Sicurezza informatica in seno al Servizio delle attività informative della Confederazione

Rapporto della Delegazione delle Commissioni della gestione delle Camere federali (riassunto) del 30 agosto 2013

Parere del Consiglio federale

del 30 ottobre 2013

Rapporto

1 Introduzione

1.1 Antefatti

Il Servizio delle attività informative della Confederazione (SIC) esiste nella forma attuale dal 1° gennaio 2010. In precedenza i suoi compiti erano ripartiti tra il Servizio di analisi e prevenzione (SAP, fino a fine 2008 accorpato al DFGP) e il Servizio informazioni strategico (SIS, DDPS). Le sue basi legali si trovano in particolare nella legge federale del 3 ottobre 2008 sul servizio informazioni civile (LSIC; RS *121*) e nella legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI; RS *120*). Queste norme saranno sostituite da una nuova legge sul servizio informazioni, il cui avamprogetto è stato posto in consultazione fino al 30 giugno 2013.

1.2 Sinergie e risorse

Decisione del Consiglio federale del 25 marzo 2009

Il 25 marzo 2009 il Consiglio federale ha incaricato il DDPS «di raggruppare per il 1° gennaio 2010 il Servizio di analisi e prevenzione (SAP) e il Servizio informazioni strategico (SIS) in un unico nuovo Ufficio federale». Nel relativo documento interlocutorio sono state elencate anche le condizioni di attuazione:

1. attuazione in tempo utile;
2. attuazione nell'ambito della vigente legislazione;
3. attuazione senza necessità di risorse supplementari;
4. trasparenza e controllo come compito permanente.

Riguardo alla terza condizione è stato puntualizzato quanto segue: «La soluzione ricercata deve essere realizzata senza far capo a risorse supplementari.»

Iniziativa parlamentare Hofmann

Già l'iniziativa Hofmann del 13 marzo 2007 (07.404, Trasferimento dei compiti dei servizi informazioni civili a un dipartimento) rivendicava un incremento dell'efficienza dei servizi di informazione:

«L'iniziativa chiede soltanto l'ottimizzazione dello sfruttamento dei dati raccolti nell'ambito delle attività dei servizi di informazione. Il raggruppamento delle missioni del SAP e del SIS in seno a un unico dipartimento consentirà contemporaneamente di creare sinergie e di garantire l'impiego ottimale delle risorse disponibili.»

Conformemente a questa rivendicazione, anche il Consiglio federale aveva fatto dell'impiego ottimizzato delle risorse disponibili una delle sue preoccupazioni principali, come espresso nel proprio parere del 23 aprile 2008 sul rapporto della Commissione della gestione del Consiglio degli Stati del 29 febbraio 2008 (FF *2008* 3460 seg.).

Come evidenziato dai diversi interventi parlamentari e dibattiti che hanno portato alla creazione del SIC, dal nuovo servizio ci si attendevano soprattutto prestazioni supplementari nel suo campo d'attività principale.

Situazione iniziale del SAP e del SIS prima della fusione nel SIC

La concentrazione di due unità organizzative consente di regola di realizzare effetti sinergici in seguito all'eliminazione di doppioni nelle strutture organizzative. Da questo punto di vista, il SAP e il SIS presentavano premesse sostanzialmente diverse.

L'uno e l'altro disponevano in misura limitata o addirittura non disponevano affatto di funzioni trasversali e di supporto (informatica, servizi centrali, comunicazione, personale, sicurezza, diritto e funzioni di supporto specifiche all'acquisizione di informazioni). Il SAP acquisiva quasi tutte le prestazioni presso i servizi centrali del DFGP e non disponeva di funzioni di supporto proprie. Il SIS disponeva soltanto in parte di funzioni di supporto sufficienti e acquisiva gran parte delle relative prestazioni presso la SG-DDPS. Dopo la fusione, il SIC ha dovuto assicurare autonomamente le necessarie funzioni di supporto attingendo alle risorse disponibili. Per contro, a livello dipartimentale ne è risultato un certo sgravio finanziario.

Il SIC nel piano di attuazione della verifica dei compiti

Nel proprio rapporto del 14 aprile 2010 sul piano di attuazione della verifica dei compiti della Confederazione, il Consiglio federale ha definito le tappe per la realizzazione delle 25 misure a lungo termine affidate ai dipartimenti. Queste tappe sono state aggiornate con l'adozione del messaggio del 1° settembre 2010 concernente la legge federale sul programma di consolidamento 2012–2013. La misura numero 13 riguardava lo «sfruttamento del potenziale di sinergie dei servizi d'informazione civili» e prevedeva che nel 2011 il Consiglio federale avrebbe dovuto decidere in merito all'entità e all'impiego di tale potenziale: «Ne [dalla riunione dei servizi] risultano guadagni in termini di sinergia che devono ancora essere quantificati in modo esauriente e contabilizzati a favore del bilancio della Confederazione.»

In un rapporto confidenziale del 27 maggio 2011, il DDPS indicava al Consiglio federale che la fusione del SAP e del SIS nel SIC aveva consentito di sfruttare sinergie e di realizzare economie interne. A questi vantaggi si contrapponevano però nuovi compiti non finanziati, che il SIC doveva finanziare con i risparmi realizzati. A conti fatti, la Confederazione non realizzava alcun risparmio ma concretizzava l'auspicato incremento dell'efficienza delle attività informative.

Con l'adozione del summenzionato rapporto, il 10 giugno 2011 il Consiglio federale ha espunto il SIC dalla verifica dei compiti.

Dal momento della fusione, l'informatica del SIC ha puntato per forza di cose a garantire il funzionamento di un sistema in continua evoluzione, sia sotto il profilo delle applicazioni e che delle infrastrutture. A tal fine, si è dovuto far capo occasionalmente a fornitori e collaboratori esterni. Nel rapporto summenzionato, il Consiglio federale era stato reso attento anche al fatto che le sinergie realizzate dal 2010 erano impiegate per lo sviluppo delle varie funzioni trasversali.

1.3 Obiettivi del Consiglio federale realizzati

Il Consiglio federale ha accompagnato la creazione del SIC integrandola nei propri obiettivi annuali e presentando i relativi rapporti.

2010: predisposizione delle basi organizzative

Il grosso dei lavori per la creazione del SIC è stato portato a termine nel 2010. Il modello dei processi SIC, la struttura operativa e i processi pilota per la realizzazione di un sistema di gestione delle pratiche sono stati definiti e documentati. I processi normativi sono stati documentati e attuati come previsto dalla pianificazione. Sempre nel 2010, il Consiglio federale ha anche stabilito il seguito dei lavori per quanto concerne la legislazione applicabile al SIC. Il 27 ottobre 2010 ha adottato il messaggio aggiuntivo concernente la modifica della legge federale sulle misure per la salvaguardia della sicurezza interna («LMSI II ridotta»). Il 24 agosto 2010 il capo del DDPS ha approvato la proposta di progetto e il concetto per l'avamprogetto di nuova legge sul servizio informazioni (LSI); il relativo mandato era stato impartito il 27 novembre 2009.

2011: priorizzazione degli ambiti operativi e controlli di qualità

Nel 2011 l'attenzione si è concentrata sulla priorizzazione degli ambiti tematici del nuovo mandato fondamentale del SIC, sull'adeguamento delle basi legali e sull'attuazione delle raccomandazioni della Delegazione delle Commissioni della gestione (DelCG) sui controlli di qualità per il Sistema d'informazione Sicurezza interna (ISIS). La priorizzazione degli ambiti tematici si è conclusa a inizio 2011 con la definizione del nuovo mandato fondamentale da parte del Consiglio federale; l'attuazione delle misure e la liquidazione delle pendenze nel sistema ISIS sono avvenute come previsto ed è stato allestito il concetto normativo per la LSI.

2012: conclusione dell'attuazione delle misure previste dal rapporto ISIS della DelCG – Strategia nazionale per la protezione della Svizzera contro i rischi informatici.

Nel 2012 sono state attuate le misure necessarie (adeguamento di ordinanze, istruzioni e prescrizioni organizzative) per l'attuazione della LMSI II, entrata in vigore il 16 luglio 2012. Le misure raccomandate nel rapporto ISIS della DelCG sono state pienamente attuate. Il SIC ha fornito un apporto sostanziale anche alla definizione della Strategia nazionale per la protezione della Svizzera contro i rischi informatici, approvata dal Consiglio federale il 27 giugno 2012.

2013: messaggio per una nuova legge sul servizio informazioni

Nel 2013 il SIC si è di nuovo concentrato sulle attività legiferative, occupandosi della preparazione del messaggio sulla nuova LSI (in consultazione fino a fine giugno) e del messaggio sulla revisione parziale della LSIC. Quest'ultimo è stato adottato dal Consiglio federale il 14 agosto 2013. La revisione parziale della LSIC è intesa a consentire al SIC di mantenere in funzione la banca dati ISAS, contenente informazioni di provenienza estera importanti per la politica di sicurezza, anche oltre la scadenza del giugno 2015 qualora la nuova LSI non entrasse in vigore entro quella data.

1.4 Liquidazione di pendenze delle organizzazioni preesistenti

La costituzione del SIC rispondeva sin dal principio anche alla preoccupazione di smaltire varie pendenze accumulate dalle preesistenti organizzazioni.

Revisione della LMSI

La revisione della LMSI («LMSI II ridotta»), per la quale il Consiglio federale aveva elaborato un messaggio aggiuntivo licenziato il 27 ottobre 2010, si è conclusa il 23 dicembre 2011 con la votazione finale del Parlamento, dopo circa un decennio di lavori.

Pendenze nel trattamento dei dati nel sistema ISIS

Subito dopo la creazione del SIC si è manifestata un'urgente necessità di intervento in rapporto con i ritardi accumulati nei controlli di qualità sul trattamento dei dati nel sistema ISIS. Il 21 giugno 2010 la DelCG ha pubblicato un rapporto d'ispezione al riguardo. Nel proprio parere del 20 ottobre 2010, il Consiglio federale ha sostanzialmente accettato tutte le raccomandazioni. Il SIC ha predisposto le necessarie misure per risolvere al più presto la situazione. Nel proprio rapporto di gestione 2012, il Consiglio federale ha potuto annunciare che i lavori di rettifica dei dati, che in base al rapporto della DelCG andavano sottoposti a una verifica globale ordinaria, si sono conclusi il 5 dicembre 2012. L'ex consigliere agli Stati Hansruedi Stadler, delegato dal DDPS come incaricato esterno della protezione dei dati, ha confermato che le pendenze accumulatesi nel controllo delle registrazioni e nella verifica globale dei dati sono state interamente liquidate.

1.5 Sfide per il SIC dovute alle contingenze

Dal 2010 il SIC si trova confrontato, in quanto servizio che raggruppa le attività informative concernenti l'estero e la Svizzera, a diverse sfide dovute all'evoluzione della situazione.

Mutamento delle priorità nell'ambito dell'acquisizione e dell'analisi

Sebbene la Svizzera non rappresenti tuttora un obiettivo primario dichiarato di attentati di matrice jihadista, negli ultimi tre anni diversi nostri concittadini sono rimasti vittime all'estero di rapimenti con moventi politici o terroristici. In seguito ai violenti sconvolgimenti politici che hanno investito i Paesi arabi e nordafricani, si è inoltre constatato, in Europa ma anche in Svizzera, un aumento dei viaggi con finalità jihadiste.

Negli ultimi tre anni, con l'inasprirsi della situazione nel Medio Oriente, in Svizzera si è registrata un'intensificazione degli sforzi compiuti da alcuni Paesi per procurarsi illecitamente beni a duplice impiego da utilizzare per lo sviluppo e la fabbricazione di armi di distruzione di massa e dei relativi vettori. Sono diventate prioritarie anche la prevenzione e la difesa da attacchi alle infrastrutture informatiche critiche. Si constata pure un incremento delle attività di spionaggio da parte di servizi informazioni esteri nei confronti degli oppositori stranieri in Svizzera a regimi dittatoriali e

delle attività di acquisizione illegale di informazioni sulla piazza scientifica, industriale, finanziaria e commerciale svizzera, con predilezione per il ricorso ad attacchi informatici.

Adeguamento delle capacità

Il Consiglio federale prende atto che il SIC ha adottato una serie di misure per affrontare le nuove sfide risultanti dal mutamento della situazione:

- dal 2010 il SIC, in collaborazione con i Cantoni, adegua regolarmente il proprio programma di prevenzione PROPHYLAX per sensibilizzare in merito alla minaccia rappresentata dalla proliferazione e dallo spionaggio economico. Il programma si rivolge alle imprese potenzialmente a rischio e agli istituti di ricerca e formazione e interessa oltre 1800 ditte e 100 istituti di ricerca in Svizzera e nel Principato del Liechtenstein. A fine settembre 2013 è stata contattata la millesima ditta;
- dal 2011 il SIC esegue, in collaborazione con la Polizia giudiziaria federale, un monitoraggio del jihadismo. Il 10 giugno 2010, nell'ambito dell'attuazione della mozione Büchler (07.3751), il Consiglio federale ha affidato al SIC l'incarico di assicurare le attività di osservazione di siti Internet jihadisti;
- nel 2012, con la presentazione della situazione comune, il SIC ha allestito per la prima volta in forma elettronica una panoramica nazionale che funge da base per una valutazione costantemente aggiornata della situazione nel settore dell'estremismo violento. Dopo l'introduzione della pertinente base legale nella LMSI, è stato quindi possibile soddisfare una richiesta dei Cantoni di lunga data;
- sempre nel 2012, il SIC ha partecipato, con l'unità informativa della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, all'elaborazione di una Strategia nazionale per la protezione della Svizzera contro i rischi informatici. Il 27 giugno 2012 il Consiglio federale ha approvato un documento di base in tal senso, esaudendo in tal modo quanto richiesto da diversi interventi parlamentari;
- il 1° maggio 2013 il Consiglio federale ha approvato il disciplinamento dei compiti, delle competenze e delle responsabilità dei servizi del DFAE, del DFGP e del DDPS implicati nella soluzione dei casi di rapimento. In tale contesto, il SIC ha il compito di monitorare gli sviluppi, di provvedere all'analisi e all'aggiornamento della rappresentazione della situazione nonché di fornire prestazioni operative.

Collaborazione mirata con partner in Svizzera e all'estero

Nei primi tre anni di attività, il SIC ha allacciato e sviluppato in modo mirato rapporti di collaborazione con partner in Svizzera e all'estero.

I partner del SIC in Svizzera sono soprattutto i Cantoni e, a livello di Confederazione, i servizi federali rappresentati in seno al Comitato ristretto Sicurezza. La collaborazione con i Cantoni è stata rafforzata con l'introduzione di nuovi programmi di formazione, la definizione di requisiti per i controlli di qualità e una nuova regola-

mentazione in materia di sorveglianza degli organi cantonali preposti alla protezione dello Stato.

Sul fronte della collaborazione con servizi esteri, il SIC ha focalizzato la propria attenzione sui partner che adempiono compiti ai sensi della LMSI e/o della LSIC. La politica praticata dal SIC nei confronti dei servizi partner è sottoposta annualmente al Consiglio federale per approvazione.

2 Misure adottate dal Consiglio federale dopo l'incidente

2.1 Verifiche e rapporti del capo del DDPS

Il 22 aprile 2013 il DDPS ha presentato al Consiglio federale un rapporto che illustra le circostanze in cui è avvenuto il trafugamento di dati e le successive misure avviate o previste. Nel rapporto si constata che nessun dato è finito in possesso di persone non autorizzate. Senza le rapide e decise reazioni susseguitesi internamente ed esternamente all'Amministrazione, dati dell'intelligence avrebbero potuto essere trasmessi a terzi – in Svizzera o all'estero – oppure diventare di pubblico dominio.

Il rapporto precisa inoltre che subito dopo i fatti, il DDPS e il SIC hanno adottato senza indugio le necessarie decisioni in materia di condotta. Diversi organi e gruppi di periti interni ed esterni all'Amministrazione sono stati incaricati di analizzare la situazione e di individuare le misure necessarie. Nella propria sfera di competenza, il SIC ha individuato e avviato 40 misure sia a livello tecnico e organizzativo sia nell'ambito delle limitazioni dei diritti di accesso e degli accessi fisici.

Il Consiglio federale ha successivamente trasmesso il rapporto del DDPS per conoscenza alla DelCG e il DDPS ha provveduto a pubblicarlo il 30 aprile 2013.

2.2 Aumento dell'effettivo del personale negli ambiti dell'informatica e della sicurezza

Oltre ad elaborare il rapporto summenzionato, con istanza del 26 aprile 2013 il DDPS ha chiesto al Consiglio federale di aumentare l'effettivo del personale addetto all'informatica e alla sicurezza del SIC.

Con decisione del 1° maggio 2013, il Consiglio federale ha preso atto che il necessario e vitale aumento della sicurezza e della sicurezza informatica in seno al SIC comporterà un maggior fabbisogno di personale quantificabile in otto posti a partire dal 2014 e in ulteriori tre posti a partire dal 2015. Nel quadro della valutazione complessiva delle risorse di personale per il 2013, il 26 giugno 2013 ha quindi accolto l'istanza del DDPS assegnandogli otto nuovi posti a partire dal 2014. Il DDPS ha autorizzato già nel corso del primo semestre 2013 l'immediato finanziamento di questi otto posti attingendo alle riserve del Dipartimento.

L'attribuzione dei posti supplementari consentirà di colmare ampiamente le lacune critiche per la sicurezza facendo capo a collaboratori interni e di realizzare i progetti di migrazione accumulati. Nell'ambito della sicurezza informatica e d'esercizio potranno essere acquisite capacità mancanti e realizzate ridondanze. Sarà quindi

possibile rispettare il principio del doppio controllo, in particolare in attività particolarmente delicate, durante gli orari d'esercizio ampliati.

2.3 Misure del DFF per l'informazione e la formazione dei quadri dell'Amministrazione federale

Il 15 marzo 2013, in seguito all'avvenuto trafugamento di dati, il Consiglio federale ha incaricato il DFF di attuare misure per l'informazione e la formazione dei quadri dell'Amministrazione federale sulle questioni di sicurezza delle informazioni. Ulteriori miglioramenti sul fronte della sicurezza saranno introdotti con una nuova legge sulla sicurezza delle informazioni (LSIn), il cui progetto è in corso di elaborazione sotto l'egida del DDPS. Secondo i piani attuali, la procedura di consultazione sulla LSIn dovrebbe essere avviata nel gennaio 2014.

Il Consiglio federale riconosce dunque le necessità di intervento che risultano dalle raccomandazioni della DelCG, e in particolare la necessità di misure per il miglioramento della sicurezza informatica e la gestione dei rischi. Decidendo di potenziare gli effettivi nel settore dell'informatica e della sicurezza, ha anche compiuto i passi necessari per incrementare la sicurezza del Servizio delle attività informative.

3 Osservazioni sulle raccomandazioni della DelCG

In merito alle singole raccomandazioni il Consiglio federale si esprime come segue:

Raccomandazione 1

La DelCG raccomanda al Consiglio federale di incaricare il DDPS di eseguire un'analisi approfondita e dettagliata delle risorse di personale necessarie per l'adempimento degli ulteriori compiti previsti dalla nuova legge sul servizio informazioni.

Nel suo messaggio sulla nuova legge sul servizio informazioni (LSI), il nostro Collegio illustrerà le ripercussioni finanziarie e sull'effettivo del personale generate dalle singole nuove misure. Alle carenze riscontrate dopo il furto di dati nell'ambito della sicurezza informatica sarà posto rimedio mediante le misure decise il 1° maggio 2013. Nonostante l'entrata in vigore della nuova legge sul servizio informazioni, il SIC continuerà tuttavia a disporre, nel confronto internazionale, di risorse molto limitate e dovrà pertanto definire delle priorità.

Raccomandazione 2

La DelCG chiede al Consiglio federale di assicurarsi che, entro giugno 2014, il DDPS gli riferisca sullo stato della gestione dei rischi in seno al SIC e illustri in che modo il SIC applica adeguatamente le disposizioni della Confederazione in materia.

Il nostro Collegio aderisce alla raccomandazione; la relativa concretizzazione è già in corso. Il 9 gennaio 2013 il capo del DDPS ha incaricato la Vigilanza sulle attività informative di valutare costantemente l'impostazione della gestione dei rischi in seno al SIC e le relative misure. Su tale base il Consiglio federale è in grado di garantire che il SIC concretizza adeguatamente le suddette disposizioni.

Raccomandazione 3

La DelCG chiede al DDPS di provvedere affinché l'incaricato della sicurezza informatica del Dipartimento verifichi entro la fine del 2014 che tutte le applicazioni e i sistemi del SIC siano corredati di un valido concetto di sicurezza che preveda una valutazione dei rischi fondata e completa. Per rimediare a eventuali carenze sarà elaborato un piano di provvedimenti vincolante.

Il nostro Collegio condivide il parere della DelCG secondo cui le applicazioni e i sistemi del SIC debbano essere corredati di un valido concetto di sicurezza che preveda una valutazione dei rischi fondata e completa. È stato allestito un inventario completo degli oggetti da proteggere. Su tale base il SIC elaborerà prossimamente, in coordinamento con l'incaricato della sicurezza informatica del DDPS, un piano di provvedimenti per ogni oggetto da proteggere. Il Consiglio federale aderisce pertanto alla raccomandazione.

Raccomandazione 4

La DelCG chiede al Consiglio federale di incaricare il DDPS di verificare entro la fine del 2013 se la disposizione dell'articolo 7 capoverso 1 OSI-SIC relativa alla crittazione del SiLAN può essere applicata in modo che gli oneri siano proporzionati agli utili per la sicurezza informatica del SIC. In base al risultato di questo esame la disposizione dovrà essere applicata in tempo utile o altrimenti immediatamente abrogata.

Il nostro Collegio aderisce alla raccomandazione concernente la crittazione del SiLAN. La formulazione presente nell'articolo 7 capoverso 1 OSI-SIC relativa alla crittazione è stata redatta sulla base di una svista legislativa che non era stata rilevata nel corso dell'elaborazione dell'ordinanza. Ciononostante, in seguito al furto di dati, la crittazione del SiLAN è stata presa in considerazione dal SIC quale futura misura auspicabile per un incremento della sicurezza informatica. Nel corso della pianificazione della concretizzazione è tuttavia risultato che i vantaggi supplementari derivanti dalla crittazione sarebbero stati del tutto sproporzionati rispetto ai corrispondenti oneri e ai rischi per la sicurezza informatica: una crittazione totale avrebbe richiesto infatti un massiccio incremento delle prestazioni di carattere tecnico, con corrispondenti costi. Di conseguenza la misura è stata respinta. Nei mesi di agosto e settembre 2013, il SIC ha svolto la consultazione degli uffici relativa alla prevista modifica della OSI-SIC, nel cui quadro il SiLAN è menzionato correttamente come una piattaforma autonoma e protetta, parzialmente cifrata nell'ambito delle vie di trasmissione. È possibile che in futuro, grazie a ulteriori progressi tecnici, la crittazione totale diventi un'opzione realistica.

Raccomandazione 5

La DelCG raccomanda al Consiglio federale di fare in modo che, mediante una revisione della OCSP, vengano definite per i collaboratori esterni le stesse condizioni di CSP degli impiegati della Confederazione che assolvono compiti identici. Il servizio federale che è il destinatario finale della prestazione fornita da aziende e collaboratori esterni si assume la responsabilità di far loro osservare le pertinenti disposizioni.

L'OCSP vigente è già conforme all'esigenza che per i collaboratori esterni (terzi) siano definite le stesse condizioni di CSP degli impiegati della Confederazione che assolvono compiti identici. A seconda dell'accesso previsto, possono essere svolti per la verifica di terzi sia controlli di sicurezza di base (art. 10 cpv. 2 OCSP) sia controlli di sicurezza ampliati (art. 11 cpv. 2 OCSP) oppure controlli di sicurezza ampliati con audizione (art. 12 cpv. 1 OCSP). Non si è pertanto in presenza di una lacuna giuridica: la questione si situa piuttosto al livello dell'applicazione delle disposizioni vigenti.

All'articolo 14 capoverso 1 lettera c OCSP è stabilito che «per i terzi che partecipano a progetti classificati a partire dal livello di classificazione CONFIDENZIALE» ad essere competenti per l'avvio di un controllo di sicurezza relativo alle persone sono «l'autorità che conferisce il mandato e le imprese titolari di un valido attestato di sicurezza nel quadro della procedura di tutela del segreto». Ogni servizio che conferisce a terzi un mandato classificato a partire dal livello di classificazione CONFIDENZIALE è pertanto competente per l'avvio di un controllo di sicurezza relativo alle persone di livello adeguato.

Gli organi della Confederazione competenti per l'avvio di un controllo di sicurezza relativo alle persone secondo l'articolo 14 capoverso 1 OCSP sono inoltre connessi al Sistema informatizzato per i controlli di sicurezza relativi alle persone (SIBAD) di cui agli articoli 144 segg. della legge federale sui sistemi d'informazione militari (LSIM; RS *510.91*), gestito dal servizio specializzato CSP DDPS (al riguardo vedasi l'art. 148 cpv. 1 lett. c LSIM). Pure gli uffici della Confederazione incaricati di compiti di sicurezza nel quadro dell'OCSP sono per la maggior parte connessi al SIBAD o possono ottenere, previa richiesta, un accesso al sistema conformemente all'articolo 148 capoverso 1 lettera d LSIM. Mediante procedura di richiamo, gli organi connessi al SIBAD possono verificare nel sistema se terzi sono stati oggetto di controlli, a quale livello si situano i controlli svolti e se quest'ultimi sono ancora valevoli. Ciò fornisce agli uffici la necessaria visione d'insieme e consente loro di avviare, se necessario, un nuovo controllo di sicurezza relativo alle persone.

Il nostro Collegio sottolinea pertanto che, per quanto concerne i controlli di sicurezza relativi alle persone nei confronti di terzi, sussistono chiare basi giuridiche e che anche per quanto riguarda le corrispondenti responsabilità non sono di principio necessari ulteriori chiarimenti. In via complementare, i dipartimenti e la Cancelleria federale provvederanno a sensibilizzare al riguardo i rispettivi servizi competenti.

Raccomandazione 6

La DelCG raccomanda al Consiglio federale di spiegare in modo dettagliato nel suo messaggio concernente la legge sulla sicurezza delle informazioni quali ruoli rivestono il controllo di sicurezza relativo alle persone e la gestione del personale nell'ambito della sicurezza informatica e di differenziarli chiaramente l'uno dall'altro. Parallelamente, in un rapporto separato deve essere fornita una stima delle risorse di personale che la Confederazione dovrebbe impiegare per l'esecuzione dei CSP e una descrizione del contributo che essa intende apportare alla protezione delle informazioni.

Il nostro Collegio è disposto a illustrare in modo dettagliato nel suo messaggio concernente la legge sulla sicurezza delle informazioni quali ruoli rivestono il controllo di sicurezza relativo alle persone e la gestione del personale nell'ambito della sicurezza informatica e a differenziarli chiaramente l'uno dall'altro.

Le risorse di personale che la Confederazione impiega per l'esecuzione dei controlli di sicurezza relativi alle persone dipendono direttamente dal numero dei controlli di sicurezza necessari svolti dai servizi specializzati su incarico della Confederazione. L'attuale fabbisogno di risorse potrebbe pertanto non corrispondere a quello futuro in virtù della legge sulla sicurezza delle informazioni. Tale fabbisogno sarà illustrato dal Consiglio federale nel suddetto messaggio.

Raccomandazione 7

La DelCG raccomanda al capo del DDPS di provvedere affinché il SIC ricollochi la cellula di sicurezza in modo che essa non sia più subordinata alla divisione Supporto alla condotta e all'impiego (NDBU). Allo stesso tempo bisogna riflettere sulla ripartizione dei compiti relativi alla gestione dei rischi in seno al Servizio.

Il nostro Collegio aderisce parzialmente alla raccomandazione. Le questioni di ordine organizzativo sono sottoposte a verifica dal DDPS, unitamente al SIC, in un contesto più ampio e in considerazione della gestione dei rischi, della garanzia della qualità e dell'osservanza di disposizioni, direttive e regole comportamentali («compliance»). Anche la summenzionata subordinazione della cellula di sicurezza sarà verifica in tale contesto.

Raccomandazione 8

La DelCG raccomanda al DDPS di fare in modo che il SIC possa occupare i posti di lavoro di informatico attingendo alle riserve di personale del Dipartimento già nel 2013, sebbene il Consiglio federale abbia dato la propria autorizzazione per il 2014.

Già nel primo semestre del 2013, il DDPS ha autorizzato a favore del SIC il finanziamento di otto posti di lavoro per l'incremento della sicurezza informatica; nel frattempo la maggior parte di detti posti ha potuto essere occupata. Va osservato che,

affinché siano rispettate le condizioni quadro definite dalla Confederazione, l'estensione della sicurezza informatica e il reclutamento di specialisti TIC richiedono un certo lasso di tempo. Secondo i dati attualmente a disposizione, il SIC è in grado di occupare tutti gli otto posti entro il 1° gennaio 2014.

Raccomandazione 9

La DelCG raccomanda al Consiglio federale di elaborare delle proposte al fine di migliorare il processo di controllo dello stato della sicurezza informatica in seno alla Confederazione. Le misure devono permettere al Consiglio federale di identificare i rischi legati alla sicurezza informatica in modo tempestivo, di adottare le misure richieste per ridurre tali rischi e di monitorare la loro applicazione nel quadro di un processo istituzionalizzato.

Il nostro Collegio è disposto ad aderire alla raccomandazione e, in particolare, a sviluppare ulteriormente il processo di controllo dello stato della sicurezza TIC in seno all'Amministrazione federale centrale.

Nell'ambito del processo di sicurezza TIC in seno all'Amministrazione federale è fatta una chiara distinzione tra direttive, concretizzazione e controlling.

In virtù dell'ordinanza sull'informatica nell'Amministrazione federale (OIAF; RS *172.010.58*), l'Organo direzione informatica della Confederazione (ODIC) elabora pertinenti direttive licenziate dal Consiglio federale ed è competente per la definizione dei relativi dettagli. Dette direttive si fondano su un'analisi della minaccia e su un'analisi globale del fabbisogno di protezione costantemente aggiornate. La concretizzazione delle direttive rientra nella sfera di competenza dei dipartimenti e delle unità amministrative interessati (responsabilità gerarchica: art. 9 cpv. 1 e art. 10 OIAF). Alla gerarchia incombe anche il compito della verifica interna della concretizzazione; l'assunzione delle proprie responsabilità da parte della gerarchia è sottoposta a verifica dal Controllo federale delle finanze in qualità di servizio addetto alla revisione informatica (art. 28 OIAF).

Per sostenere il Consiglio federale nell'assunzione della sua responsabilità generale per l'impiego delle TIC in seno all'Amministrazione federale (art. 14 OIAF), l'ODIC sottopone al Consiglio federale un rapporto annuale redatto in base alle pertinenti dichiarazioni dei singoli dipartimenti (controlling) e presenta, laddove necessario, proposte di miglioramento (art. 11 OIAF). Sulla base del processo sin qui descritto – il quale, anche nel rapporto della DelCG, è stato valutato, al pari delle verifiche del Controllo federale delle finanze, idoneo al conseguimento degli obiettivi –, il Consiglio federale è disposto a sviluppare ulteriormente i processi, al fine di concretizzare la raccomandazione della DelCG.

Raccomandazione 10

La DelCG raccomanda al Consiglio federale di creare un gruppo di lavoro interdipartimentale, posto sotto la direzione dell'Ufficio federale del personale (UFPER), con il compito di elaborare delle condizioni di impiego particolari che permettano di migliorare le possibilità di reazione degli organi di gestione del personale di fronte a rischi di attacchi interni. Per ottenere il necessario consenso

dai collaboratori interessati, andrebbero esaminate in particolare anche misure di compensazione finanziaria o di altro tipo. Il Consiglio federale è invitato a esprimersi sui risultati ottenuti dal gruppo di lavoro entro la fine del 2014.

La legislazione vigente in materia di personale prevede già la possibilità della sospensione dal servizio. Tale misura può essere adottata sia durante un rapporto di impiego non disdetto (cfr. art. 103 dell'ordinanza sul personale federale, OPers; RS *172.220.111.3*) sia a disdetta avvenuta (art. 103*a* OPers). Nel suo rapporto, la DelCG auspica in particolare un'estensione della possibilità di ricorrere a una rapida sospensione durante un rapporto di impiego non disdetto. All'articolo 103 capoverso 1 OPers sono sancite le seguenti condizioni per la sospensione durante un rapporto di impiego non disdetto:

«[1] Se l'esecuzione corretta dei compiti è compromessa, l'autorità competente ai sensi dell'articolo 2 può sospendere in via cautelare l'impiegato dal servizio oppure attribuirgli un'altra funzione se:

a. sono constatati o supposti avvenimenti gravi dal punto di vista penale o disciplinare;
b. sono rilevate irregolarità ripetute; oppure
c. è ostacolato un procedimento in corso».

Raccomandazione 11

La DelCG chiede al capo del DDPS di vigilare sul rispetto incondizionato dei diritti all'informazione garantiti alla Sorveglianza delle attività informative dalla legge (art. 8 LSIC in combinato disposto con l'art. 26 cpv. 1 LMSI) e dall'ordinanza (art. 33 cpv. 1 O-SIC). Il SIC non può limitare questi diritti all'informazione né di sua propria iniziativa, né in accordo con il capo del Dipartimento.

La tematica delle competenze e delle prestazioni dell'organo di controllo interno al DDPS addetto alla vigilanza sulle attività informative è stata affrontata dal DDPS già nell'autunno del 2012. L'elaborazione della nuova legge sul servizio informazioni e il furto di dati in seno al SIC hanno indotto il capo del DDPS a sottoporre alla verifica di un perito esterno sia i presupposti per un controllo efficace del SIC sia l'efficacia dell'organo Vigilanza sulle attività informative istituito all'inizio del 2009. L'incarico è stato assegnato al prof. dott. Heinrich Koller, ex direttore dell'Ufficio federale di giustizia. La perizia ha tra l'altro fornito chiarezza sulle modalità di valutazione dell'efficacia della «Vigilanza sulle attività informative» nella sua attuale forma organizzativa e risposte all'interrogativo se la Vigilanza disponga o meno dei mezzi e dei diritti necessari.

I diritti e i doveri della Vigilanza sulle attività informative nonché, in particolare, il diritto globale a essere informata sono sanciti agli articoli 31–34 dell'ordinanza del Consiglio federale sul Servizio delle attività informative della Confederazione (O-SIC; RS *121.1*) e precisati nelle istruzioni che disciplinano la Vigilanza sulle attività informative, interne al Dipartimento ed emanate dal capo del DDPS in data 20 gennaio 2011 (Weisungen über die Nachrichtendienstliche Aufsicht / Directives concernant la Surveillance des services de renseignement). In virtù degli atti men-

zionati, i collaboratori del SIC sono tenuti a fornire alla Vigilanza sulle attività informative indicazioni veritiere e complete. In via complementare, il prof. Koller ha raccomandato nel suo rapporto finale di fine marzo 2013 di elevare il rango della Vigilanza sulle attività informative nell'organico dipartimentale, di semplificarne l'accesso diretto al capo del DDPS e di sancirne a livello di legge formale l'indipendenza nell'adempimento dei compiti.

Nel quadro della concretizzazione delle raccomandazioni appena menzionate, il capo del DDPS ha ordinato a fine aprile 2013 l'allestimento di un catalogo di misure globali per il rafforzamento della Vigilanza sulle attività informative. La principale misura prevista concerne la definizione a livello legale formale, nella legge sul servizio informazioni, dell'indipendenza della Vigilanza sulle attività informative nell'espletamento degli incarichi. Il tenore dell'avamprogetto dell'8 marzo 2013 della legge sul servizio informazioni sarà ampliato come segue: «La Vigilanza sulle attività informative non è vincolata a istruzioni per lo svolgimento dei suoi compiti di vigilanza». Il nostro Collegio considera essenziale che la Vigilanza sulle attività informative, chiamata a verificare la legalità, l'opportunità e l'efficacia dei servizi informazioni, possa adempiere in maniera indipendente ed efficace tale sua funzione chiave. In quest'ottica, il Consiglio federale aderisce alla raccomandazione.

4 Conclusioni

Un'illustrazione delle carenze evidenti in seno a un sottosettore del SIC non corredata del riconoscimento delle prestazioni globali del Servizio delle attività informative della Confederazione non corrisponde alla percezione effettiva che i committenti e i beneficiari hanno delle prestazioni del SIC. Il Consiglio federale sottolinea che, dalla fusione dei servizi informazioni, anche la fiducia dei partner stranieri nel SIC ha registrato un aumento.

Nell'ambito della propria attività, un servizio informazioni deve costantemente valutare dei rischi – a livello politico, giuridico, tecnico o umano. Il nostro Collegio è del parere che, dopo la fusione del servizio informazioni interno e del servizio informazioni concernente l'estero, auspicata dagli organi di vigilanza parlamentari, il nuovo servizio informazioni è riuscito con successo, senza registrare perdite nel suo portfolio di conoscenze né gravi problemi a livello di personale, a garantire la legalità della sua attività e a instaurare una comune cultura di lavoro, continuando nel contempo a fornire prestazioni di elevata qualità.

Il fatto che, nella fattispecie oggetto delle indagini, la reazione sia stata lenta – oppure, secondo il giudizio espresso dalla DelCG, tardiva – deve costituire per il SIC e per l'Amministrazione federale un'opportunità per trarre utili insegnamenti. La fattispecie oggetto del rapporto illustra in maniera esemplare quanto sia difficoltoso riconoscere tempestivamente e sanare efficacemente eventuali conflitti a livello di obiettivi tra i doveri del datore di lavoro, i diritti dei lavoratori e gli interessi dello Stato in materia di sicurezza e di tutela del segreto.