



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Autorità di vigilanza indipendente sulle  
attività informative

# Rapporto di attività 2019

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



# 1. Sintesi

Per il 2019 l'AVI-AIn aveva previsto 21 verifiche<sup>1</sup>. Le verifiche 19-13 (Processo di reclutamento, di assistenza e di uscita), 19-15 (Esercizio, contenuto e utilizzo dei sistemi d'informazione GEVER SIC, memorizzazione dei file in BURAUT, memorizzazione dei file in SiLAN [valutazioni temporanee]) e 19-16 (Classificazioni di informazioni) riguardavano diversi servizi o sistemi e pertanto sono state suddivise in due o tre rapporti separati. Le verifiche 19-17 (Ambiente informativo SIM) e 19-21 (Accesso a/da sistemi d'informazione di terzi [Confederazione, Cantoni, servizi esteri, perseguimento penale]) non hanno potuto essere avviate a causa di altre attività prioritarie. La verifica 19-19 è stata avviata poco prima della fine di dicembre 2019 e pertanto nel presente rapporto non è possibile riferire al riguardo.

Nel 2019 l'AVI-AIn ha iniziato a verificare la collaborazione del SIC con i Cantoni. Ha verificato i servizi informazioni cantonali (SICant) di Ginevra, Giura, Berna, Grigioni e Sciaffusa. I SICant, che in quasi tutti i Cantoni sono integrati nei corpi di polizia cantonali, sono finanziati principalmente con mezzi della Confederazione. Le prestazioni fornite dai Cantoni nel 2019 corrispondevano complessivamente a un volume di 124 posti a tempo pieno. L'AVI-AIn ha sviluppato a tal fine una verifica standard ed emesso diverse raccomandazioni, soprattutto di ordine organizzativo.

L'AVI-AIn ha condotto 5 verifiche nel campo delle misure di acquisizione soggette ad autorizzazione e delle operazioni e 4 verifiche in quello del trattamento dei dati e dell'archiviazione.

Rispetto al numero totale di abitanti della Svizzera, il numero di persone toccate da misure di acquisizione soggette ad autorizzazione è insignificante<sup>2</sup>. L'AVI-AIn ritiene che questo strumento, il più invasivo a disposizione del SIC, venga utilizzato nel rispetto del principio di proporzionalità. Con queste

misure il SIC esercita una profonda ingerenza nei diritti fondamentali delle persone interessate; pertanto, la tendenziale prudenza nel suo utilizzo è da considerarsi adeguata. Di conseguenza l'AVI-AIn seguirà attentamente i futuri sviluppi in questo campo.

Per il SIC, l'AVI-AIn intravede un potenziale di miglioramento soprattutto per quanto riguarda il trattamento dei dati. Il SIC deve poter spiegare in modo trasparente i motivi per cui registra e gestisce certe informazioni su certe persone nelle proprie banche dati e di quali informazioni si tratta. È anche lecito porre esigenze elevate circa l'ordine adottato per la registrazione di queste informazioni e circa il disciplinamento della loro cancellazione: sotto questo aspetto il SIC può fare meglio. Le riflessioni necessarie a tal fine sono complesse, anche e soprattutto dal punto di vista tecnico. Occorre inoltre considerare che un servizio informazioni deve fornire delle previsioni. Uno dei principi importanti delle attività informative detta di immaginare l'impossibile e di dedurre degli scenari. Spesso oggi non si sa quali basi occorran domani per l'estrapolazione di questi scenari.

Gli organi controllati sono tenuti a garantire la trasparenza nei confronti delle autorità di vigilanza. Queste ultime hanno diritto di accedere a documenti, processi e locali che non solo non sono pubblici, ma in parte sono addirittura deliberatamente resi inaccessibili al pubblico. Gli organi controllati hanno sempre garantito all'AVI-AIn questo diritto di accesso e visione, in qualsiasi situazione.

L'AVI-AIn ha emesso numerose raccomandazioni nell'ambito dell'organizzazione, delle strutture e dei processi del SIC. Secondo l'articolo 78 capoverso 7 LAln<sup>3</sup>, il Dipartimento federale della difesa, dalla protezione della popolazione e dello sport (DDPS) provvede all'attuazione delle raccomandazioni. Pertanto ordina al SIC, al SIM e al COE di attuare le raccoman-

dazioni emesse dall'autorità di vigilanza. Per quanto riguarda le indicazioni emesse, il DDPS esige di norma che l'organo controllato ne tenga conto anche quando non sono vincolanti. L'AVI-AIn ha emesso 63 raccomandazioni e 40 indicazioni. L'attuazione delle raccomandazioni consente di ridurre ulteriormente i rischi esistenti e di incrementare l'efficienza. Considerata la struttura del personale del SIC, questa è una delle preoccupazioni principali dell'AVI-AIn.

I due settori militari delle attività informative, ossia il COE e il SIM, hanno competenze più ristrette. I due servizi informazioni militari dipendono in un certo qual modo dal SIC. Entrambi i servizi devono posizionarsi rispetto al SIC, colmare le nicchie in modo ottimale e sfruttare e ottimizzare le sinergie.

Accanto alle attività di controllo, l'AVI-AIn ha dedicato del tempo a guardare oltre l'orizzonte settoriale nell'ambiente nazionale e internazionale e a concentrarsi di nuovo sul suo compito fondamentale, a trasferire conoscenze e a sviluppare ulteriormente la collaborazione con i nostri partner e destinatari.

Il rapporto di attività<sup>4</sup> è stato presentato per consultazione al DDPS e alla Delegazione delle Commissioni della gestione DelCG dal 13 al 23 gennaio 2020. 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.



<sup>1</sup> I piani di controllo sono pubblicati in Internet sul sito [www.ab-nd.admin.ch](http://www.ab-nd.admin.ch).

<sup>2</sup> Nel 2018 queste misure hanno interessato 28 persone, cfr. anche il rapporto del SIC sulla situazione «La sicurezza della Svizzera 2018»

<sup>3</sup> RS 121

<sup>4</sup> esclusi i capitoli 3 e 8

## 2. Contenuto

<b>1. Sintesi</b>	<b>2</b>
<b>2. Contenuto</b>	<b>4</b>
<b>3. Nota personale</b>	<b>5</b>
<b>4. Trasparenza e tutela del segreto</b>	<b>6</b>
4.1 Quanta trasparenza occorre nei confronti dell'opinione pubblica?	6
4.2 Domande LTras sui rapporti	10
<b>5. Attività di vigilanza</b>	<b>12</b>
5.1 Piano di controllo	12
5.2 Verifiche del 2019	13
5.2.1 Strategia e pianificazione	13
5.2.2 Organizzazione	14
5.2.3 Collaborazione	14
5.2.4 Misure di acquisizione soggette ad autorizzazione	17
5.2.5 Operazioni	19
5.2.6 Risorse	21
5.2.7 Trattamento dei dati / archiviazione	23
5.3 Consenso	28
5.4 Controlling di raccomandazioni e indicazioni	28
<b>6. Vista interna</b>	<b>29</b>
6.1 Revisione della LAIn	29
6.2 Formazione continua dei collaboratori dell'AVI-AIn	29
<b>7. Coordinamento</b>	<b>31</b>
7.1 Contatti nazionali	31
7.2 Contatti internazionali	31
<b>8. Vista esterna</b>	<b>33</b>
<b>9. Cifre al 31 dicembre 2019</b>	<b>36</b>
<b>10. Allegato</b>	<b>37</b>
10.1 Piano di controllo 2019	37
10.2 Elenco delle abbreviazioni	38

## 3. Nota personale



Thomas Fritschi, capo AVI-AIn

«Svizzeri arrestati all'estero come terroristi, crescita dell'estremismo di destra, raccolta ossessiva di informazioni e schedature da parte del SIC, sorveglianza sistematica, ciberrattacchi, reduci della jihad e sospetti terroristi, spie russe, intelligence buona soltanto quando tutto va bene: ecco alcuni dei temi a cui hanno accennato i media nei contributi dedicati alle attività informative nell'anno in rassegna. Ve ne ricordate ancora?»

Dovreste ricordare bene o male qualche titolo, a seconda delle vostre preoccupazioni e dei vostri interessi. Personalmente ricordo un giornalista che dopo la conferenza stampa sul rapporto di attività dell'anno scorso aveva detto con aria delusa che l'autorità di vigilanza non era riuscita a presentare nessun

rale è promotore del sito Öffentlichkeitsgesetz.ch, gestito da un'associazione indipendente. L'obiettivo consiste nell'imporre la legge sulla trasparenza in Svizzera come strumento incisivo a disposizione dei giornalisti. Dalla pagina 33 illustra il suo modo di vedere le cose.

Nel novembre 2019 cadeva il 30° anniversario dello scandalo delle schedature. All'epoca avevo vent'anni, il muro di Berlino era appena crollato, un indirizzo e-mail non l'avevo ancora, e tantomeno uno smartphone. Dal punto di vista delle attività informative, da allora la situazione è radicalmente cambiata, e così l'organizzazione e le basi legali dei servizi informazioni. Tecnicamente oggi abbiamo in generale ben altre possibilità per il trattamento dei dati. La piena digitalizzazione pone sfide enormi alla nostra società. In tale contesto, un servizio di intelligence è chiamato a fornire informazioni chiave per l'individuazione tempestiva dei pericoli, a essere più rapido e attendibile dei media e a evitare al tempo stesso di raccogliere informazioni false o in quantità eccessiva. Un compito indubbiamente molto impegnativo.

Noi abbiamo seguito l'adempimento di questo compito e constatato che molte attività sono state eseguite correttamente, ma che sono stati commessi anche errori. In certi casi sono stati conservati troppo a lungo troppi dati, oppure sono stati scritti rapporti poco meticolosi. Crediamo anche che adeguando l'organizzazione e migliorando i processi l'efficienza dei servizi di intelligence possa essere ulteriormente incrementata.

Con il nostro lavoro vogliamo in futuro contribuire a eliminare o quantomeno minimizzare i rischi legati alle attività di intelligence, e contemporaneamente garantire il rispetto e la realizzazione dei diritti fondamentali delle persone che vivono in Svizzera. Buona lettura!»

Thomas Fritschi, capo AVI-AIn

### «La trasparenza è il filo conduttore del presente rapporto di attività.»

Thomas Fritschi

vero scandalo nel campo delle attività informative e ovviamente lo vede come un indicatore per il nostro lavoro. A me sembra piuttosto vero il contrario. Meno scandali ci sono, migliore è la supervisione.

Nel 2019 abbiamo effettuato 19 verifiche in loco presso i servizi informazioni. Abbiamo effettuato 119 interviste con i collaboratori e avuto libero accesso alle banche dati del SIC. In tutto e per tutto, abbiamo avuto e abbiamo tuttora un'immagine trasparente delle attività informative. E condividiamo volentieri una parte di questa trasparenza. Il rapporto di attività è una delle possibilità che permettono di meglio spiegare il contesto delle attività informative, e pertanto il tema della trasparenza costituisce il filo conduttore del presente rapporto.

Quest'anno il punto di vista esterno sarà presentato da Martin Stoll. Il corrispondente della Sonntagszeitung a Palazzo fede-

## 4. Trasparenza e tutela del segreto

Per la realizzazione della nostra visione «Noi rafforziamo la fiducia», è estremamente importante che l'AVI-AIn riferisca in modo trasparente al capo del DDPS, ai servizi delle attività informative e alla popolazione svizzera. Quest'ultima è una sfida particolare, ed è per questo che abbiamo voluto evidenziare alcuni fattori nel testo che segue.

### 4.1 Quanta trasparenza occorre nei confronti dell'opinione pubblica?

Per l'AVI-AIn, la rivelazione di aspetti relativi alle attività informative è un costante gioco di equilibrio. Da un lato, i principi applicabili alle attività di intelligence, quali il principio del «need to know», ossia della necessità di «limitare l'accesso alle sole informazioni strettamente necessarie», richiedono un alto grado di segretezza e riservatezza. D'altro lato, la divulgazione di conoscenze sulle attività informative può favorire la comprensione della popolazione nei confronti di questo tipo di attività. Comunque sia, in quanto cittadini tendiamo a diventare diffidenti quando ci vengono negate certe informazioni e non possiamo capire l'agire dello Stato, nel nostro caso l'attività di intelligence.

I servizi informazioni sono tenuti a tenere segrete le informazioni sensibili su attori che minacciano la sicurezza interna della Svizzera. Le strategie di protezione e i metodi usati devono essere tenuti nascosti agli avversari. Essi rappresentano la nostra «prima linea di difesa» («first line of defense») per la sicurezza della Svizzera. Perciò, le spie di Paesi stranieri, i potenziali terroristi, i trafficanti di armi nucleari e gli estremisti violenti devono sapere il meno possibile sul lavoro dei servizi informazioni.

Per essere un partner affidabile nella comunità internazionale dell'intelligence e poter accedere a informazioni segrete, deve dimostrarsi degno di fiducia e quindi nascondere al pubblico per quanto possibile le proprie attività e strategie. Se

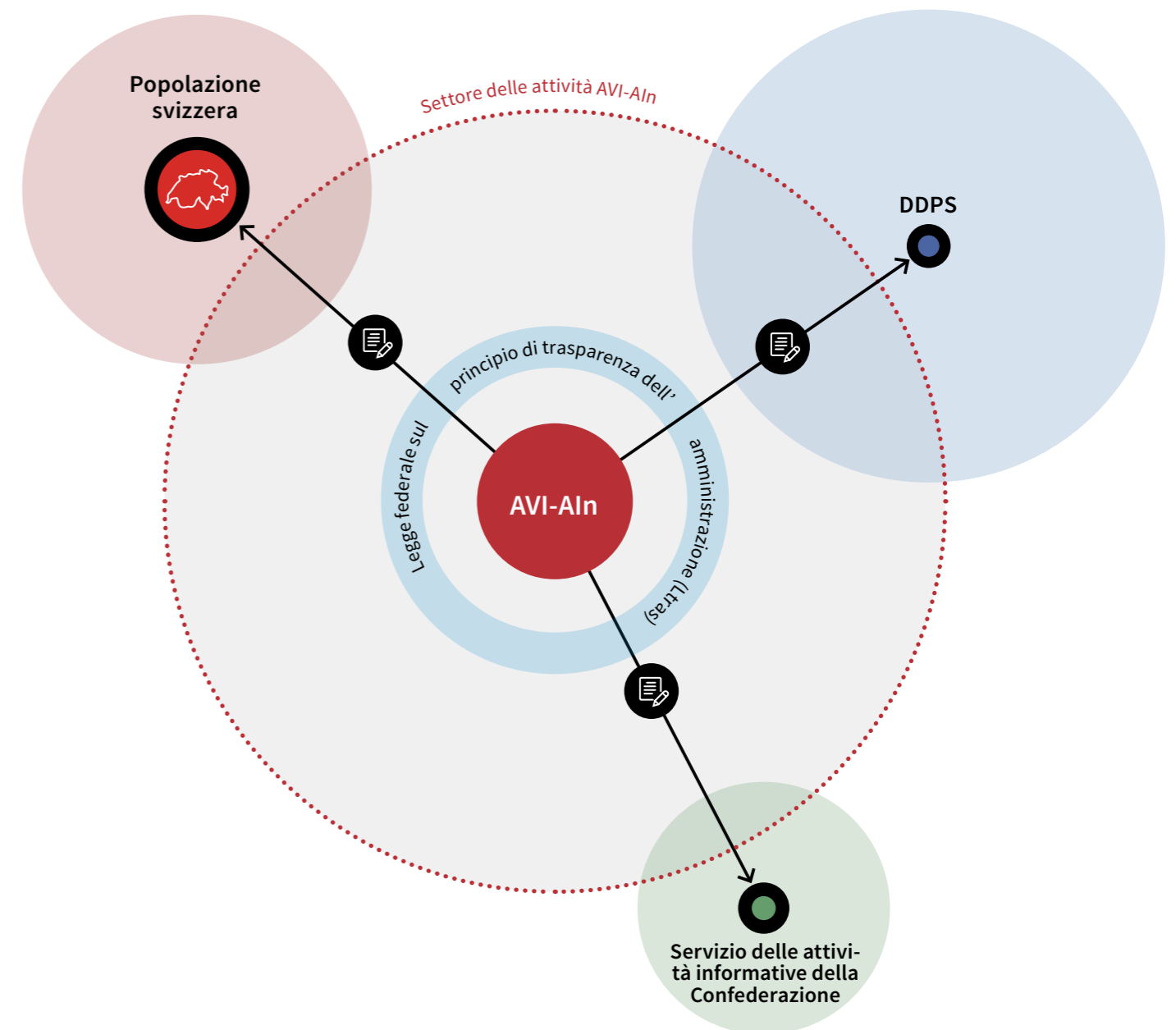
queste informazioni finiscono sulle cronache perché i principi di segretezza sono stati violati, i servizi partner possono decidere di escludere i servizi segreti in questione dallo scambio di informazioni rilevanti per la sicurezza. Un simile risultato creerebbe a sua volta dei rischi per la sicurezza interna della Svizzera. Questo è quanto accaduto ad esempio l'anno scorso al servizio informazioni interno austriaco, che in seguito al sequestro di numerosi supporti di dati ha vissuto una pesante perdita di credibilità negli ambienti internazionali dei servizi di intelligence, e da allora lotta per riabilitarsi.<sup>5</sup>

I servizi informazioni, e ancor più i servizi segreti, suscitano molta diffidenza in alcune fasce della popolazione, o addirittura vengono contestati. I troppi esempi negativi che troviamo nelle pagine della storia, e le loro conseguenze dolorose e catastrofiche per etnie, dissidenti politici o in genere per le minoranze, spiegano questo atteggiamento. Le attività segrete di questi servizi possono rafforzare i pregiudizi esistenti.

Il lavoro di un servizio informazioni consiste principalmente nella raccolta e nella valutazione delle informazioni. Tuttavia, le disposizioni di legge devono essere rigorosamente rispettate. In Svizzera, le notizie apparse l'anno scorso sulla raccolta selvaggia di informazioni, le operazioni di schedatura e il presunto spionaggio ai danni di personaggi politici hanno dato un'immagine negativa dell'operato del SIC, facendo affiorare il ricordo dello scandalo delle schedature e dell'epoca in cui ampie fasce della popolazione venivano segretamente

<sup>5</sup> Quotidiano «Neue Zürcher Zeitung», edizione del 10 aprile 2019: «Ist Österreichs Geheimdienst noch vertrauenswürdig?»

### Rapporti trasparenti



«Le strategie di protezione e i metodi usati devono essere tenuti nascosti agli avversari.»

«Rapporti per quanto possibile trasparenti possono rendere più limpidi e comprensibili le attività dei servizi informazioni.»



sorvegliate. Rispondendo alle richieste di accesso, il SIC fornisce un contributo essenziale alla trasparenza del servizio nei riguardi dell'opinione pubblica. Attualmente vengono consacrate molte risorse per rispondere alle numerose richieste di informazione.

In virtù del mandato di verifica impartito dalla legge, l'AVI-AIn conosce in dettaglio le attività dei servizi informazioni svizzeri, i quali sono tenuti a essere trasparenti nei suoi confronti. Nell'ambito delle attività di verifica correnti, questa trasparenza è stata generalmente garantita. Tutt'altra questione è invece quella di sapere in che misura l'AVI-AIn possa informare il pubblico a tale riguardo. Ogni tanto si ha la sensazione che l'uno o l'altro fatto riguardante le attività di intelligence potrebbe essere rivelato al vasto pubblico facilmente senza compromettere tangibilmente la sicurezza. Simili rivelazioni favorirebbero la comprensione e in definitiva la fiducia della popolazione svizzera nei confronti delle attività informative e dei collaboratori dei servizi informazioni.

È vero, ad esempio, che i nomi delle persone politicamente attive sono registrati nelle banche dati del SIC. In genere, tuttavia, tali nomi sono stati tratti da fonti pubbliche, ad esempio dai media. Naturalmente, anche sotto questo aspetto le norme di legge vanno rispettate. Le informazioni sulle attività politiche, ad esempio, possono essere acquisite e trattate solo in casi eccezionali, quando esistono concreti indizi che i diritti politici vengono esercitati per preparare o svolgere attività terroristiche, di spionaggio o di estremismo violento. L'anno scorso l'AVI-AIn ha effettuato controlli a campione sul trattamento delle informazioni concernenti i personaggi politici nel sistema di gestione delle pratiche del SIC, e nel presente rapporto riferisce in merito alle constatazioni effettuate e alle raccomandazioni emesse.<sup>6</sup>

Ma oltre che con gli atti di verifica e i relativi rapporti, l'AVI-AIn contribuisce all'informazione del pubblico sulle attività informative anche con altri mezzi. Le sue attività rientrano nel campo d'applicazione della legge federale del 17 dicem-

bre 2004 sul principio di trasparenza dell'amministrazione (Legge sulla trasparenza, LTras)<sup>7</sup>. La LTras ha lo scopo di promuovere la trasparenza sulle attribuzioni, l'organizzazione e l'attività dell'amministrazione, ossia, nel caso nostro, la vigilanza sui servizi informazioni. L'AVI-AIn ne è consapevole e assume questo mandato di legge con serietà. Si è dunque occupata con serietà di due domande di accesso fondate sulla LTras, e nel presente rapporto riferisce in merito alle esperienze acquisite.<sup>8</sup>

Infine, promuove la trasparenza anche la pubblicazione annuale del nostro rapporto di attività. Secondo la legge, l'AVI-AIn presenta il proprio rapporto al DDPS. Il rapporto viene in seguito messo a disposizione del pubblico. Anche se in esso vengono materialmente rispettate le prescrizioni sulla segretezza, l'intenzione è comunque quella di informare la popolazione in modo comprensibile circa le attività dei servizi informazioni. L'AVI-AIn può riferire in particolare in merito ai motivi che hanno giustificato l'avvio delle verifiche e sulle metodologie adottate. Le spiegazioni relative alle attività di intelligence e al gergo utilizzato sono intese a promuovere ulteriormente la comprensione e la chiarezza.

L'AVI-AIn è persuasa che un rapporto per quanto possibile trasparente possa rendere più limpido e comprensibile il campo d'azione dei servizi informazioni. Si tratta certo di un compito impegnativo, poiché gli interessi di segretezza che vi si oppongono devono essere accuratamente soppesati, al fine di garantire la sicurezza della Svizzera.

Una particolare difficoltà nel garantire la trasparenza consiste nel rispetto delle norme della LTras. Pertanto, l'AVI-AIn riferisce nelle pagine che seguono sulle prime esperienze da essa acquisite a questo riguardo.

<sup>6</sup> Rapporto di verifica 19-15

<sup>7</sup> RS 152.3

<sup>8</sup> vedi pagina 10

## «Una sfida particolare consiste nel rispettare i requisiti della legge sulla trasparenza.»

### 4.2 Domande LTras sui rapporti di verifica 18-9 e 18-11

Dopo la conferenza stampa sul suo primo rapporto di attività, l'AVI-AIn ha ricevuto due domande di accesso fondate sulla LTras. La LTras ha lo scopo di promuovere la trasparenza sulle attribuzioni, l'organizzazione e l'attività dell'amministrazione, e quindi di far luce su schedari e archivi. Le domande, inoltre da un quotidiano svizzero, riguardavano i rapporti di verifica 18-9 (Verifica dei selettori<sup>9</sup> nel sistema) e 18-11 (Panoramica sulle misure di riduzione dei rischi presso il SIM).

Il disegno di LAIn prevedeva l'esclusione dell'intero spettro di attività del SIC dal campo di applicazione della LTras. L'incaricato federale della protezione dei dati e della trasparenza (IFPDT), in quanto tutore del principio di trasparenza, si era allora opposto a tale esclusione. In definitiva è rimasto escluso dal campo d'applicazione della LTras, in virtù dell'articolo 67 LAIn, soltanto il settore più sensibile, ossia quello dell'acquisizione di informazioni.

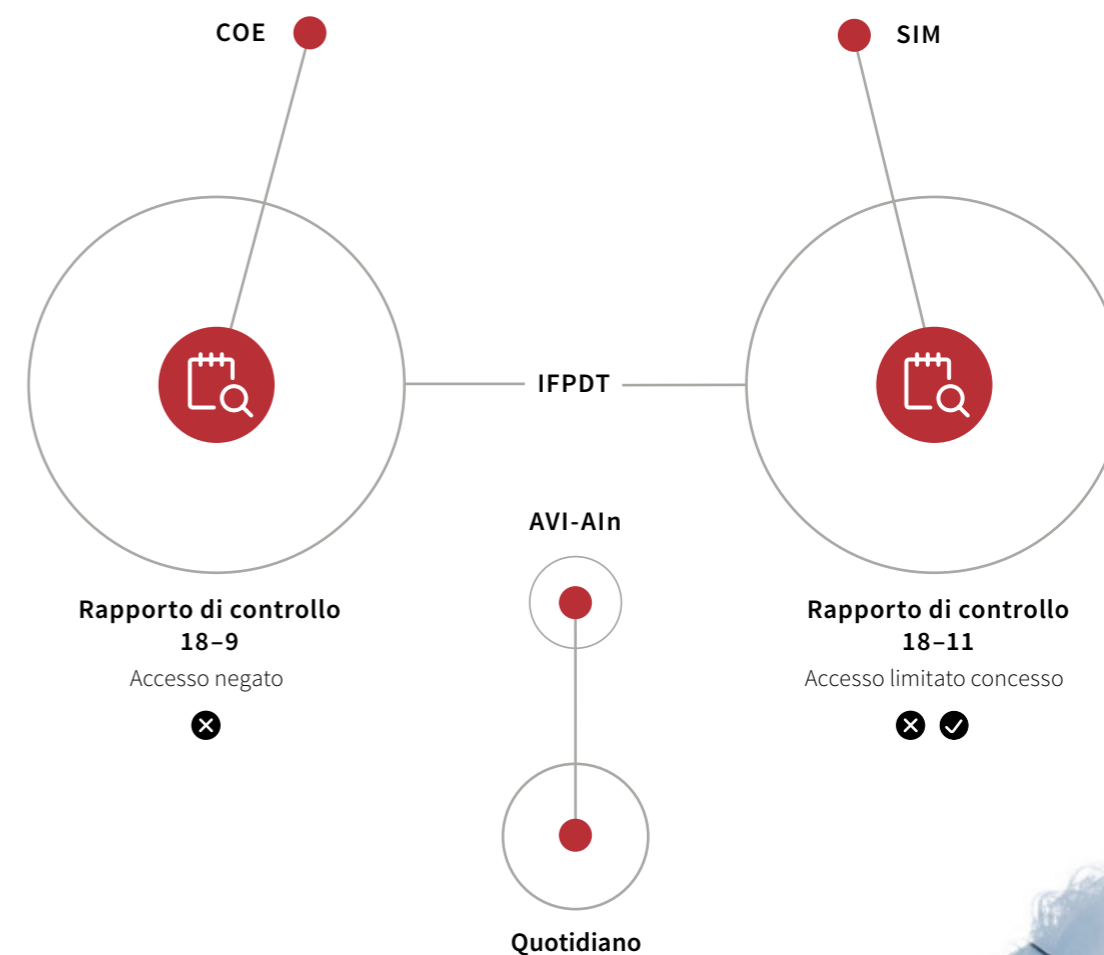
Il rapporto di verifica 18-9 riguarda la produzione, il controllo e l'eventuale adeguamento dei selettori che servono al COE per gestire le proprie attività di acquisizione delle informazioni. L'AVI-AIn ha pertanto ritenuto che l'accesso a questo rapporto di verifica dovesse essere negato in virtù dell'articolo 67 LAIn. Tale decisione non è stata contestata.

L'AVI-AIn ha invece deciso diversamente riguardo al rapporto di verifica 18-11. Secondo la LTras, l'accesso a documenti ufficiali può essere limitato anche se rischia di compromettere ad esempio la pubblica sicurezza. Le informazioni sull'organizzazione, l'attività o le strategie di autorità che svolgono compiti di sicurezza, come nel caso specifico il SIM, possono essere oggetto di questa restrizione. Secondo l'AVI-AIn, tuttavia, non tutti i contenuti del suddetto rapporto di verifica erano atti, se rivelati, a compromettere la pubblica sicurezza. Essa ha pertanto deciso di concedere, anche se in modo limitato, l'accesso al rapporto annerendone alcune parti e informazioni.

Dato che il rapporto riguardava soprattutto il SIM come organo controllato, l'AVI-AIn ha invitato tale servizio a emettere un preavviso. Il SIM si è detto contrario in toto alla divulgazione del rapporto di verifica. Richiamandosi alla classificazione, ha sostenuto che la pubblicazione di un rapporto parzialmente annerito avrebbe considerevolmente ostacolato l'adempimento dei suoi compiti. I vertici dell'esercito hanno confermato questa posizione.

L'AVI-AIn ha considerato il problema come una questione di principio e, avendo interesse a chiarire questa divergenza dal punto di vista giuridico, ha seguito l'argomentazione del SIM e negato l'accesso al rapporto di verifica 18-11. Il quotidiano in questione ha contestato tale decisione inoltrando all'IFPDT una domanda di mediazione. La procedura intesa per quanto possibile a trovare un'intesa tra le parti, nello specifico tra l'AVI-AIn e il SIM da un lato e il quotidiano interessato dall'altro. Durante l'udienza dinanzi all'IFPDT le parti si sono accordate sulla concessione dell'accesso a gran parte del rapporto.

L'esito dell'udienza di mediazione ha confermato l'approccio dell'AVI-AIn, consistente nel promuovere la comprensione e la fiducia garantendo la trasparenza a ogni occasione nella misura di quanto possibile e lecito.



<sup>9</sup> Rapporto di attività 2018, pag. 17

## 5. Attività di vigilanza



### 5.1 Piano di controllo

L'AVI-Aln prepara un piano di controllo annuale basato sui rischi che funge anche da strumento di pianificazione per l'adempimento dei suoi compiti. A questo scopo analizza gli oggetti figuranti nel repertorio dei temi sottoposti a verifica e li pondera in base alla probabilità che i rischi si realizzino e alle relative ripercussioni. Il piano di controllo 2019 prevedeva verifiche in ciascuno dei seguenti ambiti:

- strategia e pianificazione;
- organizzazione;
- collaborazione;
- misure di acquisizione soggette ad autorizzazione;
- operazioni;
- risorse;
- trattamento dei dati e archiviazione.

Il piano di controllo 2019 è stato elaborato tra settembre e dicembre 2018. Nello stesso periodo l'allora capo del DDPS e le autorità sottoposte a vigilanza hanno potuto esprimersi in merito alla bozza elaborata. Il piano di controllo definitivo è stato trasmesso per conoscenza anche ad altri organi di vigilanza in materia di attività informative.

«Con quattro operazioni e 170 misure di acquisizione soggette ad autorizzazione, la lotta allo spionaggio è una delle principali attività del SIC.»

### 5.2 Verifiche del 2019

Per il 2019 erano previste in tutto 21 verifiche. In seguito alla suddivisione delle verifiche 19-13, 19-15 e 19-16 in due o tre parti separate, sono stati allestiti 7 rapporti. Per varie ragioni, e a causa della continua ridefinizione delle priorità, le verifiche 19-17 «Ambiente informativo SIM» e 19-21 «Accesso a/da sistemi d'informazione di terzi (Confederazione, Cantoni, servizi esteri, perseguimento penale)» non sono state avviate. Esse sono state posticipate e saranno inserite in piani di controllo futuri. La verifica 19-19 «Strumenti per l'analisi di dati al COE» è stata avviata poco prima della fine di dicembre 2019 e pertanto nel presente rapporto non è possibile riferire al riguardo. L'anno 2019 ha segnato anche l'inizio delle verifiche presso i Cantoni. L'AVI-Aln ha verificato la collaborazione tra il SIC e cinque SICant.

Inoltre ha proceduto ad accertamenti interni senza dover far capo agli organi controllati. Le verifiche condotte nel 2019 sono illustrate qui di seguito, suddivise in base agli ambiti del piano di controllo.

#### → Spionaggio

Per spionaggio si intende l'insieme degli atti volti all'acquisizione di informazioni protette o segrete a profitto di uno Stato estero o di un'impresa estera. I servizi di controspionaggio di un Paese hanno il compito di scoprire le attività di spionaggio e possibilmente di impedire che ne vengano svolte altre.

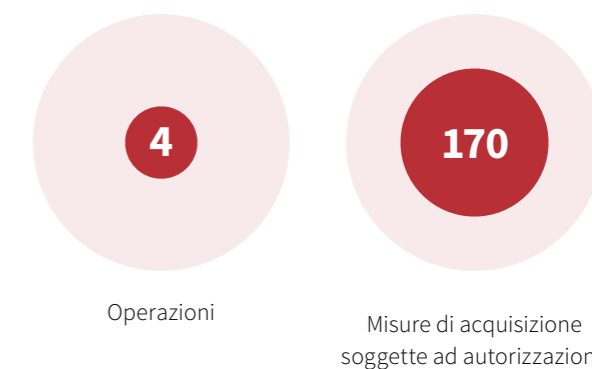
### 5.2.1 Strategia e pianificazione

#### 19-1 Strategia di difesa dallo spionaggio

Il rapporto del SIC sulla situazione «La sicurezza della Svizzera 2019» evidenzia che il nostro Paese è confrontato con persistenti attività di spionaggio aggressive, condotte da alcuni Stati. Con quattro operazioni e 170 misure di acquisizione soggette ad autorizzazione, il controspionaggio si attesta come una delle attività principali del SIC. Pertanto, l'AVI-Aln aveva motivo sufficiente per analizzare le riflessioni strategiche e le conseguenti misure in materia di controspionaggio.

Dall'analisi effettuata è risultato che il SIC considera come uno dei suoi compiti principali quello di chiarire le minacce derivanti dalle attività di spionaggio e dalle attività di intelligence importune svolte in Svizzera. Nell'attuare misure vere e proprie di controspionaggio, il SIC dipende largamente dai decisori politici. Sulle questioni strategiche di questo tipo, si focalizza pertanto sulla collaborazione con altre autorità e sugli aspetti metodologici e organizzativi. L'AVI-Aln ha ritenuto che le misure già adottate fossero efficaci e ha raccomandato di rafforzare ulteriormente la formulazione di altri aspetti strategici.

#### Controspionaggio 2019



## 5.2.2 Organizzazione

### 19-2 Gestione delle informazioni d'intelligence tra il sensore «addetto alla difesa» e il SIC

L'AVI-AIn si è interessata alla gestione e al coordinamento delle fonti d'informazione all'estero. Il SIC è responsabile dell'acquisizione di informazioni di intelligence da parte della rete di sensori rappresentata dagli addetti alla difesa. La collaborazione tra il SIC e l'esercito ai sensi dell'articolo 11 capoverso 2 LAIn non è ulteriormente concretizzata. La gestione di addetti alla difesa tra le varie organizzazioni è in parte documentata. La gestione adeguata delle missioni informative degli addetti da parte del SIC riveste un'importanza determinante e deve essere rafforzata per incrementarne l'efficacia. Il valore aggiunto informativo prodotto dagli addetti alla difesa deve essere consolidato.

## 5.2.3 Collaborazione

I servizi informazioni cantonali (SICant) sono i servizi designati di ciascun Cantone che collaborano con il SIC per l'esecuzione della LAIn. Essi acquisiscono e trattano, di propria iniziativa o su incarico del SIC, informazioni sul terrorismo, sullo

spionaggio, sulla proliferazione, sulle infrastrutture critiche e sull'estremismo violento. Sono per così dire occhi ed orecchi del SIC a livello cantonale. Questi sensori, integrati nei corpi cantonali di polizia, sono finanziati in larga parte dalla Confederazione. Le risorse finanziarie sono concesse in base a una chiave di riparto che viene rivista ogni tre anni. Le prestazioni fornite dai Cantoni nel 2019 corrispondevano complessivamente a 124 posti a tempo pieno.

Le facoltà di vigilanza dell'AVI-AIn comprendono sia le attività del SIC sia quelle dei SICant. Nel pianificare le ispezioni, era chiaro all'AVI-AIn che occorreva includere l'esame della legalità, adeguatezza ed efficienza della collaborazione tra questi due attori. Nel 2018 essa si è dunque prefissa di effettuare una verifica di tutti i 26 SICant entro il quinquennio successivo. A tale scopo è stata sviluppata una verifica standard riguardante l'organizzazione, la gestione, la legalità, il trattamento dei dati, la sicurezza e l'impiego delle risorse, in modo tale da consentire anche un confronto tra i Cantoni. Oltre alla verifica dei documenti rilevanti, le attività di controllo comprendono anche un sondaggio annuale tra collaboratori del SIC, nell'ambito del quale viene verificata la collaborazione con i servizi cantonali controllati. L'AVI-AIn si reca presso i Cantoni per un colloquio approfondito al quale viene invitata l'autorità di vigilanza cantonale. In caso di necessità si tengono anche altre riunioni.

### → Addetti alla difesa

Gli addetti alla difesa intessono una rete di contatti a prova di crisi e indipendente da qualsiasi alleanza, conforme alle esigenze della politica di sicurezza svizzera e dell'esercito. Utilizzano questa rete e la trasformano in uno strumento efficiente e performante.

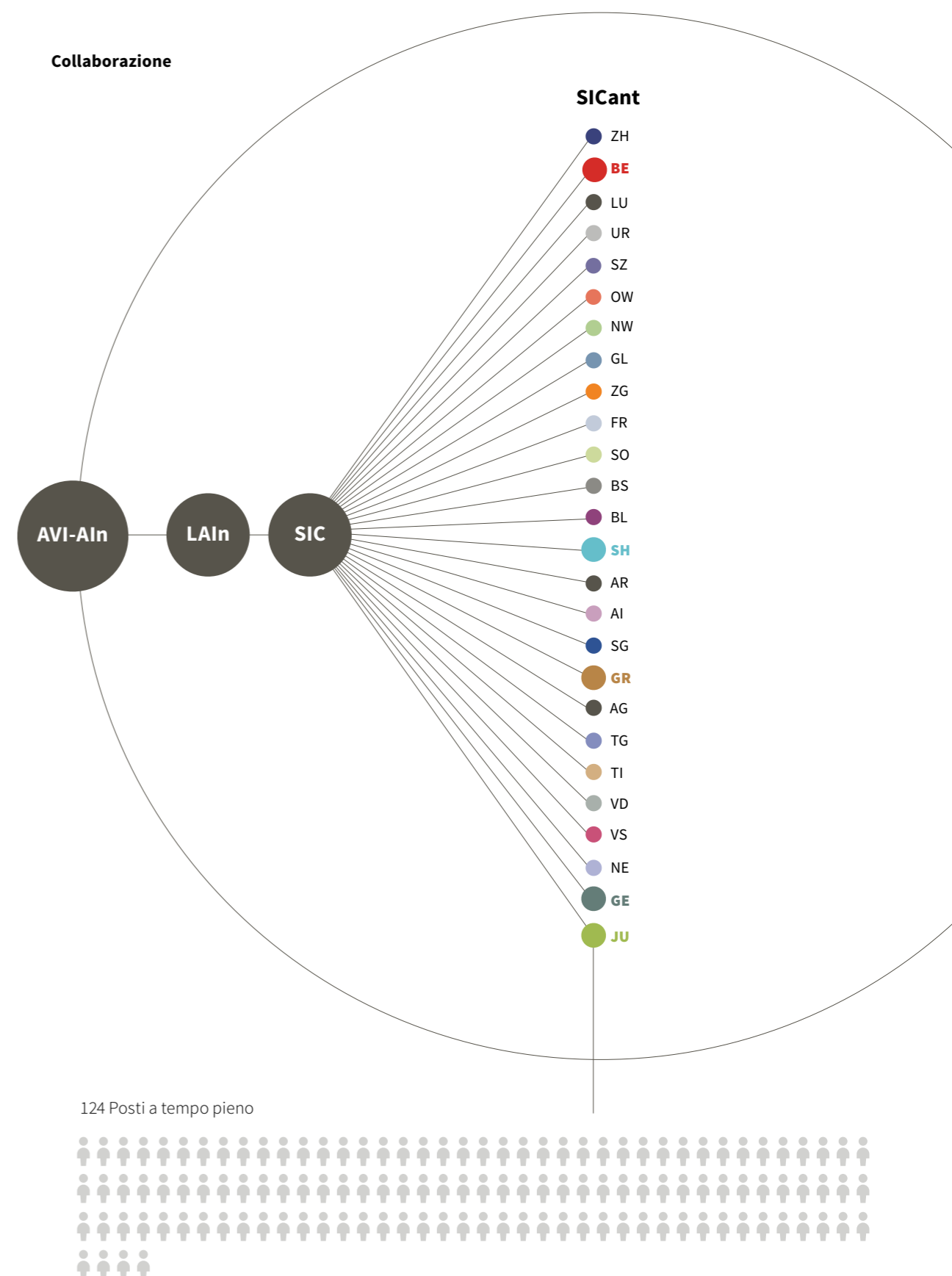
Al 12 agosto 2019, la rete degli addetti alla difesa svizzeri comprendeva 19 accreditamenti principali e 39 accreditamenti secondari<sup>10</sup>, tre dei quali inattivi a causa di conflitti (Yemen, Siria e Libia). Tale dispositivo è periodicamente sottoposto a verifica.

I compiti degli addetti alla difesa sono stati definiti dal Consiglio federale nel quadro della Convenzione di Vienna.

Gli addetti alla difesa sono incorporati nell'Esercito svizzero. Essi ricevono incarichi definiti da vari attori e trasmessi centralmente dal SIC. La loro gestione compete al settore Relazioni internazionali Difesa in seno allo Stato maggiore dell'esercito. La gestione a livello di attività informative è assicurata dal SIC.

Essi seguono una formazione speciale di sei mesi impartita dall'esercito, dal SIC e da altre autorità, tra cui ad esempio la Segreteria di Stato della migrazione (SEM) o il Dipartimento federale degli affari esteri (DFAE).

<sup>10</sup> <https://www.vtg.admin.ch/de/aktuell/themen/internationale-beziehungen/einsatz.html>, non tradotto in italiano; ultima visita: 27.12.2019



### 19-3 Controllo SICant GE

La collaborazione tra il SICant del Cantone di Ginevra (SICant GE) e il SIC si è svolta in parte correttamente. Tuttavia il Cantone dovrebbe ancora adeguare determinati aspetti riguardanti il trattamento dei dati per conformarli alla LAIn, eventualmente in collaborazione con il SIC. Per quanto riguarda l'efficacia e l'adeguatezza è stato riscontrato un potenziale di miglioramento, in particolare nell'ambito della collaborazione operativa, dell'impiego delle risorse e dell'uso dei mezzi tecnici.

### 19-4 Controllo SICant JU

Dal controllo è emerso che la collaborazione tra il SICant del Cantone del Giura (SICant JU) e il SIC si è svolta correttamente. Dopo aver constatato che negli ultimi anni il servizio cantonale in questione aveva raramente acquisito informazioni di propria iniziativa, l'AVI-Aln ha richiamato quest'obbligo e le responsabilità a esso legate. Il controllo dell'adeguatezza e dell'efficacia ha inoltre evidenziato che la politica del SIC in materia di feedback si era rivelata insufficiente. L'AVI-Aln ha dunque raccomandato al SIC di fornire ai SICant almeno una volta all'anno un feedback su temi quali lo spirito d'iniziativa, la qualità dell'adempimento degli incarichi o il potenziale di miglioramento. Ha inoltre invitato il SIC, a tutela delle informazioni di quest'ultimo, a informare in dettaglio le autorità di vigilanza cantonali sulla procedura da seguire per l'accesso ai dati dei servizi segreti ai sensi dell'articolo 11 dell'ordinanza del 16 agosto 2017 sulle attività informative (OAI)<sup>11</sup>.

### 19-5 Controllo SICant GR

Ai fini del presente rapporto, l'AVI-Aln ha verificato la collaborazione del SIC con il SICant del Cantone dei Grigioni (SICant GR). A questo scopo ha condotto varie interviste con i collaboratori competenti del SIC. Inoltre, il 2 luglio 2019 ha fatto visita

in loco al servizio in questione. Al momento del controllo, la collaborazione tra il SIC e il SICant GR è risultata conforme alla legge, adeguata e in parte anche efficace. L'AVI-Aln ha avuto l'impressione (a parte la sproporzione esistente tra le prestazioni del SICant GR e l'indennità forfettaria versata dalla Confederazione) che la collaborazione tra le due organizzazioni fosse ben impostata e funzionante.

I Cantoni vengono indennizzati per le prestazioni da loro fornite a favore del SIC. L'entità delle indennità versate dipende in misura determinante dal credito a disposizione del SIC, definito nel preventivo. Le risorse sono ripartite in base a una chiave di riparto, tenendo conto delle spese dei Cantoni. In considerazione della menzionata sproporzione, l'AVI-Aln ha raccomandato al SIC e al SICant GR di valutare congiuntamente la situazione, sia dal punto di vista degli incarichi e dei rapporti, sia da quello dell'indennità forfettaria versata dalla Confederazione. Se incarichi e rapporti, rispettivamente le prestazioni del SICant GR, non dovessero corrispondere all'indennità versata, occorrerà aumentare le prestazioni del SICant GR a favore del SIC oppure ridurre l'indennità della Confederazione. Sempre a questo riguardo, l'AVI-Aln ha inoltre raccomandato ai due servizi interessati di esaminare congiuntamente le condizioni di un eventuale futuro coinvolgimento regolare del SICant GR nel World Economic Forum (WEF). L'incontro annuale a Davos tra capi di Stato e leader economici può prestare il fianco ad attività di spionaggio da parte di delegazioni estere.

Il SIC si impegna molto per promuovere la collaborazione con il SICant GR, ad esempio organizzando regolarmente eventi formativi, mettendo a disposizione mezzi tecnici e offrendo la propria consulenza. Il SICant GR ha saputo approfittare di questo appoggio e degli scambi curati congiuntamente. Per entrambe le parti, la cultura del feedback può essere migliorata. L'AVI-Aln seguirà gli ulteriori sviluppi a questo riguardo.

### 19-6 Controllo SICant SH

Come in tutte le altre verifiche effettuate presso i SICant nel 2019, anche in quella presso il SICant del Cantone di Sciaffusa (SICant SH) l'AVI-Aln ha concentrato la propria attenzione sulla collaborazione con il SIC. L'ispezione in loco a Sciaffusa è stata effettuata l'11 aprile 2019. Lo stesso giorno sono state intervistate le persone coinvolte a livello cantonale.

Le informazioni raccolte hanno evidenziato che la collaborazione tra il SICant SH e il SIC si era svolta in modo conforme alla legge, adeguato ed efficace. Entrambe le parti si sono concentrate soprattutto sull'adempimento dei compiti di intelligence e sull'importante ruolo di sensore svolto dal SICant. Quest'ultimo si è dimostrato d'accordo con quanto esposto nel rapporto di verifica dell'AVI-Aln e ha già avviato o addirittura terminato l'attuazione delle sue raccomandazioni, tra cui ad esempio quella che chiedeva un controllo documentato delle cancellazioni di dati di informazioni di intelligence ai sensi della LAIn nell'ambiente informatico cantonale.

### 19-7 Controllo SICant BE

L'11 marzo 2019 l'AVI-Aln ha condotto una verifica presso gli uffici del SICant del Cantone di Berna (SICant BE). Ha inoltre discusso con il segretario generale supplente del Dipartimento di polizia e degli affari militari, autorità di vigilanza cantonale. In tale occasione l'AVI-Aln ha riscontrato la mancanza di un controllo documentato delle cancellazioni di dati di informazioni di intelligence ai sensi della LAIn nell'ambiente informatico cantonale. Ha pertanto raccomandato alla direzione del SICant BE di adottare le necessarie misure al fine di garantire che le informazioni di intelligence salvate temporaneamente nel sistema cantonale in vista dell'importazione nel sistema d'informazione del SIC vengano cancellate dall'ambiente operativo cantonale entro 60 giorni dalla loro archiviazione. Tali cancellazioni dovrebbero essere documentate.

Nella collaborazione tra il SIC e il SICant BE, l'AVI-Aln non ha riscontrato alcuna irregolarità. Al contrario, ha avuto invece l'impressione che tale collaborazione sia ben consolidata e che funzioni, sicuramente anche grazie alla prossimità geografica.

## 5.2.4 Misure di acquisizione soggette ad autorizzazione

### → Misure di acquisizione soggette ad autorizzazione

Le misure di acquisizione soggette ad autorizzazione comprendono la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, l'impiego di apparecchi tecnici speciali di localizzazione e sorveglianza in luoghi non accessibili al pubblico, l'infiltrazione in sistemi e reti informatici e le perquisizioni di locali, veicoli o contenitori. Tutte queste misure offrono al SIC la possibilità di individuare tempestivamente le minacce al fine di proteggere la Svizzera e la sua popolazione. Esse possono essere ordinate soltanto se sussiste una concreta minaccia per la sicurezza interna o esterna della Svizzera, legata al terrorismo, allo spionaggio, alla diffusione di armi di distruzione di massa e della tecnologia relativa ai loro vettori (proliferazione) o a un attacco a infrastrutture critiche, oppure se devono essere adottate per decisione del Consiglio federale al fine di difendere importanti interessi nazionali. Per ragioni legate al principio di proporzionalità, non possono essere ordinate per lottare contro l'estremismo violento.

Inoltre, il ricorso a queste misure presuppone l'esistenza di una minaccia sufficientemente grave, e che altri accertamenti di intelligence siano rimasti infruttuosi, non possano dare risultati o sarebbero esageratamente difficoltosi.

Le misure di acquisizione soggette ad autorizzazione devono sempre essere approvate dal Tribunale amministrativo federale (TAF) e ricevere il nullaosta del capo del DDPS previa consultazione dei capi del DFAE e del Dipartimento federale di giustizia e polizia (DFGP). Le istanze preposte all'approvazione delle misure hanno accesso a tutte le informazioni rilevanti sulla fattispecie.

In un complesso di casi possono essere necessarie diverse di queste misure.

Per quanto riguarda le cifre, rimandiamo al rapporto annuale del SIC sulla sicurezza della Svizzera.

<sup>11</sup> RS 121.1

### 19-8 Adeguatezza ed efficacia delle misure di acquisizione soggette ad autorizzazione

La verifica ha evidenziato che il SIC ha impiegato le misure soggette ad autorizzazione in modo piuttosto adeguato ed efficace. Il quadro giuridico per l'attuazione di queste misure era noto e i risultati ottenuti sono stati conformi alle aspettative. Nella maggior parte dei casi, ad esempio, le misure adottate hanno permesso di convalidare l'attenzione del SIC nei confronti delle persone controllate o di escluderle. Dal canto loro, le risorse tecniche e di personale per l'attuazione di queste misure potrebbero essere ancora ottimizzate. Per le traduzioni da una lingua all'altra occorrerebbe sviluppare una prassi generale, invece di trovare una soluzione di volta in volta.

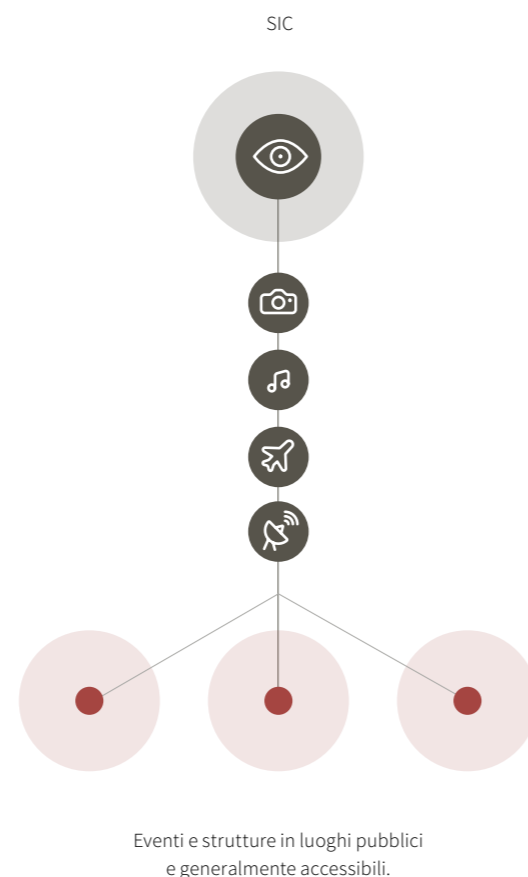
Infine la legge distingue tra misure soggette ad autorizzazione e misure che possono essere attuate senza previa autorizzazione. Secondo il legislatore queste ultime, tra cui le osservazioni di persone in luoghi pubblici e liberamente accessibili, sono meno moleste. L'AVI-AIn ha pertanto raccomandato al SIC di essere più preparato, a partire da inizio 2020, a condurre osservazioni in base alle necessità. In tal modo l'ordine previsto dalla legge per le misure di acquisizione potrà essere rispettato. La data fissata corrisponde a quella del previsto cambiamento nella struttura organizzativa e nella ripartizione dei compiti per le attività di osservazione.

### 19-9 Attuazione delle misure di acquisizione soggette ad autorizzazione

Nell'ambito della verifica 19-9 l'AVI-AIn ha controllato se il SIC ha attuato le misure di acquisizione secondo le decisioni del TAF e se ha rispettato le condizioni poste. La verifica ha riguardato la corretta attuazione di circa 35 autorizzazioni concernenti misure di acquisizione di vario tipo. L'AVI-AIn ha inoltre controllato se le condizioni poste relativamente alla durata delle misure sono state rispettate. Durante le attività di verifica ha constatato che in generale il SIC ha attuato in maniera efficiente le misure di acquisizione soggette ad autorizzazione, rispettato le condizioni ed i limiti imposti dal diritto. Tuttavia, sarebbe possibile introdurre un ulteriore mi-

### → Osservazione

L'osservazione è una misura di acquisizione non soggetta ad autorizzazione mediante la quale il SIC osserva fatti e installazioni in luoghi pubblici e liberamente accessibili. Le registrazioni su supporto audiovisivo sono ammesse dalla legge. L'impiego di aeromobili e satelliti è espressamente autorizzato. Tuttavia la sfera privata protetta deve essere rispettata in ogni caso.



glioramento garantendo un quadro efficiente ed efficace di queste misure, semplificando la gestione e il controllo e organizzando i rapporti in modo più efficiente. Pertanto, l'AVI-AIn ha raccomandato di migliorare ulteriormente le capacità relative all'utilizzazione, all'amministrazione e al controllo dei mezzi tecnici impiegati per attuare le misure.

## 5.2.5 Operazioni

### 19-10 Operazioni

Per il SIC, le operazioni di intelligence sono un elemento centrale per l'acquisizione di informazioni. Si tratta di azioni che per importanza, estensione, dispendio o segretezza travalicano le attività di intelligence correnti. Ma questo ruolo cruciale nel contesto dell'acquisizione di informazioni comporta anche rischi:

- Le risorse a disposizione per l'acquisizione di informazioni sono effettivamente impiegate per lottare contro le principali minacce per la sicurezza interna ed esterna della Svizzera?
- Le disposizioni di legge sono rispettate?
- I metodi operativi adottati dal SIC nell'ambito delle operazioni sono oggettivamente i migliori per raggiungere un obiettivo di intelligence?
- Quanto si avvicina il risultato ottenuto, quantitativamente e qualitativamente, al risultato auspicato?

Per trovare risposta a queste domande, l'AVI-AIn sottopone a verifica il settore Operazioni del SIC almeno una volta all'anno. Sulla base di una serie di criteri selezionati e ponderati, l'AVI-AIn ha elaborato una matrice di decisione e alla fine ha

### → Operazioni

Nel gergo dell'intelligence, un'«operazione» consiste nell'acquisizione di informazioni su avvenimenti correlati che per importanza, estensione, dispendio o segretezza travalica le attività di intelligence correnti. Le operazioni di intelligence hanno una durata limitata. Inoltre devono essere iniziate e concluse formalmente.

Nell'ambito di un'operazione di intelligence possono essere adottate sia misure di acquisizione non soggette ad autorizzazione (per es. osservazioni in luoghi pubblici e liberamente accessibili), sia misure soggette ad autorizzazione (per es. misure di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni). Il SIC può adottare misure di acquisizione soggette ad autorizzazione soltanto nell'ambito di un'operazione di intelligence.

scelto otto operazioni di intelligence, quattro delle quali già concluse, per una verifica più approfondita. Le verifiche effettuate hanno evidenziato che le operazioni in questione erano state condotte in modo conforme alla legge, adeguato ed efficace. Esse erano state definite con chiarezza, limitate nel tempo e documentate separatamente.

L'ottimizzazione e la formalizzazione del processo di gestione e controllo delle operazioni potrebbe contribuire a migliorare l'adeguatezza e l'efficienza delle operazioni nel loro complesso.

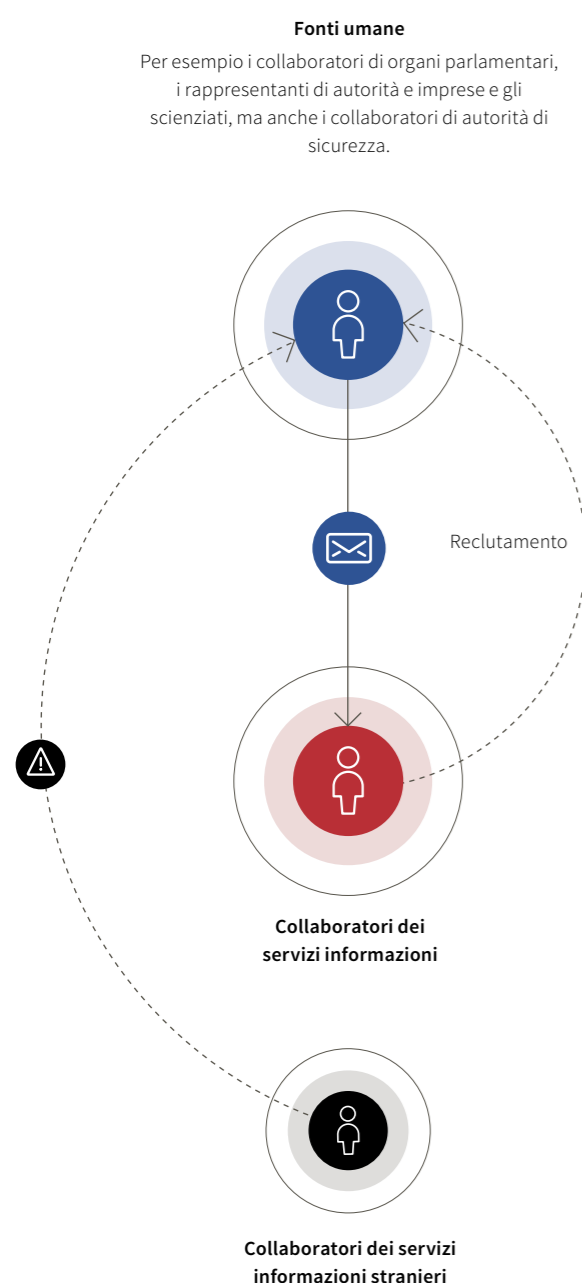
### 19-11 Fonti umane (HUMINT)

Nell'ambito della verifica 19-11 l'AVI-AIn si è occupata delle fonti umane, esaminando il modo in cui il SIC ha gestito concretamente queste fonti. L'AVI-AIn ha dunque verificato la legalità, l'adeguatezza e l'efficacia nell'ambito di quattro casi selezionati di gestione di fonti del SIC. 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. Il controllo sarà completato nel 2020.

### 19-12 Protezione delle fonti in seno al SIC focalizzandosi sulla copertura e l'identità fittizia

In virtù dell'articolo 35 LAIn, il SIC garantisce la protezione delle sue fonti e ne tutela l'anonimato. Per proteggere la loro vita e la loro integrità fisica, le fonti e le persone a loro vicine possono dunque essere dotate di una copertura o di un'identità fittizia al termine della loro collaborazione con il SIC. L'assegnazione di coperture e identità fittizie deve essere autorizzata dal capo del DDPS.

«Secondo l'AVI-AIn, la chiara definizione di processi e responsabilità riduce la probabilità di errori e abusi.»



### → Fonti umane

Per HUMINT (acronimo dall'inglese Human Intelligence) si intende l'acquisizione di informazioni per mezzo di fonti umane. In pratica vi sono due persone: una che fornisce un'informazione e l'altra che la riceve. Il ricevente è agente di un servizio di intelligence. Come sinonimo di HUMINT viene utilizzata anche l'espressione «esplorazione operativa». Con l'aggettivo «operativa» si intende che viene impiegata una misura mirata nell'ambito di una determinata operazione di intelligence per ottenere un'informazione, per esempio osservando una persona o sfruttando appunto una fonte umana.

Le fonti umane vengono selezionate e reclutate in modo mirato. Devono avere accesso a informazioni e supporti di informazioni sensibili di particolare rilevanza per la Svizzera. La protezione delle fonti e delle persone impone in questo campo uno speciale livello di segretezza. Normalmente, le persone che lavorano come fonti forniscono volontariamente informazioni ai servizi di intelligence, perlopiù consapevolmente, in parte gratuitamente, se ciò favorisce il raggiungimento dei loro scopi personali o politici. Il reclutamento di fonti umane riguarda in particolare le persone che sembrano idonee a servire come fonte d'informazioni a lungo termine. Tra i criteri importanti vi sono le possibilità attuali di accesso a informazioni e le prospettive professionali delle fonti umane. Entrano per esempio in considerazione i collaboratori di organi parlamentari, i rappresentanti di autorità e imprese e gli scienziati, ma anche i collaboratori di autorità di sicurezza. Gli agenti dei servizi di intelligence utilizzano però anche metodi cospirativi per acquisire informazioni particolarmente sensibili.

Anche gli agenti di servizi di intelligence stranieri si adoperano per instaurare contatti con persone in Svizzera che possiedono particolari conoscenze o possibilità di accesso. Questi servizi sono spesso insediati presso le ambasciate o i consolati dei loro Paesi in Svizzera. Essi acquisiscono informazioni direttamente, apertamente o in segreto, oppure forniscono supporto per operazioni di intelligence condotte direttamente dai quartier generali in patria. Spesso godono dello statuto diplomatico e sfruttano la relativa immunità. Se queste persone vengono smascherate, possono essere espulse dalla Svizzera.

Le fonti umane, in quanto contatto diretto, sono tuttora uno strumento fondamentale per i servizi di intelligence, quantunque questo metodo tradizionale abbia perso importanza con la diffusione dell'impiego di mezzi elettronici. Esse possono essere imprescindibili in particolare nel campo dello spionaggio politico, in cui occorre soprattutto acquisire informazioni secondo direttive specifiche dei servizi di intelligence.

L'assegnazione di una copertura a collaboratori del SIC o a collaboratori delle autorità d'esecuzione cantonali può però essere autorizzata anche dal direttore del SIC. In questo caso lo scopo consiste nel dissimulare l'appartenenza dei collaboratori al loro servizio. Gli stessi collaboratori possono beneficiare anche di un'identità fittizia per un periodo limitato, ma prorogabile, se si tratta di garantire la sicurezza delle persone interessate o se necessario per l'acquisizione di informazioni. La differenza tra copertura e identità fittizia consiste nel fatto che per la creazione di una copertura possono essere allestiti o modificati documenti (per es. un diploma) a nome della persona interessata. Per creare identità fittizie possono invece essere allestiti o modificati anche documenti d'identità, addirittura utilizzando dati biografici fittizi quali il nome o la data di nascita.

La modifica e l'allestimento di attestati e documenti d'identità sono atti penalmente perseguibili che però vengono legittimati con l'autorizzazione del direttore del SIC o del capo del DDPS; pertanto, è importante verificare che il SIC impieghi tali misure in modo conforme alla legge.

Nell'ambito della verifica 19-12 l'AVI-AIn ha dunque esaminato se la protezione delle fonti umane, in particolare per quanto riguarda gli strumenti di protezione, ossia coperture e identità fittizie, è stata utilizzata in modo conforme alla legge, adeguato ed efficace. L'AVI-AIn ha constatato che la protezione delle fonti ha svolto un ruolo importante ed è stata trattata con serietà: il SIC ha protetto le sue fonti con varie misure a diversi livelli. Nell'ambito delle sue attività di verifica, l'AVI-AIn non ha sinora riscontrato alcuna illegalità nell'uso di coperture e identità fittizie. Nondimeno, in tutti i casi le autorizzazioni relative alle coperture sono state richieste «di scorta». In altri termini, molte sono state richieste e autorizzate ma non sono state concretizzate e sfruttate; secondo l'AVI-AIn questo modo di procedere non è adeguato.

L'AVI-AIn ha inoltre constatato che i processi e le responsabilità relativi alla richiesta, alla gestione, all'allestimento, al mantenimento e allo smantellamento di coperture e identità fittizie (e delle infrastrutture occorrenti per le coperture) erano definiti in modo incompleto e scarsamente armonizzati.

L'AVI-AIn ritiene che la chiara definizione di processi e responsabilità riduca le probabilità di errori e abusi, e che l'armonizzazione dei processi consentirebbe anche di utilizzare in modo più efficace le risorse.

## 5.2.6 Risorse

### 19-13 Processo di reclutamento, di assistenza e di uscita

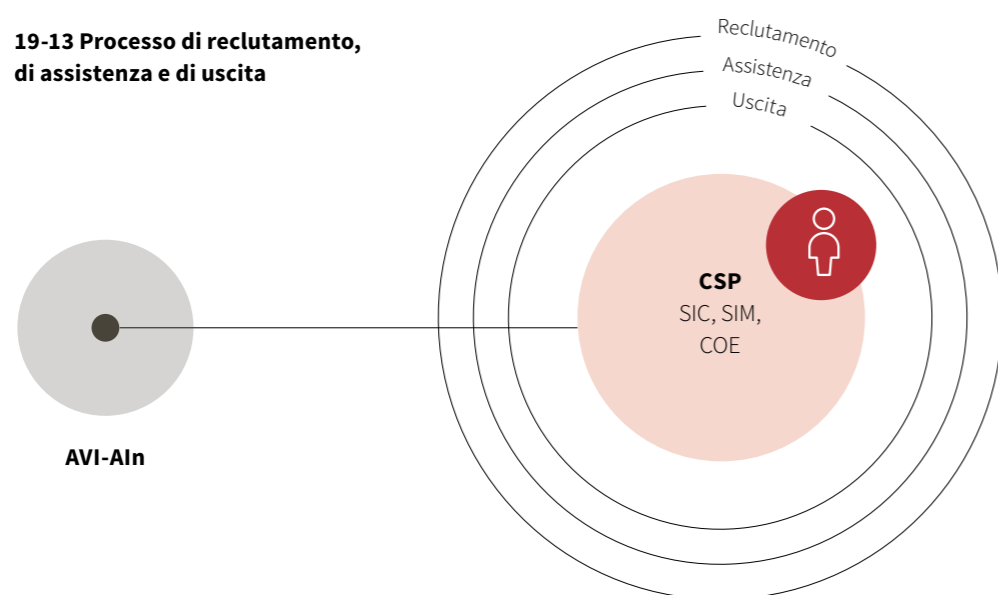
Nello svolgimento di attività informative, un rischio elevato può derivare dai propri collaboratori (tradimento, furto di dati, spionaggio ecc.). Il furto di dati avvenuto in seno al SIC nel 2012 ce ne ha fornito un esempio concreto. Per minimizzare questo rischio, è molto importante che i servizi delle risorse umane e i superiori gerarchici curino la selezione, la verifica e l'affiancamento del personale.

La verifica 19-13 è stata suddivisa in due parti e per i due servizi controllati (SIM, verifica 19-13a; COE, verifica 19-13b) è stato redatto un rapporto separato. Inizialmente era prevista anche una verifica del SIC. Tuttavia, considerato il carico rappresentato dalle verifiche previste nel 2019, l'AVI-AIn ha rinviato tale verifica a un momento successivo.

Le attività di verifica sono state incentrate su questioni riguardanti i controlli di sicurezza relativi alle persone (CSP) nei tre processi concernenti il personale, ossia il reclutamento, l'assistenza e l'uscita. Sulla scorta di una serie di interviste e dell'esame della documentazione, accompagnati da controlli a campione sulle singole fasi dei processi, la verifica mirava a stabilire se esistesse un processo per i CSP e se tale processo potesse essere considerato conforme alla legge, adeguato ed efficace.

Sia in seno al SIM sia in seno al COE vengono impiegati processi CSP che funzionano adeguatamente. In seno al COE, molti posti sono classificati nel livello di controllo più approfondito (CSP 12). A causa delle audizioni individuali supplementari, questi controlli comportano un dispendio di tempo e devono essere avviati tempestivamente. In passato vi sono stati alcuni ritardi nel rinnovo dei CSP 12 scaduti di collaboratori

### 19-13 Processo di reclutamento, di assistenza e di uscita



di lunga data. Pertanto, l'AVI-AIn ha raccomandato di avviare tempestivamente il processo di rinnovo presso il competente servizio del DDPS.

Inoltre l'AVI-AIn ha confrontato e analizzato i livelli di controllo di tutti i servizi operanti nel settore delle attività informative, e quindi anche quelli del SIC. In tale ambito ha constatato che la diversa prassi in materia di CSP applicata ai collaboratori del SIC, del SIM e del COE incaricati di attività informative non era giustificata, né sul piano giuridico né su quello materiale e logico. Per incrementare l'efficacia, le differenze attualmente esistenti nei sistemi di classificazione CSP dovrebbero essere verificate ed eliminate, armonizzando la prassi in seno a questi tre servizi. Nell'ambito di tale verifica occorrerebbe considerare anche gli eventuali futuri cambiamenti che potrebbero derivare dal progetto di una nuova legge sulla sicurezza delle informazioni attualmente pendente in Parlamento.

Dai controlli effettuati dall'AVI-AIn è emerso che nei due servizi sottoposti a verifica i rischi legati al processo di reclutamento sono stati sufficientemente considerati. Normalmente il CSP era stato concluso prima dell'inizio dell'attività. Inoltre, dopo l'inizio dell'attività i collaboratori neoassunti erano stati sensibilizzati in merito alle questioni di sicurezza e adeguatamente formati.

I rischi legati ai collaboratori già assunti sono stati affrontati adeguatamente e i superiori hanno svolto un ruolo chiave nel riconoscere i cambiamenti sul piano personale. Per quanto possibile e ragionevole, si è fatto ricorso a controlli di sicurezza organizzativi e tecnici.

Nell'ambito dell'uscita di personale ci si è assicurati che i diritti di ingresso ed accesso fossero stati disattivati o rimossi. È stata consacrata sufficiente attenzione anche al trasferimento di conoscenze e i collaboratori uscenti hanno dovuto firmare una dichiarazione di riservatezza.

### 19-14 Utilizzo sicuro di videoconferenze

Oggi gli sistemi per videoconferenze (VTC) rappresentano un mezzo di comunicazione efficiente e diffuso. Il SIC impiega tale mezzo per trasmettere informazioni ai propri partner.

Nella maggior parte dei casi il contenuto delle conversazioni è classificato SEGRETO. Perciò occorre assolutamente impedire fughe di informazioni dovute a carenze tecniche dell'impianto o a errori di utilizzazione.

Per verificare la legalità dell'acquisto e della manutenzione degli sistemi gestiti, l'AVI-AIn ha condotto una serie di colloqui con le persone responsabili in seno al SIC e ad alcuni partner, analizzando anche la documentazione esistente. Inoltre, per farsi un'idea diretta del materiale informatico disponibile nei locali VTC e del loro impiego, ha partecipato ad alcune videoconferenze del SIC.

Dalla verifica dell'AVI-AIn è emerso che questi sistemi sono stati acquistati legalmente e impiegati in modo adeguato ed efficace. Gli standard di sicurezza del settore dell'intelligence sono stati rispettati. L'autorità di vigilanza ha individuato un potenziale di ottimizzazione soltanto nell'ambito dell'esercizio.

«Nei due servizi sottoposti a verifica i rischi legati al processo di reclutamento sono stati sufficientemente considerati.»

«Dalla verifica dell'AVI-AIn è emerso che gli impianti per le videoconferenze sono stati acquistati legalmente e impiegati in modo adeguato ed efficace.»

### 5.2.7 Trattamento dei dati / archiviazione

#### 19-15 Esercizio, contenuto e utilizzo dei sistemi d'informazione GEVER SIC, memorizzazione dei file in BURAUT, memorizzazione dei file in SiLAN (valutazioni temporanee)

Nell'ambito della verifica 19-15, l'autorità di vigilanza ha analizzato la legalità dell'esercizio, del contenuto e dell'utilizzo dei sistemi d'informazione GEVER SIC<sup>12</sup> e della memorizzazione dei file in BURAUT<sup>13</sup> e in SiLAN<sup>14</sup> (valutazioni temporanee). Considerato il notevole impegno richiesto per questa verifica e la complessità di GEVER SIC, le conclusioni sono state ripartite in due rapporti. Il rapporto della verifica 19-15a tratta esclusivamente di GEVER SIC, mentre i due sistemi d'informazione SiLAN e BURAUT sono descritti nel rapporto 19-15b.

#### 19-15a GEVER SIC

Nell'ambito della verifica di GEVER SIC, l'AVI-AIn si è concentrata sulla legalità nell'assegnazione di diritti di accesso, nella registrazione di dati e nel rispetto dei relativi termini di con-

servazione nonché nella cancellazione e archiviazione di dati. Inoltre ha verificato l'efficacia dei controlli istituiti. Oltre che per mezzo di un'ampia analisi della documentazione, la verifica è stata condotta anche sulla base di interviste con specialisti responsabili del SIC e dell'Archivio federale, nonché di controlli a campione in loco presso dieci collaboratori del SIC.

Le prescrizioni in materia di protezione delle informazioni e dei dati esigono che i collaboratori del SIC abbiano accesso soltanto ai dati di cui hanno bisogno per adempiere i loro compiti.

La violazione di tali prescrizioni da parte del SIC potrebbe creare

- una minaccia per la sicurezza della Svizzera;
- il coinvolgimento del SIC in procedimenti giudiziari;
- un danno d'immagine per il servizio agli occhi della popolazione e anche dei servizi partner.

La verifica condotta dall'AVI-AIn ha evidenziato che il SIC disponeva di un concetto articolato per i diritti di accesso a GEVER SIC. I diritti di accesso erano gestiti per mezzo di diversi ruoli. L'analisi degli elenchi di autorizzazioni e i controlli a campione effettuati presso dieci collaboratori hanno confermato

<sup>12</sup> Sistema di trattamento e controllo degli affari

<sup>13</sup> Sistema di memorizzazione dei file gestito dalla BAC

<sup>14</sup> Rete informatica protetta per la memorizzazione di file

#### → GEVER

GEVER (sistema elettronico di gestione degli affari, dal tedesco GESchäftsVERwaltung) è l'acronimo che in Svizzera sta a indicare il sistema elettronico di gestione degli affari utilizzato nella pubblica amministrazione e una delle basi del governo elettronico.

Con l'introduzione di GEVER in seno all'Amministrazione federale, le unità amministrative gestiscono elettronicamente tutte le informazioni rilevanti per i loro affari, ossia tutti gli atti da esse trattati con tale sistema nell'ambito del mandato assegnato loro dalla legge.

GEVER si orienta ai processi operativi. Esso permette una gestione degli atti al tempo stesso trasparente, documentabile, conforme alla legge ed efficiente. Il ciclo di vita dei documenti gestiti è interamente visualizzato in GEVER, dalla creazione — passando per l'utilizzazione, il salvataggio e la separazione — fino all'archiviazione o alla distruzione.

## «Dal controllo effettuato dall'AVI-AIn è emerso che GEVER SIC non contiene dossier su personaggi politici allestiti esclusivamente a causa delle loro attività politiche.»

che le autorizzazioni erano concesse in modo adeguato e nel rispetto delle prescrizioni di legge. Secondo l'AVI-AIn, il processo previsto per la gestione delle autorizzazioni presentava ancora un potenziale di ottimizzazione. Inoltre occorrerebbe sottoporre a un esame il ricorso a servizi esterni per la manutenzione e il supporto relativi a GEVER SIC.

GEVER SIC dovrebbe contenere tutte le informazioni rilevanti per gli affari, in particolare per tutti i prodotti di intelligence in uscita. Ciò vale in particolare per tutti i prodotti di intelligence trasmessi all'esterno, nonché per tutte le attività ufficiali (risposte alle lettere dei cittadini, risposte agli interventi parlamentari, attività legislative). Se gli affari non sono archiviati e trattati in GEVER SIC in maniera documentata, il SIC non è in grado di sostanzialmente le informazioni contenute nei suoi prodotti in uscita. In GEVER SIC non possono essere acquisite o trattate informazioni sull'attività politica e sull'esercizio della libertà di opinione, di riunione o di associazione in Svizzera.<sup>15</sup> Eccezione: se sussistono indizi concreti indicanti che i menzionati diritti vengono esercitati per preparare o eseguire attività terroristiche, di spionaggio o di estremismo violento.

Per mezzo di controlli a campione, l'AVI-AIn ha verificato la legalità della registrazione dei dati inseriti in GEVER SIC su undici personaggi politici e il rispetto dei limiti relativi alle informazioni posti dall'articolo 5 capoverso 5 LAIn. Inoltre ha analizzato il trattamento di cinque domande di accessi presentate da privati cittadini e organizzazioni nonché da due personaggi politici, uno di sesso maschile e l'altro di sesso femminile, anch'essi registrati in GEVER SIC. Tale verifica ha confermato che nell'ambito delle domande di informazione esaminate il SIC ha fornito le informazioni richieste in modo corretto e completo. Le informazioni raccolte rispettavano sostanzialmente le prescrizioni di legge. Occorre precisare che la maggior parte delle informazioni personali contenute in GEVER SIC provenivano da articoli di giornale di pubblico dominio. Sulla base dei controlli a campione effettuati, l'AVI-

AIn ha constatato che GEVER SIC non contiene dossier su personaggi politici allestiti esclusivamente a causa delle loro attività politiche. A questo riguardo, l'autorità di vigilanza ha raccomandato al SIC di verificare la legalità della prassi attuale sulla raccolta di informazioni da fonti pubbliche.

Sinora non è stato versato all'Archivio federale alcun documento tratto da GEVER SIC. Attualmente questo aspetto non crea però difficoltà, dato il margine di manovra sufficientemente ampio concesso dal termine ventennale previsto dalla legge. A giudizio dell'AVI-AIn, la prassi applicata dal SIC, consistente nel fornire atti all'Archivio federale mano a mano, consente ragionevolmente di non trovarsi costretti ad agire in tutta fretta proprio alla scadenza dei termini legali di conservazione.

Il rapporto non sarà completato e inviato al capo del DDPS fino al primo trimestre del 2020.

### 19-15b SiLAN / BURAUT

SiLAN è una rete informatica protetta interna al SIC, che viene utilizzata per il trattamento di dati classificati fino al livello SEGRETO compreso. In questa rete viene gestita in particolare una banca dati per il trattamento di valutazioni temporanee. La verifica condotta dall'AVI-AIn era intesa a valutare la legalità dell'impiego di tale banca dati.

Nell'ambito di una verifica in loco, l'autorità di vigilanza ha esaminato in particolare i diritti di accesso al sistema di memorizzazione dei file temporanei presso dieci collaboratori del SIC. La verifica non ha messo in luce autorizzazioni di accesso inutili e ingiustificate. Dall'analisi del contenuto del sistema di memorizzazione non sono emerse irregolarità e violazioni delle vigenti prescrizioni di legge. I dati trattati non risalivano a un periodo precedente ai cinque anni ammessi. Secondo l'AVI-AIn, la valutazione annuale dell'organo di controllo della qualità del SIC (CQ SIC) e della necessaria autorizzazione da parte del detentore dei dati garantiva un controllo

sufficiente del rispetto delle prescrizioni di legge. Dalle verifiche 18-1 e 18-2 in poi, il SIC ha continuamente portato avanti e migliorato le misure da esso adottate a questo riguardo.

Oltre all'ambiente SiLAN, i collaboratori del SIC dispongono anche di una postazione di lavoro BURAUT. Questo sistema di archiviazione consiste in una piattaforma standard della Confederazione; è gestito su un server della BAC<sup>16</sup> e nei casi eccezionali autorizzati dal capo della Gestione delle informazioni, serve per memorizzare i file occorrenti per la collaborazione tra vari uffici e dipartimenti. Siccome vengono gestiti al di fuori della rete protetta del SIC, questi dati sono meno protetti contro fughe di informazioni non autorizzate. Di conseguenza, nell'ambiente BURAUT non si possono trattare informazioni non cifrate classificate CONFIDENZIALE, e tantomeno informazioni classificate SEGRETO.

A giudizio dell'AVI-AIn, l'operazione di ripulitura effettuata dal CQ SIC è riuscita e ha consentito di sensibilizzare i collaboratori e di ridurre notevolmente la mole dei dati.

### 19-16 Classificazioni di informazioni

La verifica 19-16 è stata condotta simultaneamente presso il SIC, il SIM e il COE. In tale ambito l'autorità di vigilanza ha esaminato se le informazioni fisiche ed elettroniche vengono trattate in modo conforme alla legge.

La questione della classificazione delle informazioni tocca vari altri temi e quindi non può essere considerata isolatamente. Per il trattamento di informazioni classificate, ad esempio, contano anche aspetti relativi alla sicurezza delle informazioni, alla conservazione di dati e alla sicurezza fisica.

### Sicurezza delle informazioni

Società, economia, politica e amministrazione dipendono sempre più dalla disponibilità di informazioni interconnesse.

È dunque essenziale garantire una protezione sufficiente, ma anche economicamente sostenibile, di queste informazioni. Questo principio non vale solo per le informazioni stesse, ma anche per i sistemi di informazione e comunicazione che registrano, trattano, veicolano o memorizzano le informazioni. In questo contesto si parla quindi di **sicurezza delle informazioni**: questa comprende, oltre alle tematiche della protezione e della sicurezza delle informazioni, anche la protezione dei dati.

### Protezione delle informazioni

La protezione delle informazioni comprende la protezione delle informazioni della Confederazione e dell'esercito, in particolare la loro classificazione e il loro trattamento. Classificare significa assegnare un'informazione a un livello di classificazione (SEGRETO, CONFIDENZIALE o AD USO INTERNO) in funzione delle necessità di protezione. Le informazioni vengono protette assicurandone la confidenzialità, l'integrità, la disponibilità e la tracciabilità.

L'AVI-AIn constata che nella prassi i vari concetti non vengono utilizzati operando una precisa distinzione. Ciò può creare una certa confusione: da un lato si parla di «ordinanza sulla protezione delle informazioni» e dall'altro di «sistemi di gestione della sicurezza delle informazioni» (SGSI). Inoltre, il Parlamento sta vagliando una nuova «legge sulla sicurezza delle informazioni». Quest'ultima si trova attualmente nel processo legislativo e permetterà di eliminare le incertezze.

La verifica 19-16 (Classificazioni di informazioni) è stata condotta simultaneamente presso il SIC, il SIM e il COE. In tale ambito l'AVI-AIn ha esaminato se le informazioni fisiche ed elettroniche vengono trattate in modo conforme alla legge. Essa ha potuto accertare che la protezione delle informazioni della Confederazione passava chiaramente al servizio competente attraverso il DDPS.

<sup>15</sup> Art. 5 cpv. 5 LAIn

<sup>16</sup> Base d'aiuto alla condotta dell'esercito (BAC)

«La questione della classificazione delle informazioni tocca vari altri temi e quindi non può essere considerata isolatamente.»

Grazie a un sistema completo di gestione della sicurezza delle informazioni (SGSI), ben documentato e regolarmente applicato, il SIC si è assicurato che le informazioni fossero trattate conformemente alla legge e inoltre che tutte le esigenze in materia di sicurezza delle informazioni fossero rispettate. Presso il SIM e il COE, il processo relativo alla sicurezza delle informazioni era a tratti abbozzato sotto forma di singoli concetti, manuali e presentazioni. L'AVI-AIn si aspetta che questa situazione migliorerà a partire da metà 2020 con l'introduzione di un SGSI specifico per il COE, attualmente in fase di sviluppo presso il Comando Operazioni.

All'interno dell'ambiente sicuro dei sistemi d'informazione interni ai servizi, la distinzione delle informazioni la cui conoscenza da parte di persone non autorizzate può causare uno svantaggio (AD USO INTERNO), un danno (CONFIDENZIALE) o un grave danno (SEGRETO) ha un'importanza secondaria. La classificazione CONFIDENZIALE o SEGRETO comporta invece un conseguente maggior onere amministrativo per i destinatari esterni a tale ambiente sicuro. L'autore di informazioni classificate deve esserne consapevole e utilizzare con moderazione lo strumento della classificazione. Se non si trova un equilibrio tra l'opportunità di proteggere le informazioni e un inutile maggior onere, si rischia in definitiva che la classificazione non venga più considerata con la necessaria serietà a causa della cronica sovraclassificazione dei documenti. La protezione originariamente ricercata classificando le informazioni effettivamente degne di protezione può così essere vanificata, o quantomeno indebolita. Per garantire un determinato standard, e quindi una determinata comparabilità della classificazione all'interno dell'organizzazione, si potrebbero ad esempio eseguire controlli a campione periodici. Tali controlli dovrebbero essere effettuati da un organo non coinvolto nell'attività fondamentale dei servizi.

#### 19-18 Ambiente informativo del COE

Il COE fa parte dell'esercito e adempie una serie di compiti tecnici a favore dell'esercito e dei servizi informazioni civili e militari. Il centro è responsabile in particolare dell'esplorazione di canali di comunicazione, ad esempio della comunicazione vocale tra telefoni satellitari o della comunicazione di dati in cavi terrestri. Inoltre svolge un ruolo importante in relazione a temi quali la ciberdifesa, i ciberattacchi e la ciberesplorazione.

L'AVI-AIn era dunque interessata a sapere quali sistemi d'informazione utilizza il COE per le proprie attività legate all'intelligence. Secondo l'autorità di vigilanza, l'interesse di questo tema consisteva nel fatto che solo conoscendo approfonditamente i sistemi d'informazione impiegati si sarebbero potute trarre conclusioni su altri ambiti tematici, quali ad esempio la questione della gestione di dati.

In sostanza, l'AVI-AIn ha constatato che i sistemi in questione erano ben documentati. Il loro esercizio era fondato su una solida base legale e il COE si è considerevolmente impegnato per proteggere i sistemi contro l'accesso da parte di entità non autorizzate dall'esterno.

La continua evoluzione delle tecnologie della comunicazione, la molteplicità dei canali di comunicazione e l'enorme volume di dati trasmessi pongono il COE di fronte a grandi sfide. I sistemi d'informazione e le basi legali devono pertanto essere continuamente sviluppati, onde poter soddisfare nel presente e anche nel futuro le esigenze dei beneficiari di prestazioni quali il SIC o il SIM.

«I sistemi d'informazione del COE devono essere continuamente sviluppati.»

#### 19-19 Strumenti per l'analisi di dati al COE

Questa verifica è stata avviata solo verso fine dicembre 2019 e pertanto nel presente rapporto non è possibile riferire al riguardo.

#### 19-20 Comunicazione di dati personali ad autorità estere (art. 61 LAIn)

Lo scambio di informazioni con partner esteri rientra nelle attività quotidiane del SIC; pertanto, l'AVI-AIn ha esaminato questo aspetto. La comunicazione di dati personali ad autorità estere è disciplinata espressamente all'articolo 61 LAIn.

Dalla verifica è emerso che la cerchia delle persone partecipanti alla comunicazione è circoscritta, che i processi per i vari canali di comunicazione con i partner esteri erano definiti e che le comunicazioni scambiate erano registrate e facilmente accessibili. Le interviste e i controlli a campione condotti su una trentina di comunicazioni trasmesse a partner esteri hanno evidenziato che la prassi sviluppata dal SIC consentiva in generale di adempiere i criteri di legge. Tuttavia l'adempimento dei criteri è sembrato piuttosto il risultato di una routine che non una conoscenza giuridica attiva dei criteri applicabili. Pertanto, l'AVI-AIn ha raccomandato al SIC di adottare varie misure, quali l'adeguamento di direttive interne e/o l'organizzazione di corsi regolari per i collaboratori interessati, per migliorare la conoscenza del contesto giuridico che disciplina la comunicazione. Queste misure dovrebbero consentire al SIC di garantire anche in futuro la corretta comunicazione di dati personali all'estero.

L'autorità di vigilanza ha inoltre constatato che i dati trasmessi a terzi devono provenire dal sistema di analisi integrale («integrates Analysensystem», IASA) del SIC. Questo criterio è noto ai collaboratori ed è stato ampiamente rispettato. Nell'ambito delle comunicazioni effettuate dal settore Operazioni, le informazioni possono tuttavia essere comunicate qualche giorno prima della registrazione nel pertinente sistema. Questo problema, legato a ritardi nell'immissione dei dati, era noto al SIC e dovrebbe essere parzialmente risolto nei prossimi anni grazie all'approntamento di risorse supplementari per lo smistamento dei dati. Nel frattempo il SIC è tenuto a fare il possibile per garantire il rispetto del testo dell'OAIn.

### 5.3 Consenso

Secondo l'articolo 78 capoverso 6 LAIn, l'autorità di vigilanza indipendente comunica al DDPS il risultato delle proprie verifiche e in tale contesto può formulare raccomandazioni. Oltre a queste, può emanare anche indicazioni per i servizi controllati.

Secondo la prassi dell'AVI-AIn, vi sono due casi d'applicazione in cui vengono emanate indicazioni:

- 1) nel caso di constatazioni che richiedono eventualmente ottimizzazioni che, per motivi di conformità al livello gerarchico, non devono essere attuate dal capo del DDPS, bensì a un livello operativo inferiore (per es. utilizzo di telefoni cellulari durante le riunioni in cui si discutono questioni confidenziali);
- 2) nel caso di constatazioni effettuate casualmente nell'ambito di una verifica e non direttamente coperte dal mandato di controllo, ma che rivestono ugualmente una certa importanza.

Non esiste una base legale per tali indicazioni e non è nemmeno prevista una verifica della loro attuazione da parte dell'AVI-AIn. Esse sono un importante strumento metodologico che consente di dare adito a verifiche future. Da un lato, le decisioni, le prescrizioni e il lavoro dei servizi esterni hanno un impatto sulle attività di intelligence, dall'altro, le raccomandazioni e i suggerimenti dell'AVI-AIn ai servizi di intelligence possono comportare anche effetti sui servizi esterni, il cui monitoraggio non rientra nell'ambito dell'AVI-AIn.

Secondo l'articolo 78 capoverso 7 LAIn, il DDPS provvede all'attuazione delle raccomandazioni. Pertanto, ordina alle autorità sottoposte a vigilanza di procedere in tal senso. Per quanto riguarda le indicazioni emesse, il DDPS esige di norma che l'organo sottoposto a verifica ne tenga conto anche quando non sono vincolanti. Nel 2019 l'AVI-AIn ha emanato 27 raccomandazioni e 37 indicazioni. Nel complesso tutte le raccomandazioni sono state accettate.

Nell'ambito della loro attività, i responsabili delle verifiche sono stati accolti con atteggiamento costruttivo e professionalità da tutti gli organi sottoposti a verifica. Essi hanno potuto accedere ai documenti e sistemi d'informazione necessari per poter adempiere il loro mandato di verifica. Le persone intervistate erano a loro disposizione. Le interviste hanno potuto essere programmate e attuate tempestivamente e le domande supplementari hanno ricevuto al più presto risposta.

### 5.4 Controlling di raccomandazioni e indicazioni

La verifica dell'attuazione delle raccomandazioni non è espressamente disciplinata dalla legislazione in materia di attività informative. D'intesa con il DDPS e con le autorità sottoposte a vigilanza è stato deciso che queste ultime avrebbero informato per scritto il dipartimento in merito all'attuazione delle raccomandazioni e alla verifica delle indicazioni, con copia all'AVI-AIn. Nel 2019 scadevano i primi termini per l'attuazione delle raccomandazioni. Il processo di comunicazione e verifica interno all'AVI-AIn può ancora essere ottimizzato. Attualmente le indicazioni riguardanti la quantità e soprattutto la qualità delle raccomandazioni attuate sono ancora insufficientemente rappresentative. Nel 2019 era prevista l'attuazione formale di 63 raccomandazioni e 40 indicazioni. Se è in disaccordo con le misure di attuazione realizzate, l'AVI-AIn può eventualmente sottoporle a controllo nell'ambito di verifiche successive.

## 6. Vista interna

### 6.1 Revisione della LAIn

Nel 2019 il DDPS è stato incaricato di effettuare i primi lavori di revisione della LAIn. Il 27 agosto 2019 il SIC ha invitato a una prima seduta i rappresentanti dei servizi federali e cantonali interessati. In questa occasione sono stati istituiti diversi gruppi di lavoro. L'AVI-AIn ha partecipato con tre collaboratori al gruppo di lavoro «Sorveglianza» nel quale erano presenti anche un rappresentante dell'Autorità di controllo indipendente per l'esplorazione radio e l'esplorazione dei segnali via cavo (ACI) e uno della SG-DDPS.

Al SIC sono state trasmesse proposte di modifica per il progetto di legge concernente l'articolo 142 capoversi 2 e 3 della legge sul Parlamento (LParl)<sup>17</sup> in combinato disposto con gli articoli 77-79b LAIn. Il 3 dicembre l'AVI-AIn ha partecipato alla seduta conclusiva di questa fase del progetto legislativo. Oltre alle modifiche formali nel processo di preventivazione, la fusione dell'ACI e dell'AVI-AIn e la creazione di una base legale per le attività internazionali dell'AVI-AIn sono elementi importanti.

<sup>17</sup> RS 171.10

### 6.2 Formazione continua dei collaboratori dell'AVI-AIn

Nel 2019 i collaboratori dell'AVI-AIn hanno partecipato a convegni specializzati ad esempio nel settore della sicurezza delle informazioni o della protezione dei dati e frequentato formazioni individuali, in particolare nel campo della gestione dei rischi.

Inoltre, l'AVI-AIn ha organizzato corsi interni di formazione continua in gruppi sui seguenti temi:

- controspionaggio;
- misure di acquisizione soggette ad autorizzazione;
- tecnica e tattica d'intervista;
- presentazione del sistema d'informazione GEVER SIC;
- aggiornamento soccorso d'emergenza;
- protezione dei dati;
- presentazione del sistema d'informazione IASA SIC.

Gli eventi sono stati organizzati sia dal personale specializzato interno al SIC sia in collaborazione con servizi esterni come il Servizio specializzato per i controlli di sicurezza relativi alle persone della SIO o l'IFPDT. L'AVI-AIn ringrazia in questa sede per il sostegno ricevuto.

«La trasparenza è un atteggiamento di base e non un progetto.»

### Contatti internazionali

#### Oversight Network Meetings

- L'Aia, 24 gennaio 2019
- Bruxelles, 7 marzo 2019
- Copenaghen, 27 giugno 2019
- European Intelligence Oversight Conference 2019, L'Aia, 12 dicembre 2019
- 3° simposio sul diritto dei servizi informazioni, Berlino, 7-8 novembre 2019



## 7. Coordinamento

### 7.1 Contatti nazionali

Il coordinamento dell'attività di vigilanza è un compito principale dell'AVI-Aln. Anche nel 2019 ha quindi collaborato con organi nazionali e altre autorità di vigilanza.

#### Delegazione delle Commissioni della gestione (DelCG)

La DelCG ha invitato l'AVI-Aln alle consultazioni del 23 gennaio 2019, del 12 aprile 2019 e del 23 ottobre 2019. In queste occasioni, l'AVI-Aln ha informato la DelCG, tra l'altro, in merito ai rapporti di controllo del 2018 e del 2019 (18-5 Condotta delle operazioni/ritmo di condotta, 19-12 Protezione delle fonti in seno al SIC focalizzandosi sulla copertura e l'identità fittizia) e al suo primo rapporto d'attività.

La DelCG ha, tra l'altro, invitato l'AVI-Aln a una conferenza tenutasi a Berna il 26 febbraio 2019 a cui hanno partecipato rappresentanti degli organi di vigilanza parlamentare di 21 Cantoni. In quell'occasione l'AVI-Aln ha potuto presentare le sue competenze in materia di vigilanza sui servizi informazioni cantonali.

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

Il 4 gennaio 2019 si è svolto un incontro tra il capo dell'AVI-Aln e il presidente dell'ACI. Essi hanno discusso, tra l'altro, delle sfide future della vigilanza sull'esplorazione dei segnali via cavo. Nel limite del possibile, il coordinamento tra le attività di vigilanza e quelle di verifica avviene sempre bilateralmente.

#### Tribunale amministrativo federale (TAF)

La Corte I del Tribunale amministrativo federale decide in merito alle richieste del SIC concernenti le misure di acquisizione soggette ad autorizzazione e dell'esplorazione dei segnali via cavo. Sebbene il TAF non sia sottoposto alla vigilanza dell'AVI-Aln, per quest'ultima lo scambio di esperienze con il TAF è importante. Il 30 gennaio 2019 e il 2 ottobre 2019 si sono quindi tenuti scambi di esperienze bilaterali.

### Richieste dei cittadini

Nel 2019 l'AVI-Aln ha ricevuto otto richieste da parte di cittadini. Tra queste vi erano richieste di studenti riguardo alle attività di vigilanza, ma anche richieste di persone che si sentivano disturbate o minacciate da presunte attività informative. L'AVI-Aln può integrare le informazioni ottenute nella sua attività di verifica. Ad esempio può verificare se un'azione descritta può essere imputata a un servizio informazioni e, in caso affermativo, se la legalità è stata garantita. Così, le informazioni ottenute attraverso l'input dell'associazione «grundrechte.ch» sono state prese in considerazione e integrate nel controllo 19-15 a (GEVER SIC). L'AVI-Aln non è però un organo di ricorso, ragion per cui non è autorizzata a fornire informazioni a una singola persona in merito a eventuali elementi che riguardano la persona stessa. È possibile chiedere all'IFPDT se eventuali dati concernenti singole persone sono trattati in modo lecito e se il differimento della comunicazione è giustificato.

Nel 2019 la direzione dell'AVI-Aln si è trovata per uno scambio di opinioni con le persone seguenti:

- capo del DDPS (19 marzo, 29 agosto)
- segretario generale DDPS (6 maggio)
- direttore del SIC (12 marzo, 11 giugno, 4 ottobre e 29 novembre)
- capo del SIM (12 febbraio, 28 giugno e 1° ottobre)
- capo COE (9 gennaio)
- IFPDT (16 gennaio)

### 7.2 Contatti internazionali

In linea di principio le competenze degli organi di vigilanza dei servizi informazioni finiscono al confine nazionale, anche se i dati e le informazioni tra gli stessi servizi sono scambiati in modo transfrontaliero. La cooperazione internazionale tra i servizi è all'ordine del giorno ed è particolarmente intensa tra i servizi partner. Lo scambio internazionale è quindi importante anche per gli organi di vigilanza. Con lo scambio di esperienze e metodi di controllo e con il confronto dei risultati e delle conclusioni ottenuti, le autorità di vigilanza possono sviluppare una migliore comprensione reciproca e per il lavoro quotidiano.

## «Essere trasparenti non significa condividere ogni dettaglio.»

### Oversight Network Meeting all'Aia, Bruxelles e Copenhagen

#### L'Aia, 24 gennaio 2019

I rappresentanti delle autorità di vigilanza sui servizi informazioni di Belgio, Danimarca, Paesi Bassi, Norvegia e Svizzera hanno discusso all'Aia in merito alle possibilità di progetti di vigilanza comuni che prevedono, tra l'altro, l'impiego di cosiddetti dati PNR<sup>18</sup> da parte dei servizi informazioni. L'AVI-AIn non ha partecipato attivamente al progetto, ma ha potuto approfittare dello scambio. Inoltre le autorità di vigilanza hanno discusso sulle innovazioni nel campo della vigilanza tecnica ed elettronica. Concretamente si è trattato ad esempio di valutare in che modo i servizi di intelligence possono vigilare efficacemente sui sistemi di informazione.

#### Bruxelles, 7 marzo 2019

Oltre ai rappresentanti menzionati dell'incontro dell'Aia, a Bruxelles si sono uniti alla rete di vigilanza due rappresentanti della vigilanza britannica. Tutte le delegazioni erano unanimi sul fatto che la collaborazione futura richiede una crescita equilibrata e ragionevole in relazione al numero di membri della rete e una certa frequenza degli incontri internazionali. Oltre alla composizione della rete, i partecipanti hanno discusso di un metodo di vigilanza denominato «vigilanza basata sul sistema». Lo scopo di questo metodo non è sostituire altre forme classiche di vigilanza come l'inchiesta approfondita. Il vantaggio di una vigilanza basata sul sistema è che si fonderebbe su uno standard di verifica internazionale che deve ancora essere creato. Questo potrebbe facilitare la collaborazione. Non significa tuttavia che la vigilanza basata sul siste-

ma non possa essere adeguata alle particolarità nazionali. In alcune parti delle sue verifiche, ad esempio nella verifica 18-10 «Panoramica sulle misure di riduzione dei rischi presso il SIC (incluso il controllo del SICant da parte del SIC)», l'AVI-AIn ha già applicato una vigilanza basata sul sistema. In futuro questo tema sarà portato avanti dalla rete.

#### Copenaghen, 27 giugno 2019

In questa occasione la rete ha portato avanti i suoi sforzi in ambito di vigilanza basata sul sistema e ha discusso di possibili standard comuni per questo tipo di vigilanza. Sulla base di esempi concreti, i partecipanti si sono scambiati le loro esperienze e le «best practices», in particolare nei settori della valutazione dei rischi, dell'illustrazione dell'infrastruttura IT e dei dati o delle soluzioni tecniche per la vigilanza. Le autorità di vigilanza partecipanti hanno discusso in quattro workshop possibili norme comuni in questi settori. Per la prima volta erano rappresentate nella rete le autorità di vigilanza di Germania e Svezia con statuto di osservatrici.

#### European Intelligence Oversight Conference 2019, L'Aia, 12 dicembre 2019,

La conferenza di vigilanza europea si è tenuta all'insegna del motto «Rafforzamento della vigilanza sulla collaborazione internazionale in materia di intelligence». I partecipanti hanno sollevato temi come le future sfide per la vigilanza internazionale sui servizi informazioni o sugli standard nella vigilanza multilaterale.

#### Altri contatti

Il 7-8 novembre 2019 alcuni collaboratori dell'AVI-AIn hanno inoltre partecipato al 3° simposio sul diritto dei servizi informazioni – Servizi informazioni nell'architettura di sicurezza interconnessa, tenutosi a Berlino.

<sup>18</sup> I dati PNR, ossia dati del codice di prenotazione, sono informazioni fornite dai passeggeri dei voli e quindi dati riferiti a persone rilevati e memorizzati dalle compagnie aeree. Queste serie di dati comprendono ad esempio il nome del passeggero, l'indirizzo e-mail, la data di nascita, informazioni sul passaporto, date concernenti il viaggio o l'itinerario del viaggio.

## 8. Vista esterna

Nel rapporto di attività si dà spazio anche a un punto di vista esterno. Martin Stoll ci illustra il suo punto di vista sulla tematica della trasparenza.

### Incontri segreti

Spesso i miei informatori non lesinavano certo sugli sforzi. Gli incontri segreti si svolgevano secondo un copione definito nei dettagli. Quando dovevo recarmi al luogo convenuto venivo sorvegliato (nessuno doveva seguirmi). Talvolta trovavo documenti in una cassetta anonima. Un'altra volta ho dovuto camminare a lungo in un bosco oppure percorrere un tragitto interminabile in automobile. Si definivano nomi in codice e canali di comunicazione. Era un po' come essere in un film.

A giusta ragione i miei informatori erano prudenti. I collaboratori dei servizi segreti e dei servizi informazioni svizzeri avrebbero perso il posto o addirittura la pensione, se si fossero scoperti i nostri contatti.

In questo modo è stato portato alla luce il caso del Sudafrica in cui fu coinvolto l'ex Servizio informazioni strategico. All'insaputa della diplomazia svizzera, che si impegnava per porre fine al regime dell'apartheid, militari svizzeri intrattennero relazioni discutibili con i servizi segreti sudafricani. Si è così scoperto che un pilota del Comitato Internazionale della Croce Rossa (CICR) fu assunto quale spia in Angola dal servizio informazioni svizzero. Oppure è stato possibile confermare che durante l'occupazione dell'ambasciata della Polonia a Berna del 1982, il servizio di intelligence aveva sottratto atti concernenti lo spionaggio in un'azione illegale secondo il diritto internazionale pubblico.

Si è trattato di operazioni molto scottanti a livello politico che mostrano come il servizio informazioni, allora aggregato al Dipartimento militare federale, non avesse pressoché nessun tabù.

In anni più recenti mi è stato illustrato come un informatico del Servizio delle attività informative della Confederazione (SIC) abbia copiato enormi quantità di informazioni confidenziali e segrete. Solo all'ultimo istante, l'uomo, che si sentiva oggetto di mobbing e voleva vendere i dati, è stato fermato su suggerimento di una grande banca. Mi è stato comunicato che il SIC aveva sospeso temporaneamente un collaboratore di lunga data. Si è trattato dell'inizio del caso concernente l'agente infiltrato privato zurighese Daniel M., incaricato dal servizio informazioni svizzero di spiare le autorità tedesche delle finanze.

### Per i giornalisti gli scandali che riguardano i servizi segreti sono una manna

Nella maggior parte dei casi gli autori delle indiscrezioni erano mossi da motivi rispettabili. Si trattava di persone che si preoccupavano «del servizio». Secondo questi informatori qualcosa stava andando storto, ma non c'era nessuno per porre rimedio.

Dopo i titoli dei media si susseguivano di volta in volta indagini e rapporti della vigilanza parlamentare, contribuendo a riportare alla normalità elvetica i processi usciti dai binari. Per i



Da 35 anni **Martin Stoll** (nato in 1962) lavora quale giornalista investigativo. In veste di reporter per la «Tages-Anzeiger», negli anni Novanta si è infiltrato nell'ambiente a luci rosse zurighese, dove si è imbattuto in una connection segreta tra il servizio di intelligence svizzero e l'ex regime dell'apartheid in Sudafrica. Per la «Sonntagszeitung» ha creato il desk investigativo. Inoltre è fondatore e direttore della piattaforma sulla trasparenza «Öffentlichkeitsetz.ch», corrispondente dall'Amministrazione federale per la «Sonntagszeitung», formatore nell'ambito del giornalismo investigativo e vicepresidente dell'associazione dei giornalisti «investigativ.ch».

servizi segreti che (a ragione) operano sovente ai limiti della legalità, è un procedimento necessario e importante.

Per un giornalista, le informazioni interne che mi venivano confidate erano una manna. In Svizzera la gestione dell'indignazione nei casi concernenti i servizi segreti è semplice. Già in merito agli scandali più innocui che coinvolgono agenti, i lettori sono molto attenti e non possono trattenersi dallo scuotere la testa: «Che cos'hanno di nuovo combinato quelli del servizio informazioni?».

Si potrebbe qui rimproverare agli operatori dei media di agire per motivi disonesti: interesse personale, massimizzazione della tiratura, scandali inutili. Naturalmente vogliamo avere successo, anche presso il nostro pubblico. Tuttavia è anche il nostro compito e la nostra passione, osservare, chiarire le zone d'ombra e portare alla luce eventuali irregolarità.

Nel frattempo la strategia che il servizio segreto svizzero ha sviluppato per trattare l'opinione pubblica critica si è rivelata sbagliata. Oggi il SIC fa di tutto per evitare di fare scalpore. Se ne sta in disparte, osserva e agisce impotente quando viene a trovarsi sotto la luce dei riflettori. Dovrebbe invece chiedersi senza esitazione: perché quando succede qualcosa veniamo messi così rapidamente con le spalle al muro? Perché le ondate non si appianano neanche con spieazioni ragionevoli?

Quando vengono alla luce casi e scandali risulta palese che, anche a distanza di trent'anni dall'affare delle schedature, il servizio informazioni svizzero non è riuscito a migliorare nel suo datore di lavoro – la popolazione – la comprensione per il suo operato. L'opinione pubblica non sa perché il servizio informazioni è valido, quali sono i suoi compiti, i suoi vantaggi e il suo margine d'azione.

Anche la politica miope del SIC in materia di trasparenza degli ultimi anni ha le sue colpe. La promessa del consigliere federale Adolf Ogi, che dopo l'affare del contabile dei servizi segreti Dino Bellasi del 2001 aveva dichiarato «Glasnost nel Pentagono», è rimasta sino ad oggi una «barzelletta» politica.

#### **L'eccessivo timore nei confronti dell'opinione pubblica danneggia la reputazione**

Le cifre riguardanti l'attuazione della legge sulla trasparenza (LTras) evidenziano che la trasparenza nel servizio segreto elvetico è un elemento marginale. La legge offre la possibilità ai cittadini e quindi anche ai giornalisti di consultare documenti dell'Amministrazione. Obiettivo della legge è promuovere la comprensione dell'opinione pubblica per il lavoro dell'Amministrazione.

Anche il SIC sottostà a questa legge. Dal 2012 fino al 2018 complessivamente 62 giornalisti, organizzazioni non governative e cittadini hanno inoltrato al SIC domande di accesso. Solo per otto domande il SIC ha autorizzato l'accesso completo ai documenti. In 33 casi il servizio giuridico del SIC ha respinto totalmente la domanda. Nell'ottica del cittadino e dei media si tratta di un bilancio estremamente povero.

Per comprendere la politica di trasparenza del SIC, nel 2014 ho chiesto sulla base della LTras di poter consultare le domande di accesso inoltrate al SIC negli ultimi tre anni. L'aspetto positivo è che ho ricevuto i documenti richiesti in forma anonima. Quello negativo è che la maggior parte delle 16 domande di accesso sono state rifiutate con l'osservazione standard secondo cui la sicurezza interna o esterna della Svizzera sarebbe minacciata in caso di pubblicazione.

Se il servizio segreto si pone sistematicamente nell'ombra e blocca qualsiasi accesso, lede la sua reputazione. Ne è la conferma l'esempio tratto dalla serie di domande che ho potuto esaminare e che concerne un tema che ben conosco. 23 anni dopo la caduta del muro di Berlino un richiedente ha chiesto l'accesso al «Dossier Walter B.». B alias «Max» è stata una delle più importanti spie della Svizzera durante la Guerra fredda. L'allora autista presso l'ambasciata della RDT fu reclutato dal controspionaggio dopo che era stato preso con le mani nel sacco in occasione di un furto in un grande magazzino bernese. In seguito B. ha permesso alla Svizzera per diversi anni di osservare in dettaglio le operazioni dei servizi segreti dell'Est. Nonostante «Max» mi abbia raccontato la sua storia durante lunghi colloqui, nonostante atti e video della sicurezza dello Stato della RDT a Berlino siano accessibili (più tardi «Max» è stato arrestato e condannato a Berlino Est), il SIC ha rifiutato l'accesso al richiedente. Così facendo ha perso l'occasione di contribuire all'elaborazione di un'interessante pezzo della storia recente e di legittimare in tal modo il rischioso lavoro dei servizi.

L'atteggiamento generalmente schivo nei confronti dell'opinione pubblica è emerso anche quando il SIC ha preteso per l'ambito operativo la deroga al principio di trasparenza nella nuova legge sulle attività informative. Un atteggiamento totalmente inutile (i segreti possono essere tutelati efficacemente anche con la LTras) e anche un'altra opportunità mancata: affinché possa spiegare in modo plausibile il proprio lavoro, in linea di principio il SIC non dovrebbe operare segretamente, bensì per quanto possibile in modo trasparente.

Se ciò non sarà il caso, anche in futuro il servizio segreto verrà giudicato unicamente per i suoi insuccessi e fallimenti. La cultura di una classificazione eccessiva oggi propugnata, presto o tardi avrà un nuovo effetto boomerang, perché una cosa è scontata: il prossimo scandalo dei servizi segreti è una certezza.

## 9. Cifre al 31 dicembre 2019



### Collaboratori

1.1.2019	9
31.12.2019	10
Disdette	0



### Verifiche

Verifiche previste	21
Verifiche senza preavviso	0
Verifiche effettuate	19



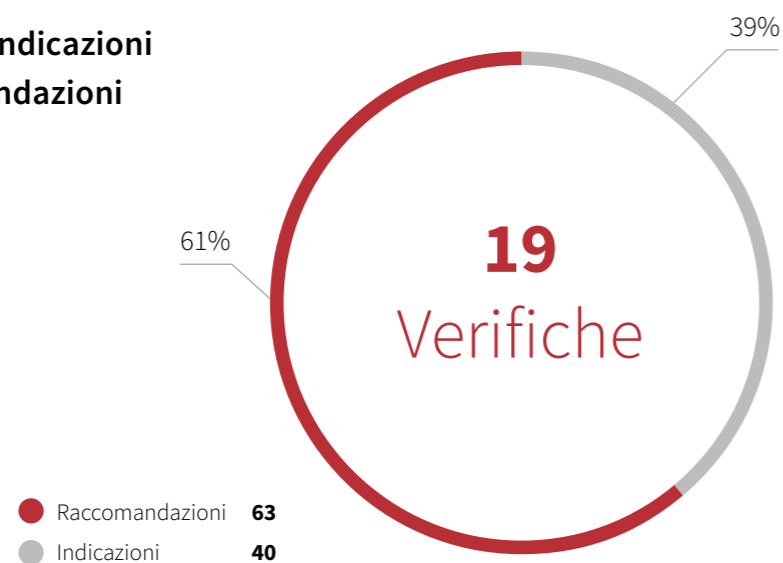
### Numero di interviste effettuate nel 2019

119

### Effettivo di personale preventivato

10 posti

### Verifiche, indicazioni e raccomandazioni



## 10. Allegato

### 10.1 Piano di controllo 2019

N.	Titolo	Organo controllato
19-1	Strategia di difesa dallo spionaggio	SIC
19-2	Gestione delle informazioni d'intelligence tra il sensore «addeito alla difesa» e il SIC	SIC
19-3	Controllo SICant GE	SICant GE
19-4	Controllo SICant JU	SICant JU
19-5	Controllo SICant GR	SICant GR
19-6	Controllo SICant SH	SICant SH
19-7	Controllo SICant BE	SICant BE
19-8	Adeguatezza ed efficacia delle misure di acquisizione soggette ad autorizzazione	SIC
19-9	Attuazione delle misure di acquisizione soggette ad autorizzazione	SIC
19-10	Operazioni	SIC
19-11	Fonti umane (HUMINT)	SIC
19-12	Protezione delle fonti in seno al SIC focalizzandosi sulla copertura e l'identità fittizia	SIC
19-13	Processo di reclutamento, di assistenza e di uscita	SIM/COE
19-14	Utilizzo sicuro di videoconferenze	SIC
19-15	Esercizio, contenuto e utilizzo dei sistemi d'informazione GEVER SIC, memorizzazione dei file in BURAUT, memorizzazione dei file in SiLAN (valutazioni temporanee)	SIC
19-16	Classificazioni di informazioni	SIC, SIM, COE
19-17	Ambiente informativo SIM	SIM
19-18	Ambiente informativo COE	COE
19-19	Strumenti per l'analisi di dati al COE	COE
19-20	Comunicazione di dati personali ad autorità estere (art. 61 LAIn)	SIC
19-21	Accesso a/dai sistemi d'informazione di terzi (Confederazione, Cantoni, servizi esteri, perseguimento penale)	SIC
19-22	Controlling raccomandato	SIC, SIEs, COE

## 10.2 Elenco delle abbreviazioni

<b>AVI-AIn</b>	Autorità di vigilanza indipendente sulle attività informative	<b>OAIIn</b>	Ordinanza sulle attività informative (OAIIn; RS 121.1)
<b>ACI</b>	Autorità di controllo indipendente per l'esplorazione radio e l'esplorazione dei segnali via cavo	<b>per es.</b>	per esempio
<b>art.</b>	articolo	<b>RDT</b>	Repubblica democratica tedesca
<b>BAC</b>	Base d'aiuto alla condotta	<b>RS</b>	Raccolta sistematica del diritto federale
<b>BE</b>	Berna	<b>SEM</b>	Segreteria di Stato della migrazione
<b>BURAUT</b>	sistema di memorizzazione dei file del SIC	<b>SG</b>	Segreteria generale
<b>C</b>	capo	<b>SGSI</b>	Sistema di gestione della sicurezza delle informazioni
<b>CICR</b>	Comitato Internazionale della Croce Rossa	<b>SH</b>	Sciaffusa
<b>COE</b>	Centro operazioni elettroniche	<b>SIC</b>	Servizio delle attività informative della Confederazione
<b>cpv.</b>	capoverso	<b>SICant</b>	Servizio informazioni cantonale
<b>CQ SIC</b>	organo di controllo della qualità del SIC	<b>SiLAN</b>	rete informatica protetta del SIC
<b>CSP</b>	controllo di sicurezza relativo alle persone	<b>SIM</b>	Servizio informazioni militare
<b>DDPS</b>	Dipartimento federale della difesa, della protezione della popolazione e dello sport	<b>TAF</b>	Tribunale amministrativo federale
<b>DeICG</b>	Delegazione delle Commissioni della gestione	<b>WEF</b>	World Economic Forum (Forum mondiale dell'economia) di Davos
<b>DFAE</b>	Dipartimento federale degli affari esteri		
<b>DFGP</b>	Dipartimento federale di giustizia e polizia		
<b>ecc.</b>	eccetera		
<b>GE</b>	Ginevra		
<b>GEVER</b>	sistema di gestione degli affari: termine generico per il sistema elettronico di gestione degli affari in uso nell'Amministrazione federale		
<b>GR</b>	Grigioni		
<b>HUMINT</b>	Human Intelligence, acquisizione di informazioni tramite fonti umane		
<b>IFPDT</b>	Incaricato federale della protezione dei dati e della trasparenza		
<b>JU</b>	Giura		
<b>LAIIn</b>	Legge federale sulle attività informative (LAIIn; RS 121)		
<b>LTras</b>	Legge federale sul principio di trasparenza dell'amministrazione (LTras; RS 152.3)		



**Autorità di vigilanza indipendente sulle  
attività informative**

Maulbeerstrasse 9, 3003 Berna  
Telefono +41 58 464 20 75  
[www.ab-nd.admin.ch](http://www.ab-nd.admin.ch)