesta lo statuto di osservatore in seno all'IOWG.

Incontro dell'IOWG con un'autorità statunitense e varie organizzazioni non governative (ONG), 27 novembre 2023, Washington

La mattina del 27 novembre 2023 l'IOWG ha organizzato, a margine dell'IIOF di Washington (vedi più avanti) un incontro con il *Privacy and Civil Liberties Oversight Board* (PCLOB). Il PCLOB è un'autorità indipendente integrata nel governo statunitense e costituita con il *9/11 Commission Act* del 2007. Si tratta di un comitato sovrapartitico composto da cinque persone, nominato dal presidente e confermato dal Senato. La persona che presiede il comitato opera a tempo pieno, mentre gli altri quattro membri esercitano la loro funzione a tempo parziale. Il comitato ha il compito di provvedere affinché le attività del governo federale in materia di prevenzione del terrorismo possano conciliarsi con la necessità di tutelare la sfera privata e le libertà civili. Si è rivelato particolarmente interessante lo scambio sul termine «open» nell'ambito delle acquisizioni open source (OSINT) nonché sul rapido sviluppo e sull'impiego di strumenti IA.

Nel pomeriggio si è tenuto un incontro presso il *Center for Democracy & Technology* e con altre ONG. Anche in questo contesto si è ampiamente discusso di acquisizioni OSINT e in particolare la possibilità di ricorrere ai *data broker*. In seguito i partecipanti si sono occupati della questione se o come i servizi di intelligence potrebbero condividere informazioni ed eludere in tal modo l'obbligo di autorizzazione previsto per la loro acquisizione.

European Intelligence Oversight Conference (EIOC), 9 e 10 novembre 2023, Oslo

Il ricco programma dell'edizione 2023 della conferenza comprendeva temi molto vari:

- metodi di vigilanza in generale;
- utilizzo sproporzionato di dati accessibili pubblicamente da parte dei servizi di intelligence e misure da adottare al riguardo;
- uno scambio approfondito sulla recente giurisprudenza della Corte europea dei diritti dell'uomo;
- metodi di vigilanza tecnici;
- aspetti della comunicazione da parte delle autorità di vigilanza.

L'AVI-AIn ha tratto beneficio anche dallo scambio a livello personale sui metodi di vigilanza e sul contesto legislativo con i vari partecipanti presenti alla riunione.

International Intelligence Oversight Forum (IIOF), 28 e 29 novembre 2023, Washington DC

Il 28 e 29 novembre 2022 si è tenuto il sesto «International Intelligence Oversight Forum (IIOF)» presso l'*American University Washington College of Law* di Washington. Il capo dell'AVI-AIn e un collaboratore vi hanno partecipato insieme a numerosi membri di varie autorità di vigilanza (amministrative e parlamentari) nel campo dell'intelligence, ma anche a rappresentanti di servizi di intelligence, autorità competenti in materia di protezione dei dati e ONG.

Sono stati trattati i temi seguenti:

- vigilanza necessaria e proporzionata: proteggere la vita privata e la sicurezza nazionale sulle due sponde dell'Atlantico;
- dichiarazione dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) del 14 dicembre 2022 sull'accesso da parte dei poteri pubblici ai dati personali detenuti da entità del settore privato: che cosa significa e cosa succederà in seguito?
- condivisione di buone pratiche sul modo di integrare le opportune garanzie nelle operazioni condotte dai servizi di intelligence;
- sfide simili, contesti diversi: analisi comparativa del modo in cui i Paesi disciplinano le proprie attività di intelligence;
- articolo 11 della Convenzione 108+ del Consiglio d'Europa: stato di avanzamento dei lavori, sfide e insegnamenti tratti.

Dopo le varie presentazioni e i successivi dibattiti si è tenuta una visita all'*Intelligence Community Campus* di Bethesda, con discussione in merito alle risorse messe a disposizione dei vari servizi di intelligence americani per assicurare un equilibrio costante e conforme alla legge dei vari interessi in gioco, tra sicurezza nazionale e diritti fondamentali dei cittadini.

I temi trattati e gli scambi avvenuti sono stati realmente utili per l'attività di vigilanza dell'AVI-AIn. Inoltre, si è constatato che le autorità di vigilanza possono imparare dagli ambienti della ricerca (università, ONG ecc.), i quali gettano uno sguardo critico e spesso costruttivo sul ruolo della vigilanza. Il confronto con i vari modi di esercitare la vigilanza, risultanti da contesti legali e/o culture diversi, nonché con i vincoli e le sfide che si pongono nel campo delle attività di vigilanza, consentono all'AVI-AIn di riflettere sulle sue pratiche, di svilupparle e di migliorarle.

8 Allegato

8.1 Piano di controllo 2023

N.	Titolo	Organo verificato
Strategia e pianificazione		
23-1	Produzione ed effetti dei prodotti informativi del Servizio delle attività informative della Confederazione (SIC)	SIC
Organizzazione		
23-2	Servizi giuridici nel SIC	SIC
23-3	Protezione e sicurezza nel SIC	SIC
23-4	Business Continuity Management dell'informatica (IT) e Disaster Recovery-IT nel SIC	SIC
Collaborazione		
23-5	Servizio informazioni cantonale (SICant) Lucerna	SICant / SIC
23-6	SICant Nidvaldo	SICant / SIC
23-7	SICant Obvaldo	SICant / SIC
23-8	SICant Uri	SICant / SIC
23-9	Elaborazione dei mandati sui sensori tecnici nel Centro operazioni elettroniche (COE)	COE
23-10	Collaborazione del SIC con privati	SIC
Acquisizione di informazioni		
23-11	Operazioni, necessità di accertamenti operativi e misure di acquisizione soggette ad autorizzazione del SIC	SIC
23-12	Fonti umane (HUMINT) nel SIC	SIC
23-13	Impiego di agenti virtuali nel SIC	SIC
Risorse		
23-14	Attuazione delle raccomandazioni dell'AVI-Aln	SIC / SIM ⁴ / COE
Trattamento dei dati / archiviazione		
23-15	Attuazione del diritto d'accesso nel SIC	SIC
23-16	Sistemi d'informazione, sistemi di memorizzazione e memorie di dati al di fuori dell'articolo 47 della legge federale sulle attività informative	SIC

⁴ Servizio informazioni militare

8.2 Elenco delle abbreviazioni

ACE	Servizio delle attività ciber ed elettromagnetiche
ACI	Autorità di controllo indipendente per l'esplorazione radio e l'esplorazione dei segnali via cavo
AFS	Archivio federale svizzero
Art.	Articolo
AVI-AIn	Autorità di vigilanza indipendente sulle attività informative
BCM	Business Continuity Management
CAS	Certificate of Advanced Studies
CDF	Controllo federale delle finanze
COE	Centro operazioni elettroniche (fino al 31.12.2023)
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DeICG	Delegazione delle Commissioni della gestione
FSCD	Fornitori svizzeri di servizi di comunicazione derivati
GEVER	Gestione elettronica degli affari nell'Amministrazione federale
HUMINT	Human Intelligence, acquisizione di informazioni per mezzo di fonti umane
IFPDT	Incaricato federale della protezione dei dati e della trasparenza
IIOF	International Intelligence Oversight Forum
IOWG	Intelligence Oversight Working Group
ISACA	Information Systems Audit and Control Association
IT	Information Technology, tecnologia dell'informazione
ITSCM	IT Service continuity management
IVF	Identità virtuali fittizie
LAIn	Legge federale del 25 settembre 2015 sulle attività informative (LAIn; RS 121)
LPD	Legge federale del 25 settembre 2020 sulla protezione dei dati (LPD; RS 235.1)
LSCPT	Legge federale del 18 marzo 2016 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni
N-SIS	Parte nazionale del Sistema d'informazione di Schengen
OAIIn	Ordinanza del 16 agosto 2017 sulle attività informative (RS 121.1)
OSINT	«Open Source Intelligence», messa a disposizione di dati provenienti da fonti accessibili al pubblicoRS
segg.	e seguenti
SIC	Servizio delle attività informative della Confederazione
SICant	Servizi informazioni cantonali
SIM	Servizio informazioni militare della Confederazione
TAF	Tribunale amministrativo federale