Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FF 2021
www.dirittofederale.admin.ch
La versione elettronica firmata
è quella determinante

Caso Crypto AG

Rapporto della Delegazione delle Commissioni della gestione delle Camere federali

del 2 novembre 2020

L'essenziale in breve

A partire dall'autunno 1993 il Servizio di informazioni strategico (SIS) è riuscito a ottenere informazioni attendibili in merito alla società Crypto AG. È così giunto a conoscenza che la società apparteneva a servizi di intelligence stranieri ed esportava apparecchi «deboli», la cui cifratura poteva essere violata con poco sforzo. Per decrittare la cifratura di questi apparecchi, il SIS ha cominciato a procurarsi informazioni tecniche sulle procedure di cifratura utilizzate e sugli elenchi di clienti della società. Successivamente, quando è diventato un ufficio federale in ambito civile, è riuscito ad assicurarsi un accesso a queste conoscenze con il consenso dei servizi di intelligence statunitensi.

In un'ottica giuridica, la Delegazione delle Commissioni della gestione (DelCG) presuppone dunque una collaborazione con i servizi di intelligence stranieri, così come prevista un tempo dalla legge militare e oggi dalla legge sulle attività informative (LAIn). Il fatto che il SIS e i servizi americani agissero di comune accordo implica una corresponsabilità delle autorità elvetiche nelle attività della Crypto AG. In un'ottica giuridica era ammissibile che il SIS e un servizio estero si avvalessero congiuntamente di un'impresa con sede in Svizzera per procurarsi informazioni concernenti l'estero. Tuttavia, considerando la grande valenza politica di tale collaborazione, la DelCG ritiene sbagliato che, prima dell'attuale responsabile del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), nessuno dei suoi predecessori sia stato informato in merito a questa operazione.

Inoltre, gli elementi acquisiti dal SIS sulla Crypto AG durante il caso Bühler, sul quale la Polizia federale (Polfed) ha indagato nel 1994 e nel 1995, non avrebbero dovuto essere tenuti nascosti alla direzione politica della Svizzera. Secondo quanto ha dichiarato alla DelCG, l'allora capo del Dipartimento militare federale (DMF) non è giunto a conoscenza della verità sulla Crypto AG neppure per altre vie. Inoltre, la DelCG non ha trovato prove di un'ingerenza illecita da parte di esponenti politici sulle inchieste condotte dalla Polfed. Il capo del Dipartimento federale di giustizia e polizia (DFGP) si è sforzato piuttosto di fare luce sull'assetto proprietario della società. La Polfed ha poi dovuto sospendere la sua inchiesta senza riuscire a rispondere a questa domanda.

Nel 1994 la DelCG ha chiesto a più riprese di essere informata sull'inchiesta in corso da parte della Polfed. Tuttavia, così come le massime cariche militari e politiche del SIS, la DelCG non ha ricevuto alcuna informazione in merito agli elementi acquisiti dal servizio di intelligence estero sulla Crypto AG. La società non figurava mai neppure nelle informazioni fornite dal DDPS quando l'autorità di alta vigilanza si è occupata specificamente del tema della crittologia nel 2007 e nel 2009.

Per l'ispezione della DelCG si sono rivelati preziosi soprattutto i dossier operativi del SIS e della Polfed, che il Servizio delle attività informative della Confederazione (SIC) custodiva in un'installazione K riconvertita. I dossier devono essere ancora archiviati secondo le prescrizioni. Considerando la prassi di archiviazione dei servizi di informazione, non c'è alcuna garanzia che tutti i documenti importanti siano ancora disponibili. In alcuni casi, la distruzione di questi documenti era consentita in termini di legge e di ordinanza, ma in altri è avvenuta violando le prescrizioni in

vigore. Tra il 2011 e il 2014, per esempio, il SIC ha distrutto documenti concernenti scambi avvenuti con servizi partner stranieri, invece di conservarli al proprio interno come prescritto. L'ispezione della DelCG le ha mostrato come la distruzione di documenti da parte del servizio di informazione non costituisca uno strumento efficace per proteggere le fonti e rischi piuttosto di mettere a repentaglio vecchie fonti quando le autorità agiscono inconsapevolmente.

Le imprese e le organizzazioni che operano in Svizzera beneficiano all'estero dell'immagine di cui gode la Svizzera in qualità di Stato neutrale. Di conseguenza, i servizi di intelligence stranieri possono avere tutto l'interesse a svolgere attività informative a discapito di altri Stati nascondendosi dietro il paravento di una società svizzera. In determinate condizioni la società in questione può realizzare, con le sue attività, gli elementi costitutivi del reato di spionaggio a danno di Stati terzi. Tuttavia, secondo il diritto vigente, una tale operazione è consentita se un servizio estero si avvale di una società svizzera in collaborazione con il SIC per acquisire informazioni concernenti l'estero (cfr. art. 34 cpv. 2 LAIn). La DelCG è del parere che, prima di condurre un'operazione in tal senso, sia necessario procedere a una valutazione politica delle possibili conseguenze per la Svizzera, ma anche per i collaboratori della società eventualmente coinvolti. Il Consiglio federale dovrebbe dunque chiarire in linea di principio quale margine di manovra intende concedere al DDPS.

Il caso Crypto AG dimostra che le società poste sotto l'influenza di servizi di intelligence stranieri possono produrre apparecchi che utilizzano procedure di cifratura «deboli». La DelCG presuppone tuttavia che la Crypto AG non abbia mai fornito apparecchi di cifratura «deboli» alle autorità elvetiche. In proposito si è rilevato importante che le autorità elvetiche abbiano potuto verificare la sicurezza degli apparecchi acquistati o, addirittura, influenzarne la progettazione, ma ciò è possibile soltanto nel caso di fornitori che sviluppano e producono i propri apparecchi in Svizzera. Per motivi di sicurezza non è sostenibile che la Confederazione acquisti soluzioni di cifratura da fornitori esteri. Sin dall'inizio il Consiglio federale non ha riservato la necessaria attenzione al ruolo che i fornitori indigeni svolgono nel garantire alle autorità elvetiche la disponibilità di tecniche di cifratura sicure. In qualità di dipartimento responsabile, il DDPS non ha analizzato in tempo utile i rischi per la sicurezza dell'approvvigionamento sottoponendo la propria valutazione al Consiglio federale.

La direzione del SIS ha celato molto bene il fatto di avere accesso alle informazioni concernenti la Crypto AG. Al momento della creazione del Servizio delle attività informative della Confederazione (SIC), questo elemento non è stato trasmesso al suo primo direttore che alcuni anni dopo, quando è stato confrontato con la questione, si è rifiutato di assumersi la sua responsabilità di condotta.

Solo con l'attuale direttore del SIC, nell'estate 2019, è stato conferito l'incarico di stilare un bilancio della situazione, sebbene egli non fosse stato informato dal suo predecessore e il SIC non fosse a conoscenza che i media stavano svolgendo ricerche sulla Crypto AG. Le informazioni così ottenute non sono state tuttavia sfruttate per sottoporre a un'analisi critica lo sviluppo delle relazioni tra le organizzazioni che hanno preceduto il SIC, i servizi di intelligence americani e la Crypto AG. Invece di chiarire il contesto giuridico e riconoscere la portata politica, il SIC si è accontentato di minimizzare l'importanza del caso Crypto AG per l'attuale servizio.

Neppure il DDPS, che ha informato il Consiglio federale e la DelCG già nel novembre 2019, ha riconosciuto la necessità di intervenire a livello politico. Il gruppo di lavoro interdipartimentale di cui il DDPS si è avvalso non è riuscito a fornire un supporto efficace alla direzione politica a causa della riluttanza del SIC a condividere informazioni sul caso che si stava delineando.

Nella sua proposta destinata alla seduta del Consiglio federale del 20 dicembre 2019, il DDPS affermava che le informazioni disponibili in quel momento non erano sufficienti a discutere i contenuti del caso Crypto AG. Questa constatazione non era tuttavia più pertinente dopo la scoperta dei dossier nell'installazione K che il DDPS aveva reso nota al Consiglio federale. Dal momento che il SIC non aveva ancora esaminato i voluminosi dossier prima della seduta del Consiglio federale, questi ha deciso di istituire un comitato di esperti esterno per chiarire gli aspetti ritenuti di carattere puramente storico. Sin dall'inizio il Consiglio federale ha quindi ceduto la direzione strategica della gestione del caso Crypto AG.

Quando la DelCG ha avviato la sua ispezione il 13 febbraio 2020, l'ex giudice federale Niklaus Oberholzer lavorava già da un mese in qualità di esperto esterno su incarico del Consiglio federale, tuttavia senza aver ottenuto l'accesso ai dossier rinvenuti nell'installazione K. Una volta chiesti tutti i documenti rilevanti di cui il SIC era in possesso, la DelCG ha riconosciuto che il caso Crypto AG andava ben al di là della semplice storiografia ed era di assoluta attualità. Di conseguenza, la scelta del DDPS di indagare separatamente sugli aspetti storici e su quelli attuali del caso si è dimostrata poco opportuna. Considerando gli stretti legami tra le diverse inchieste, la DelCG ha ritenuto necessario discutere con la responsabile del DDPS gli aspetti irrisolti del coordinamento prima di proseguire i lavori. Tuttavia, quando il DDPS ha esteso il campo dell'inchiesta Oberholzer prima del colloquio previsto con la DelCG, quest'ultima ha revocato, il 21 febbraio 2020, la sua autorizzazione all'incarico da parte del Consiglio federale a Niklaus Oberholzer, che in qualità di inquirente della DelCG ha poi esaminato criticamente gli aspetti del caso Crypto AG legati alle attività informative dandone conto alla DelCG in un rapporto segreto.

Il 25 febbraio 2020 la DelCG ha discusso la revoca dell'autorizzazione con la responsabile del DDPS. Il successivo scambio di scritti con il Consiglio federale ha portato a un incontro, tenutosi il 25 maggio 2020, con la presidente della Confederazione e la responsabile del DDPS. In quella occasione, la DelCG ha fornito le principali informazioni in merito al ruolo dei servizi delle attività informative nel caso Crypto AG. Queste informazioni sono state trasmesse anche al Consiglio federale in una comunicazione segreta.

Dopo la seduta del Consiglio federale del 20 dicembre 2019, il Dipartimento federale dell'economia, della formazione e della ricerca (DEFR) ha deciso di sospendere le autorizzazioni generali d'esportazione concesse alle imprese che sono subentrate alla Crypto AG. Evidentemente l'obiettivo era di evitare la pubblicazione nei media di notizie negative nei confronti del DEFR. Tuttavia, secondo la DelCG la sospensione di queste autorizzazioni non era giustificata né sul piano materiale né su quello giuridico, né lo era la tattica dilatoria adottata dalla Segreteria di Stato dell'economia (SECO) con l'appoggio del DEFR nei confronti delle società coinvolte. Le domande di autorizzazioni singole all'esportazione potevano comunque essere presentate e nessuna ragione giuridica si opponeva al loro rilascio, come giustamente ammesso

dal gruppo di controllo delle esportazioni il 4 marzo 2020. In considerazione della posizione assunta dal Dipartimento federale degli affari esteri (DFAE), nel mese di maggio del 2020 è stato tuttavia deciso di sottoporre tutte le domande alla decisione del Consiglio federale.

Il 25 febbraio 2020 la SECO, con il supporto del DEFR, ha sporto denuncia presso il Ministero pubblico della Confederazione (MPC). In base ai primi articoli apparsi nei media, la SECO sospettava infatti che la Crypto AG avesse violato, prima del 2018, alcuni obblighi di dichiarazione previsti dal diritto sul controllo dei beni a duplice impiego con l'esportazione di apparecchi che utilizzavano una tecnica di cifratura «debole». Il DEFR ha accolto, senza verificarla, l'argomentazione della SECO secondo cui ragioni legali imponevano una denuncia. Dal canto suo, il MPC ha sconsigliato alla SECO di sporgere denuncia e la SECO non ha consultato altri servizi federali competenti.

Dal punto di vista della DelCG, la denuncia si è basata su una valutazione non accurata dei fatti e su un'argomentazione giuridica carente. La denuncia, dal momento che era manifestamente motivata da ragioni politiche, avrebbe dovuto essere sporta non dalla SECO, ma dal DEFR.

Il 13 marzo 2020 il MPC ha chiesto al DFGP l'autorizzazione ad avviare un procedimento penale concernente le violazioni del diritto sul controllo dei beni a duplice impiego denunciate dalla SECO. Tre mesi più tardi, il DFGP ha sottoposto la richiesta di autorizzazione del MPC al Consiglio federale affinché decidesse in merito. Precedentemente, il 25 maggio 2020, il DFGP ne aveva discusso con la DelCG. A sua volta il DEFR ha chiesto al Consiglio federale, il 10 giugno 2020, di autorizzare tutte le domande d'esportazione in sospeso, nonostante avesse sostenuto la denuncia della SECO. Dopo che il Consiglio federale ha rinviato la trattazione dell'oggetto di una settimana, il DEFR gli ha chiesto, rifacendosi alla denuncia della SECO, di sospendere la decisione relativa alle domande fino alla chiusura dell'inchiesta da parte del MPC. Il 19 giugno 2020 il Consiglio federale ha accolto questa richiesta e lo stesso giorno ha concesso l'autorizzazione al MPC.

La DelCG riconosce la coerenza tra la decisione del Consiglio federale in merito alla richiesta di autorizzazione del MPC e quella riguardante le domande di autorizzazioni singole all'esportazione delle società che sono subentrate alla Crypto AG. Tuttavia, rimandando a tempo indeterminato la trattazione delle richieste, il Consiglio federale potrebbe aver contravvenuto al principio della buona fede, dal momento che ogni impresa svizzera dovrebbe in linea di principio poter contare sull'autorizzazione rapida alle sue esportazioni laddove non vi si oppongano motivi giuridici. D'altronde il diritto in materia di controllo dei beni a duplice impiego non costituiva uno strumento adeguato per reagire al caso Crypto AG e la denuncia penale è palesemente stata un tentativo di sottrarsi alla propria responsabilità politica, lasciando che fosse la giustizia a gestire il caso. In ultima analisi, il Consiglio federale ha dunque associato il procedimento del MPC con l'inchiesta che la DelCG stava conducendo, il che costituisce un problema dal punto di vista della separazione dei poteri.

Indice

Rapporto

1 Svolgimento dei lavori

Quando la Delegazione delle Commissioni della gestione (DelCG) si è costituita, il 19 dicembre 2019, il consigliere nazionale Alfred Heer, vicepresidente uscente, ne ha assunto la presidenza. La consigliera agli Stati Maya Graf, che era già stata membro della DelCG quando era consigliera nazionale, è stata nominata vicepresidente. Infine, sono entrati a far parte della Delegazione in qualità di membri la consigliera nazionale Yvonne Feri, il consigliere nazionale Stefan Müller-Altermatt e i consiglieri agli Stati Philippe Bauer e Werner Salzmann.

Nella sua prima seduta del 20 gennaio 2020, la DelCG ha preso atto della decisione del Consiglio federale di affidare all'ex giudice federale Niklaus Oberholzer l'incarico di svolgere una disamina storica del caso Crypto AG (cfr. n. 6.2). Dal suo colloquio del 25 novembre 2019 con la responsabile del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), la Delegazione non aveva ricevuto altre informazioni né documenti in materia da parte del DDPS (cfr. n. 4.1.4). Sempre più preoccupato di questa mancanza di informazioni, il presidente della Delegazione ha chiesto un incontro con il direttore del Servizio delle attività informative della Confederazione (SIC) all'inizio di febbraio 2020, ma le informazioni ricevute il 6 febbraio 2020 non sono state ritenute soddisfacenti e il presidente della DelCG ha voluto che gli fosse sottoposta immediatamente una copia del rapporto MINERVA (cfr. n. 2.1.1), di cui apparentemente erano già in possesso diversi giornalisti.

Il 12 febbraio 2020 la DelCG ha deciso di convocare una seduta straordinaria per il giorno seguente. La stessa sera il presidente della DelCG ha partecipato alla trasmissione televisiva «Rundschau». Nella seduta del 13 febbraio 2020 la DelCG ha deciso di svolgere un'ispezione formale e ne ha informato il Consiglio federale e l'opinione pubblica[1]. In particolare intendeva indagare sui legami esistenti tra i servizi dell'Amministrazione federale e i servizi di intelligence stranieri implicati e accertare se e in quale misura il Consiglio federale fosse informato dei fatti relativi alla società Crypto AG.

Al contempo la DelCG ha chiesto al DDPS che gli fossero consegnati numerosi documenti. Dalla Cancelleria federale (CaF) si è inoltre procurata gli estratti dei verbali di tutte le sedute durante le quali il Consiglio federale ha discusso il caso Crypto AG. Ha quindi immediatamente proceduto alle audizioni di persone che sono o erano al servizio della Confederazione. Tra il 19 e il 26 febbraio 2020 la DelCG aveva già ascoltato 14 persone e aveva avuto un colloquio con la responsabile del DDPS.

Fino all'ultima audizione del 26 agosto 2020, la DelCG aveva ascoltato 32 dipendenti ed ex dipendenti della Confederazione, alcuni dei quali più volte. Tra le 12 persone ascoltate che non erano più al servizio della Confederazione figuravano un ex capo del Dipartimento militare federale (DMF) e uno del DDPS (*Kaspar Villiger e Samuel Schmid*) nonché un ex capo del DFGP (*Arnold Koller*). Sono stati ascoltati tutti gli ex

[1] Ispezione della Delegazione delle Commissioni della gestione sul caso Crypto AG, comunicato stampa della DelCG del 13 feb. 2020.

direttori del SIC e del Servizio di informazioni strategico (SIS)[2] e gli ultimi capi della Polizia federale (Polfed) e del SIS.

Dopo avere revocato l'autorizzazione ad aprire un'inchiesta che il Consiglio federale aveva affidato a Niklaus Oberholzer, il 24 febbraio 2020 la DelCG ha incontrato il signor Oberholzer per essere informata dei lavori da questi svolti sino a quel momento su incarico del Consiglio federale. Ha quindi convenuto con il signor Oberholzer che egli proseguisse i lavori, ma su mandato della DelCG. In occasione del colloquio del 25 febbraio 2020, la responsabile del DDPS si è dichiarata d'accordo in merito alla procedura adottata dalla DelCG.

Il signor Oberholzer ha assunto ufficialmente la funzione di incaricato dell'inchiesta della DelCG il 2 marzo 2020. Ha avuto accesso a tutti i documenti che la DelCG aveva ricevuto e gli sono stati consegnati, a titolo informativo, tutti i verbali delle audizioni svolte in materia dalla Delegazione, secondo la quale non era tuttavia necessario che egli presenziasse alle audizioni.

Il suo lavoro era incentrato sullo studio dei dossier operativi delle organizzazioni che hanno preceduto il SIC (cfr. n. 2.1.3) e sull'analisi dei pertinenti eventi. Su questa base ha proceduto anche a contestualizzare gli eventi che si sono succeduti sotto il SIC.

Il 2 luglio 2020 il signor Oberholzer ha discusso la bozza del suo rapporto con la DelCG, dopo di che le ha consegnato la versione definitiva nella quale sono raccolte tutte le informazioni disponibili, anche quelle che la DelCG non ha inserito nel presente rapporto d'ispezione per ragioni di segretezza. Il rapporto Oberholzer, di circa 90 pagine, completa il rapporto d'ispezione ufficiale ed è destinato unicamente alla DelCG e al Consiglio federale.

2 Documenti su cui si è basata l'ispezione

2.1 Riepilogo dei fatti

2.1.1 Rapporto MINERVA

Il rapporto «MINERVA – A History» descrive come i servizi di intelligence americani abbiano sfruttato la Crypto AG, che dagli anni Cinquanta produceva apparecchi di cifratura in Svizzera, per i propri fini e con il consenso del suo proprietario svedese. Nel 1970 la società, cui era stato attribuito il nome di copertura MINERVA, è stata acquisita insieme dai servizi di intelligence americani e da quello tedesco. Il rapporto parla anche del ritiro dei Tedeschi alla fine del 1993 e riporta i fatti che sono accaduti fino al 1995.

Il rapporto MINERVA è stato redatto dai servizi americani dopo il 2000 con il coinvolgimento di rappresentanti del servizio di intelligence tedesco, che sembra abbia ricevuto, verso il 2005, una copia del rapporto al quale ha successivamente aggiunto

2 Nel 2001 il Gruppo servizio informazioni dell'esercito è stato sciolto e la sua divisione nel SIS è stata integrata nella direzione civile del SIS.

alcune valutazioni complementari. Questa versione del rapporto americano e i documenti tedeschi sono giunti nelle mani dei media che hanno cominciato a pubblicarne alcuni estratti a partire dalla seconda settimana di febbraio del 2020. A tutt'oggi i media non hanno comunque divulgato l'intero rapporto MINERVA, che conta quasi 100 pagine.

La DelCG ha analizzato il rapporto MINERVA che aveva ricevuto dal SIC. Le informazioni complementari fornite dal SIC non lasciano dubbi in merito all'autenticità del documento, ma il contenuto del rapporto sugli eventi verificatisi in Svizzera e sulle autorità elvetiche è tuttavia spesso poco preciso e descrive dettagli che si sono dimostrati errati. Ciò induce a supporre che gli autori americani conoscessero poco la Svizzera e le sue istituzioni. Tuttavia, la DelCG presuppone fondamentalmente che i redattori del rapporto abbiano riportato in assoluta buona fede i fatti di cui sono stati informati dai loro agenti presso la Crypto AG o da altre fonti e che li abbiano inquadrati secondo i propri modelli interpretativi. La DelCG conosce solo parzialmente i rapporti tedeschi, ma le informazioni disponibili non erano direttamente rilevanti per la sua ispezione.

2.1.2 Verbali dei colloqui sulla gestione del capo del DDPS

Con la trasformazione del SIS in un ufficio federale civile, il capo del DDPS ha assunto, dal 2001, la responsabilità di condotta diretta del servizio informazioni concernente l'estero. Il DDPS ha potuto trasmettere alla DelCG i verbali dei colloqui mensili tra il capo del DDPS (*Samuel Schmid*) e i direttori del SIS (prima *Hans Wegmüller,* poi *Paul Zinniker*) relativi agli anni dal 2002 al 2008. I verbali erano redatti dal relatore competente del capo del Dipartimento. Nel verbale dell'ultimo colloquio mensile del 2008 la DelCG ha trovato una nota secondo la quale l'allora capo del DDPS aveva svolto altri colloqui, non verbalizzati, con il direttore del SIS e aveva l'intenzione di far conservare le sue note personali al riguardo al di fuori dell'Archivio federale svizzero (AFS).

Dopo che la DelCG aveva pregato il DDPS e l'AFS di procedere alle necessarie ricerche, i due taccuini contenenti le note scritte a mano dall'allora capo del DDPS sono stati rinvenuti nella Biblioteca Am Guisanplatz. Evidentemente questi documenti erano stati affidati all'ex direttore della biblioteca militare, ma successivamente non erano stati archiviati in modo corretto. La DelCG provvederà affinché la Segreteria generale del DDPS (SG-DDPS) garantisca la sicurezza e la conservazione conforme alle disposizioni legali di queste note.

Dopo l'avvicendamento alla testa del Dipartimento (*nuovo capo: Ueli Maurer*) all'inizio del 2009, il primo colloquio mensile con il SIS è stato ancora verbalizzato, ma l'abolizione del posto di relatore responsabile dei servizi delle attività informative ha interrotto la verbalizzazione da parte della SG-DDPS degli ulteriori colloqui sulla gestione avuti con il direttore del SIS. La DelCG non ha trovato riferimenti alla Crypto AG in nessuno dei verbali dei colloqui sulla gestione intercorsi tra il capo del Dipartimento e i direttori del SIS.

All'inizio del 2009 il Servizio di analisi e prevenzione (SAP) è stato trasferito dal DFGP al DDPS e, all'inizio del 2010, è stato unificato con il SIS per dare vita al SIC.

I colloqui mensili tra il capo del DDPS e il direttore del SIC (*Markus Seiler*) sono stati tuttavia verbalizzati solo dall'inizio del 2014, questa volta dal capo della Vigilanza sulle attività informative interna al DDPS. La sua partecipazione ai colloqui mensili è stata in ultima istanza la conseguenza dell'inchiesta amministrativa condotta dal professor Heinrich Koller su incarico del capo del DDPS dopo il furto di dati presso il SIC e conclusasi alla fine di marzo 2013[3]. I soli documenti esistenti per gli anni precedenti sono gli ordini del giorno stilati dal direttore del SIC in preparazione dei suoi colloqui sulla gestione con il capo del DDPS.

I colloqui mensili hanno continuato a essere verbalizzati con il successivo capo del DDPS (*Guy Parmelin*). In nessuno dei documenti si trovano indicazioni che il direttore del SIC abbia fatto menzione qualsiasi della Crypto AG al suo capo Dipartimento.

2.1.3 Dossier operativi della Polfed e del SIS

Per sapere che cosa i servizi di informazioni svizzeri conoscessero della Crypto AG la DelCG ha dovuto consultare soprattutto i documenti concernenti la ricerca di informazioni effettuata dalla Polfed e dal SIS che riguardavano attività risalenti ai lontani anni Settanta.

Dopo l'«affare delle schede», la Polfed ha insistito presso l'AFS affinché i documenti da archiviare fossero distinti tra atti per uso forense e atti per uso non forense: solo i primi dovevano essere consegnati all'AFS. Come appreso dalla DelCG all'inizio del 2001, l'allora direttore dell'AFS (*Christoph Graf*), pur giudicando questa esigenza giuridicamente inammissibile, non ha potuto obbligare la Polfed a consegnargli i dossier allestiti per le attività di prevenzione della polizia.

Le inchieste di polizia che la Polfed ha svolto nel 1994 in seguito alle accuse rivolte da Hans Bühler e dai media nei confronti della Crypto AG sono avvenute nella prospettiva della successiva apertura di una procedura di polizia giudiziaria. Dal momento che sono stati considerati idonei all'uso forense, i dossier in questione sono stati rimessi all'AFS, dove hanno potuto essere recuperati piuttosto rapidamente.

L'AFS non deteneva invece documenti concernenti l'indagine che la Polfed ha svolto negli anni Settanta sulla base delle indicazioni fornite dall'ex responsabile del settore Sviluppo della Crypto AG. In quanto riguardavano investigazioni nell'ambito delle attività di prevenzione della polizia, i suddetti documenti non sono mai stati consegnati all'AFS, ma sono stati comunque conservati internamente con l'appellativo di «caso Code» (cfr. n. 3.1.1). All'inizio del 2010 sono poi stati consegnati al SIC in-

3 Ispezione a seguito dell'arresto di un'ex fonte del SIC in Germania, rapporto del 13 mar. 2018 della DelCG, n. 2.3 (FF **2018** 4303, qui 4321).

sieme con gli atti dell'«operazione Rötel» (cfr. n. 3.1.2) e rinvenuti nell'ex installazione K[4], che il SIS aveva riconvertito per la conservazione dei documenti particolarmente segreti (cfr. n. 2.1.4). È stato in questa installazione K che sono stati scoperti i dossier del SIS concernenti la Crypto AG.

2.1.4 Prassi di archiviazione dei servizi delle attività informative

La legge sull'archiviazione (LAr)[5] è entrata in vigore il 1° ottobre 1999 e ha sostituito il regolamento del Consiglio federale del 15 luglio 1966 per l'Archivio federale. La nuova legge ha introdotto l'obbligo di offerta dei documenti all'AFS in sostituzione di quello di fornirli, tuttavia l'obiettivo dell'archiviazione, ossia quello di conservare tutti i documenti «preziosi» per i posteri, è rimasto lo stesso. La LAr non prevedeva eccezioni, ma il Consiglio federale ha cominciato, per via di ordinanza, ad allontanarsi da questo principio a favore dei servizi delle attività informative.

Conformemente all'articolo 17 capoverso 7 della legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI)[6], entrata in vigore il 1° luglio 1998, nelle relazioni con l'estero la protezione delle fonti doveva essere garantita in ogni caso. In virtù di questa disposizione, nel giugno 2001 il Consiglio federale ha esonerato il SAP, che era subentrato alla Polfed, dall'obbligo di proporre all'AFS per l'archiviazione i dati classificati derivanti da relazioni dirette con autorità di sicurezza estere (art. 21 cpv. 2 OMSI)[7]. Come spiegato alla DelCG nel luglio 2001 dall'allora capo del SAP (*Urs von Daeniken*), il suo servizio distruggeva generalmente questo tipo di documenti al più tardi dopo cinque anni. Nel 2008, per esempio, il SAP ha ricevuto 8200 messaggi da servizi partner, mentre quelli inviati sono stati oltre 10 900[8].

Le investigazioni in merito ai contatti dei servizi delle attività informative elvetici con il Sudafrica, svolte dalla DelCG tra il 1999 e il 2003, hanno rivelato che il Servizio informazioni militare aveva sistematicamente distrutto documenti nel corso degli anni, sottraendoli così all'archiviazione[9]. Quando ha visitato l'AFS nel gennaio 2001, la DelCG ha constatato che i fondi d'archivio più recenti del servizio di informazioni risalivano agli anni Quaranta. Successivamente ha appreso che il nuovo direttore del

4 L'elenco AGFA (Abteilung für Genie und Festung Anlageverzeichnis [Divisione del genio e delle fortificazioni – elenco delle installazioni]) dell'ex Ufficio federale del genio e delle fortificazioni ha suddiviso le installazioni e le costruzioni dell'esercito in diverse categorie. Gli impianti di comando rientravano nelle categorie «A» o «F», come l'impianto di fortificazione A-01780 dell'organizzazione P-26 a Gstaad (cfr. rapporto annuale 2018 del 28 gen. 2019 delle CdG e della DelCG, n. 4.10 [FF **2019** 2359, qui 2443]). In passato venivano spesso designati come installazioni K (per Kriegsanlagen, installazioni di guerra) anche gli impianti di comando della condotta civile e militare.

5 Legge federale del 26 giu. 1998 sull'archiviazione (LAr; RS **152.1**).

6 Legge federale del 21 mar. 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI; RS **120**).

7 Ordinanza federale del 27 giu. 2001 sulle misure per la salvaguardia della sicurezza interna (OMSI; RU **2001** 1829).

8 Rapporto d'attività 2008 dell'Ufficio federale di polizia fedpol, mag. 2009, pag. 18.

9 Esame dei contatti del Servizio informazioni svizzero con il Sudafrica ai tempi dell'apartheid, rapporto del 18 ago. 2003 della DelCG, n. 4.3.7 (FF **2004** 1981, qui 2009).

SIS aveva tuttavia deciso, all'inizio del 2001, che nessun altro documento avrebbe dovuto essere distrutto senza il consenso dell'AFS.

All'inizio del 2004, l'entrata in vigore dell'articolo 99 capoverso 4 della legge militare (LM)[10] ha introdotto una nuova disposizione concernente la protezione delle fonti. Secondo il messaggio del Consiglio federale, il SIS aveva la competenza di derogare alla LAr[11]. In seguito, il nuovo articolo 12 capoverso 2 dell'ordinanza sui servizi d'informazione (OSINF)[12] ha previsto che il SIS non doveva offrire per l'archiviazione i documenti classificati provenienti da contatti diretti con servizi stranieri e dalla ricerca di informazioni operativa, ma conservarli internamente d'intesa con l'Archivio federale. Per conservare a lungo questo tipo di documenti in modo sicuro, il SIS ha incaricato la riconversione della summenzionata installazione K per renderla il proprio archivio a uso esclusivo (cfr. n. 2.1.3).

Se la deroga accordata al SAP ha comportato la distruzione definitiva di tutti i documenti provenienti da contatti con servizi stranieri, almeno a tenore dell'OSINF il SIS non aveva la competenza di distruggere documenti importanti. Tuttavia, il Consiglio federale ha autorizzato il SIS a tenere un proprio archivio al di fuori dell'AFS. Rimanevano comunque aperte diverse questioni in merito all'organizzazione di questa raccolta di fascicoli o alla regolamentazione della loro consultazione. Come constatato dalla DelCG nel gennaio 2011 in occasione di un colloquio con l'allora direttore dell'AFS (*Andreas Kellerhals*), in tutti quegli anni l'AFS e il SIS non sono mai riusciti a mettersi d'accordo sulle modalità di conservazione dei fascicoli nell'installazione K. Tra l'altro, l'AFS non aveva accesso a questi documenti.

Quando sono state elaborate le ordinanze per il nuovo SIC nel 2009, il direttore designato del SIC (*Markus Seiler*) ha provveduto all'armonizzazione delle disposizioni dell'OMSI e dell'OSINF concernenti le eccezioni all'obbligo di archiviazione. Il nuovo articolo 28 capoverso 2 dell'ordinanza sul Servizio delle attività informative della Confederazione (O-SIC)[13] ha abrogato l'obbligo di offrire per l'archiviazione all'AFS tutti i documenti classificati provenienti da relazioni dirette con servizi di intelligence stranieri e quelli provenienti dalla ricerca di informazioni operativa. Questa disposizione si applicava retroattivamente a tutti i documenti che non erano ancora stati forniti. La distruzione irreversibile, già praticata dal SAP, dei fascicoli provenienti da relazioni con servizi stranieri è stata espressamente estesa nell'ordinanza ai documenti provenienti dalla ricerca di informazioni operativa. A tenore della disposizione, tale distruzione era tuttavia consentita soltanto dopo una durata di conservazione di 45 anni.

Dal punto di vista della DelCG queste nuove norme derogatorie che il Consiglio federale aveva accordato al SIC non erano conciliabili con le nuove basi legali che reg-

10 Legge federale del 3 feb. 1995 sull'esercito e sull'amministrazione militare (legge militare, LM; RS **510.10**).
11 Messaggio del 24 ott. 2001 concernente la riforma Esercito XXI e la revisione della legislazione militare (FF **2002** 768, qui 788).
12 Ordinanza del 26 sett. 2003 sui servizi d'informazione del DDPS (OSINF; RU **2003** 4001).
13 Ordinanza del 4 dic. 2009 sul Servizio delle attività informative della Confederazione (O-SIC; RU **2009** 6937).

gono il SIC concepite dalla Delegazione stessa nell'ambito dell'iniziativa parlamentare (Iv. Pa.) Hofmann[14]. La nuova legge federale sul servizio informazioni civile (LSIC)[15] ha abrogato le disposizioni sulla protezione delle fonti della LM e della LMSI e, per quest'ultima, anche la legittimazione riconosciuta dal Consiglio federale alla distruzione di documenti provenienti da relazioni con servizi partner. Secondo l'articolo 7 LSIC, vanno protette in ogni caso solo le persone che sono esposte a pericolo a causa della loro attività informativa sull'estero. Tuttavia, questa disposizione non era pensata per servire a eludere le prescrizioni della LAr.

Dopo aver chiesto un parere all'Ufficio federale di giustizia (UFG) e, all'inizio del 2011, aver condotto audizioni con il direttore dell'AFS e alcuni rappresentanti del SIC, la DelCG ha deciso di proporre che fosse esplicitamente prescritto nella legge, alla prima occasione, l'archiviazione completa e sicura di tutti i fascicoli del SIC[16]. Ha ritenuto che questo modo di procedere fosse appropriato poiché, in assoluta buona fede, ha presupposto che la distruzione di altri documenti fosse esclusa a breve termine in considerazione della durata di conservazione di 45 anni.

Le Camere federali hanno dato seguito alle proposte della DelCG prima nel 2013, con la revisione della LSIC, poi l'anno successivo, in occasione dei dibattimenti concernenti la legge federale sulle attività informative (LAIn)[17]. Nel 2019 la DelCG ha cominciato a verificare l'attuazione della nuova disposizione in materia di archiviazione. Da un rapporto che il SIC aveva redatto nel maggio 2019 all'attenzione della DelCG, quest'ultima ha dovuto tuttavia concludere che, anche tra il 2011 e il 2014, il SIC aveva distrutto irreversibilmente documenti provenienti dai servizi partner dell'ex SAP. Secondo le spiegazioni fornite dal SIC nel novembre 2019, ciò era avvenuto nel passaggio a una nuova versione del Sistema d'informazione sicurezza interna (ISIS)[18].

Di conseguenza la DelCG ha pregato il capo del DDPS (*Viola Amherd*) di verificare la legalità della distruzione di questi dati e di individuare chi ne fosse responsabile. Secondo un rapporto complementare del 3 marzo 2020 del SIC e in occasione del colloquio del 25 maggio 2020 con la responsabile del DDPS, questo Dipartimento ha ritenuto legale la distruzione dei fascicoli contestata dalla DelCG. Secondo le spiegazioni fornite dal direttore del SIC (*Jean-Philippe Gaudin*), la distruzione dei fascicoli effettuata prima della scadenza del termine di conservazione di 45 anni si sarebbe fondata anche sul parere formulato dall'UFG nel 2010.

2.2 Valutazione della DelCG

L'opinione pubblica, così come il Parlamento, ha esortato la DelCG a fare piena luce, con la sua ispezione, sulle attività dei servizi delle attività informative, alcune delle

14 Iv. Pa. Hofmann del 13 mar. 2007 «Trasferimento dei compiti dei servizi informazioni civili a un dipartimento» (07.404).
15 Legge federale del 3 ott. 2008 sul servizio informazioni civile (LSIC; RU **2009** 6565).
16 Rapporto annuale 2013 del 31 gen. 2014 delle CdG e della DelCG, n. 4.4 (FF **2014** 4291, qui 4363).
17 Legge federale del 25 sett. 2015 sulle attività informative (LAIn; RS **121**).
18 Prima del 2010 l'acronimo ISIS stava per «Sistema informatizzato per il trattamento dei dati relativi alla protezione dello Stato», successivamente ha designato il «Sistema d'informazione sicurezza interna».

quali risalivano a più di 40 anni prima. La DelCG vuole quindi sottolineare che in passato il legislatore ha attribuito troppa poca importanza all'archiviazione nelle attività informative. In questo ambito un'archiviazione corretta è garantita a livello di legge soltanto dal novembre 2014, tra l'altro grazie anche all'impegno profuso dalla DelCG.

Occorre inoltre osservare che il Consiglio federale ha permesso per decenni ai servizi delle attività informative di sottrarre su vasta scala documenti importanti all'archiviazione. Ancora nel maggio 2020 il DDPS era pronto a giustificare la distruzione palesemente illegale di documenti molto recenti del SIC riferendosi, in contraddizione con i fatti, a un parere dell'UFG richiesto dalla stessa DelCG. La Delegazione giudica questo atteggiamento incomprensibile.

In retrospettiva è emerso anche che il Consiglio federale aveva previsto deroghe all'obbligo di archiviazione per i servizi delle attività informative senza un piano e in modo contraddittorio. Apparentemente né il SIC, né il DDPS né il Consiglio federale hanno un'idea chiara di quali tipi di documenti sono stati archiviati, non ancora archiviati o distrutti dai servizi delle attività informative negli ultimi decenni. L'attuale direttore del SIC (*Jean-Philippe Gaudin*) era in carica da più di un anno quando ha appreso dell'esistenza di documenti depositati in quella che una volta era un'installazione K.

Dalle sue investigazioni la DelCG ipotizza che i fascicoli ritrovati facciano luce sulle attività della Polfed in relazione con la Crypto AG in misura tale da dare all'alta vigilanza una base di informazioni idonea a consentire una valutazione di principio. Tuttavia la DelCG non ha alcuna garanzia che tutti i fascicoli riguardanti le attività di prevenzione della polizia in riferimento alla Crypto AG siano stati conservati e trasferiti nell'installazione K del SIC. Se in futuro fosse necessario indagare le relazioni della Polfed o del SAP con partner esteri, la DelCG può affermare già oggi che, a causa della prassi di distruzione degli incartamenti consentita dal Consiglio federale, i fondi di documenti non sono completi.

Per l'ispezione della DelCG è da considerare una fortuna che importanti fascicoli riguardanti la Crypto AG siano stati conservati dal SIC al proprio interno e siano stati ritrovati completi nell'installazione K. Vi ha sicuramente contribuito anche la direttiva emanata nel 2001 dall'allora direttore del SIC (*Hans Wegmüller*) che vietava l'ulteriore distruzione di documenti, tuttavia non esiste alcuna garanzia che gli incartamenti riguardanti altre e, in particolare, meno recenti attività di ricerca svolte dal Servizio informazioni militare esistano ancora in una qualità paragonabile.

Secondo la DelCG, l'attuale ispezione ha inoltre evidenziato che la distruzione dei documenti non è un mezzo efficace di protezione delle fonti e che può addirittura pregiudicare questo obiettivo. Occorre considerare infatti che spesso il SIC non è il solo a conoscere l'esistenza delle sue fonti. La fonte stessa, eventualmente i suoi familiari o anche altri servizi con i quali il SIC collabora alla ricerca di informazioni potrebbero sapere della sua attività al servizio della Svizzera.

Se la fonte è scoperta da altri senza che vi sia colpa da parte del servizio delle attività informative svizzero, il SIC deve sapere comunque dell'esistenza di questa fonte perché solo così può continuare a proteggerla nei limiti delle sue possibilità. Se queste informazioni non sono più disponibili, c'è il rischio che la reazione del SIC, del DDPS

o del Consiglio federale esponga a maggiori pericoli la suddetta fonte. A seconda della situazione, la distruzione dei documenti frutto della ricerca operativa può impedire al SIC di adempiere o di continuare ad adempiere il suo obbligo legale di protezione delle fonti sancito dall'articolo 35 LAIn.

L'ispezione compiuta dalla DelCG dimostra ancora una volta l'importanza della direzione politica del servizio delle attività informative. Deve dunque essere possibile stabilire se e come i capidipartimento si assumono la propria responsabilità di condotta diretta. La DelCG è pertanto convinta dell'importanza che i colloqui sulla gestione siano verbalizzati in modo tracciabile e che tutti i verbali siano archiviati in sicurezza.

3 Attività della Polizia federale

3.1 Riepilogo dei fatti

3.1.1 Caso «Code»

Nel 1977 l'allora capo del settore Ricerca e Sviluppo della Crypto AG si è rivolto alla Polfed con l'intermediazione di membri del Comando dell'esercito che aveva conosciuto durante il servizio militare. Secondo le sue dichiarazioni, la società apparteneva a organizzazioni tedesche e americane attive nella ricerca di informazioni e, su loro ordine, inseriva intenzionalmente falle negli apparecchi destinati all'estero. Secondo quanto da lui denunciato, i servizi di intelligence stranieri erano così in grado di decrittare e leggere i messaggi cifrati.

Per fare luce su queste accuse, la Polfed si è rivolta all'Ufficio federale delle truppe di trasmissione (UFTRM). Nell'aprile 1979 l'UFTRM aveva consigliato di procurarsi un apparecchio sospetto all'estero e di analizzarlo per procedere a investigazioni più approfondite. Il servizio giuridico del Ministero pubblico della Confederazione (MPC) ha presentato un'analisi circostanziata delle presunte fattispecie penali nel luglio del 1979, in particolare nell'ambito del servizio vietato delle attività informative. Nell'agosto dello stesso anno, da un colloquio tra il procuratore generale della Confederazione (*Rudolf Gerber*), il capo della Polfed (*André Amstein*) e altri rappresentanti del MPC è emerso che non era possibile escludere il coinvolgimento della Crypto AG in attività informative e che era opportuno seguire la proposta dell'UFTRM. Dal momento che le investigazioni volute dall'UFTRM presso un opportuno Stato estero andavano per le lunghe, il capo della Polfed ha deciso, nel marzo 1980, di rinunciare a svolgere una procedura d'indagine di polizia giudiziaria fino a nuovo avviso.

È stato necessario attendere fino al 1982 perché l'UFTRM potesse accedere a un apparecchio di cifratura idoneo di uno Stato limitrofo. L'anno successivo l'Ufficio federale è giunto alla conclusione che le accuse secondo cui gli apparecchi sarebbero stati modificati non potevano essere né confermate né completamente confutate. È stato comunque constatato che esisteva una discrepanza tra il circuito logico e la descrizione nella documentazione per gli utenti, pertanto non era possibile escludere completamente la tesi della manipolazione.

Non si sono trovate tracce scritte della reazione da parte del MPC o della Polfed a quest'ultima presa di posizione dell'UFTRM. Tuttavia emerge che l'UFTRM ha rivolto una maggiore attenzione alla sicurezza degli apparecchi utilizzati in Svizzera, con la conseguenza che non c'erano più risorse a disposizione per la questione sollevata dalla Polfed in materia di attività informative.

3.1.2 Operazione «Rötel»

Nel 1988 è stato constatato che i servizi di intelligence dei Paesi aderenti al Patto di Varsavia cercavano di procurarsi apparecchi di cifratura della Crypto AG con l'intermediazione di terzi. Nello stesso periodo la Polfed ha ricevuto informazioni da parte della Crypto AG in merito a domande sospette ed elenchi di clienti. Questo flusso di informazioni ha tuttavia avuto una durata limitata, poiché è stato sospeso con l'uscita dalla Polfed del collaboratore competente. Le informazioni ricevute e l'accesso alle informazioni della società sembrano poi essere cadute nel dimenticatoio all'interno della Polfed.

3.1.3 Caso Bühler

Dopo essere stato incarcerato per nove mesi in Iran, Hans Bühler, rappresentante della Crypto AG, è rientrato in Svizzera nel gennaio del 1993 e nello stesso mese è stato interrogato dalla Polfed, in particolare in merito alle accuse di spionaggio che l'Iran aveva formulato nei suoi confronti. Tuttavia non sono subito seguiti accertamenti più approfonditi. Nella primavera del 1993 la Crypto AG ha rescisso il contratto di lavoro di Hans Bühler ed è allora che il caso è giunto all'attenzione dei media.

Quando, nel marzo 1994, l'interesse da parte dei media si è amplificato, la Polfed ha informato il SG-DFGP che la stampa avrebbe presto pubblicato articoli in merito e ha quindi ripreso le investigazioni volte ad accertare, da un lato, il controllo della Crypto AG da parte di servizi di intelligence stranieri, dall'altro l'accusa della manipolazione intenzionale degli apparecchi di cifratura.

Tra marzo e novembre del 1994, nell'ambito delle sue indagini di polizia, la Polfed ha interrogato Hans Bühler una seconda volta e altri 20 collaboratori non più in servizio o ancora attivi nonché membri del consiglio di amministrazione e del comitato consultivo della Crypto AG in qualità di persone informate sui fatti. Solo due degli interrogati hanno potuto riferire di presunte manipolazioni degli apparecchi di cifratura, mentre gli altri avevano sentito voci in tal senso, ma non erano in grado di fornire indicazioni concrete. Queste investigazioni non hanno permesso di confermare i sospetti al punto tale da giustificare l'avvio di una procedura d'indagine di polizia giudiziaria da parte del MPC. Nel suo rapporto finale del 3 maggio 1995 la Polfed ha tuttavia precisato che non era stato possibile identificare i veri proprietari della Crypto AG.

Il DFGP ha assistito la Polfed nelle sue indagini in merito all'assetto proprietario della Crypto AG. Dall'interrogatorio di due membri del comitato consultivo della società non sono giunte risposte soddisfacenti, pertanto il 5 maggio 1994 il segretario generale

del DFGP (*Armin Walpen*) ha pregato insistentemente il consigliere nazionale Georg Stucky, dal 1992 membro del consiglio di amministrazione della Crypto AG, di esercitare la sua influenza al fine di appurare chi fossero i proprietari della società.

In seguito alla pubblicazione del rapporto finale della Polfed, il capo del DFGP (*Arnold Koller*) lo ha inviato al capo di quello che allora era il DMF (*Kaspar Villiger*) e, nella lettera di accompagnamento del 2 giugno 1995, ha menzionato che il rapporto avrebbe potuto rivelarsi utile in un eventuale colloquio con il consigliere nazionale Stucky per chiarire la questione aperta. Del colloquio non c'è traccia nei documenti, ma sembra convalidare l'ipotesi che non abbia avuto luogo il fatto che il capo del DFGP, in base a una nota del suo segretario generale di fine giugno 1995, aveva l'intenzione di parlare personalmente con il consigliere nazionale Stucky affinché l'assetto proprietario della Crypto AG fosse reso noto. Il capo del DFGP ha dichiarato alla DelCG di avere supposto che l'incontro non avesse avuto luogo.

In base alle investigazioni condotte dalla DelCG, in particolare presso la Cancelleria federale, niente lascia supporre che il rapporto finale della Polfed sia stato discusso in seno al Consiglio federale o che le conclusioni a cui è giunto siano state pubblicate. Nel luglio 1997 la Polfed ha inviato una lettera alla Crypto AG, su richiesta di quest'ultima, nella quale erano sintetizzati i risultati degli accertamenti, in ultima istanza rimasti senza esito.

3.1.4 Informazioni trasmesse all'organo di alta vigilanza

La DelCG ha ripetutamente chiesto informazioni sulle investigazioni svolte dalla Polfed in merito al caso Bühler. Il 24 marzo 1994 il capo della Polfed (*Urs von Daeniken*) ha assicurato all'organo di alta vigilanza parlamentare che l'autorità competente avrebbe chiarito la questione dei veri proprietari della Crypto AG. Poco dopo la DelCG ha chiesto alla Polfed di sottoporle un rapporto scritto che la mettesse al corrente dello stato del procedimento e dei risultati delle investigazioni.

Con lettera del 27 maggio 1994 il capo della Polfed ha informato la DelCG che, fino a quel momento, non era emerso alcun sospetto concreto di un atto punibile, pertanto non sarebbe stata avviata una procedura di polizia giudiziaria. Secondo lui, le persone convocate non hanno potuto o voluto fornire indicazioni precise sulla presunta influenza dei servizi segreti tedeschi o americani. Il capo della Polfed ha concluso che non era possibile dimostrare la fondatezza delle accuse di manipolazione degli apparecchi di cifratura, tuttavia alcuni indizi inducevano la Polfed a credere nell'esistenza di due livelli diversi di qualità nella cifratura. Ha inoltre sorpreso la reticenza della società a rivelare l'identità dei suoi proprietari. In proposito la pista si fermava a una fondazione lussemburghese con una partecipazione tedesca.

La DelCG ha preso atto del contenuto della lettera in occasione della sua seduta di fine giugno 1994. Per quanto si possa dedurre retrospettivamente dai fascicoli in materia, alla DelCG non sono state trasmesse ulteriori informazioni né ne sono state chieste da parte sua.

3.2 Valutazione della DelCG

Guardando alle indagini condotte dalla Polfed negli anni Settanta, Ottanta e Novanta, la DelCG giunge alla conclusione che sono state svolte correttamente in base alle informazioni disponibili, pertanto non danno adito a contestazioni. Non esistono elementi tali da indurre a ritenere che istanze politiche in Svizzera abbiano intralciato o influenzato le indagini o che alcuni fatti siano stati volutamente ignorati o analizzati solo superficialmente.

In particolare, nelle sue indagini condotte negli anni Novanta la Polfed si è avvalsa di tutti gli strumenti di cui disponeva allora. La direzione del DFGP è stata informata tempestivamente ed esaustivamente, il capo del Dipartimento ha preso atto delle indagini, ma non è intervenuto direttamente nel procedimento. Tuttavia, né il capo della Polfed (*Urs von Daeniken*) né il capo del DFGP (*Arnold Koller*) sono rimasti pienamente soddisfatti del risultato delle indagini. Il DFGP ha quindi cercato di approfondire la questione dell'assetto proprietario della Crypto AG tramite canali diversi, anche una volta che le indagini erano concluse. Sembra che la cooperazione cercata con il consigliere nazionale Stucky, membro del consiglio di amministrazione della società, non si sia mai concretizzata.

Secondo il rapporto MINERVA, ma anche in base ad altri documenti che la DelCG ha pubblicato nel quadro della sua ispezione, la direzione della Crypto AG ha comunicato l'identità dei veri proprietari della società al consigliere nazionale Stucky. È presumibile che queste informazioni siano confluite nei summenzionati rapporti a partire dalla direzione, di cui alcuni membri erano a conoscenza della proprietà della società. Queste persone sapevano anche quali membri del consiglio di amministrazione le avevano informate. Nel maggio del 2020 l'ex consigliere nazionale Stucky ha tuttavia dichiarato alla DelCG di non sapere di aver lavorato per una società nelle mani dei servizi segreti americani.

In base a quanto emerge dal rapporto MINERVA, il consigliere nazionale Stucky avrebbe confidato all'allora capo del DMF (*Kaspar Villiger*) chi fossero i veri proprietari della Crypto AG. Questa informazione e le corrispondenti indicazioni figuranti in altri documenti di cui la DelCG è in possesso confermano che la direzione della Crypto AG ritenesse avvenuto il colloquio tra il consigliere nazionale Stucky e il capo del DMF. In base ai documenti consultati e alle audizioni svolte, la DelCG non è riuscita a capire se e in quale forma questo colloquio abbia effettivamente avuto luogo. L'allora capo del DMF ha tuttavia dichiarato alla DelCG che un colloquio in merito alla Crypto AG con il consigliere nazionale era presumibilmente avvenuto durante il caso Bühler, ma non ricordava di essere mai stato informato sui veri proprietari della Crypto AG e dell'operazione in materia di attività informative menzionata nel rapporto MINERVA.

4 Attività dei servizi del DMF e del DDPS

4.1 Riepilogo dei fatti

4.1.1 Accesso alle informazioni del SIS

A partire dall'autunno 1993 il SIS[19] è riuscito a ottenere informazioni attendibili in merito alla società Crypto AG. Ha così appreso che apparteneva ai servizi di intelligence americani e tedesco e, più tardi, che il servizio tedesco aveva posto fine alla sua partecipazione (cfr. n. 2.1.1). Il SIS ha saputo anche che la società esportava apparecchi «deboli», la cui cifratura poteva essere violata con uno sforzo contenuto, a differenza di quanto avveniva per gli apparecchi «forti».

Il SIS si è posto l'obiettivo di violare sistematicamente la cifratura degli apparecchi «deboli». Si è quindi procurato informazioni tecniche sulla procedura di cifratura degli apparecchi esportati. Tali conoscenze hanno potuto essere utilizzate anche per identificare eventuali procedure di cifratura «deboli» negli apparecchi acquistati dalla Svizzera.

In seguito al caso Bellasi[20], il Gruppo servizio informazioni (GSI) è stato sciolto e il SIS trasformato in un ufficio federale civile all'inizio del 2001. Sotto la guida del suo primo direttore (*Hans Wegmüller*), il SIS si è sforzato di garantire l'ulteriore ricerca di informazioni in merito alle procedure di cifratura «deboli» utilizzate dalla Crypto AG, ma in ultima istanza è stato possibile solo perché i servizi di intelligence americani erano d'accordo che la Svizzera ottenesse le informazioni auspicate in misura finalizzata allo scopo.

Per sfruttare le conoscenze acquisite in merito alle procedure di cifratura «deboli» al fine di procurarsi informazioni pertinenti a livello di politica di sicurezza, il SIS ha dovuto ottenere sistematicamente l'accesso a comunicazioni crittate. L'esplorazione radio è stata eseguita dalla Base d'aiuto alla condotta dell'esercito (BAC) su incarico del SIS. Dopo la modernizzazione dei sistemi di esplorazione delle onde corte, a partire dal 2000 sono state potenziate le capacità di esplorazione dei collegamenti dei satelliti di comunicazione[21]. Nel 2006 il sistema «Onyx» è passato alla piena operatività nella configurazione prevista. Le competenze in materia di decrittazione sono state quindi integrate nel processo di esplorazione radio gestito dal SIS.

19 Per conoscere meglio come il SIS fosse integrato nell'organizzazione del Dipartimento competente tra il 1985 e il 2009, cfr. l'esame dei contatti del Servizio informazioni svizzero con il Sudafrica ai tempi dell'apartheid, rapporto del 18 ago. 2003 della DelCG, n. 4.3.1 (FF **2004** 1981, qui 1998, 1999, 2001).

20 Eventi accaduti nel Gruppo servizio informazioni dello Stato maggiore generale («caso Bellasi»), rapporto del 24 nov. 1999 della DelCG (FF **2000** 502).

21 Sistema di esplorazione delle comunicazioni via satellite del Dipartimento federale della difesa, della protezione della popolazione e dello sport (progetto «Onyx»). Rapporto del 10 nov. 2003 della DelCG (FF **2004** 1299).

4.1.2 Informazioni fornite agli organi superiori e ai consiglieri federali

La ricerca di informazioni concernente la Crypto AG era un segreto ben custodito all'interno del SIS. Ne erano a conoscenza soltanto il capo del servizio (*Fred Schreier*), i successivi direttori (*Hans Wegmüller, Paul Zinniker*) e, a seconda del momento, uno o due dei suoi membri. Quando il SIS era subordinato al GIS, la gerarchia militare non era al corrente di questa attività.

Il SIC è nato nel 2010 dall'accorpamento del SIS e del SAP. Un anno prima quest'ultimo era stato trasferito dal DFGP al DDPS in seguito all'iniziativa parlamentare Hofmann[22]. Il direttore del nuovo servizio (*Markus Seiler*), nel primo anno del suo mandato (2010), è stato informato dell'esistenza di apparecchi «deboli» della Crypto AG e, almeno a grandi linee, delle relazioni tra la Crypto AG e i servizi americani. Nell'ultimo anno del suo mandato (2017) gli è stato mostrato anche che cosa aveva permesso al Servizio informazioni svizzero di utilizzare questa procedura di cifratura «debole». Nel contempo gli è stato spiegato che per il SIC era necessario agire presentandogli le opzioni possibili. Tuttavia, il direttore del SIC non si è ritenuto responsabile in materia e si è rifiutato di accettare una nota informativa al riguardo. Il suo sostituto (*Paul Zinniker*), già informato ai tempi del SIS, ha appoggiato la decisione del suo direttore di non attivarsi ulteriormente su questo dossier.

I predecessori dell'attuale responsabile del DDPS non sono stati informati né dal SIS né, successivamente, dal SIC che la Crypto AG era controllata dai servizi di intelligence americani e che il Servizio informazioni svizzero era a conoscenza delle procedure di cifratura «deboli», che sfruttava per la ricerca di informazioni nell'ambito delle attività informative.

4.1.3 Informazioni fornite all'attuale responsabile del DDPS e al Consiglio federale

Nella primavera del 2019, l'attuale direttore del SIC (*Jean-Philippe Gaudin*) ha ricevuto, nella sostanza, le stesse informazioni che erano state fornite al suo predecessore due anni prima ma, a differenza di quest'ultimo, ha ritenuto che fosse necessario agire. Ha quindi chiesto un resoconto dettagliato e, a metà giugno 2019, ha incaricato di stilare un bilancio della situazione.

Verso la fine di giugno del 2019, il SIC è stato informato tramite canali vicini agli ambienti delle attività informative che i media americani e tedeschi stavano indagando sulla Crypto AG e sul ruolo che la società aveva svolto in un'operazione di ricerca di informazioni su vasta scala condotta dai servizi di intelligence americani e tedesco. Questo sviluppo casuale della situazione ha indotto ad accelerare le investigazioni ordinate dal direttore del SIC.

In occasione della seduta di direzione dell'ufficio del 19 agosto 2019, il direttore del SIC ha informato la responsabile del DDPS che la Crypto AG aveva collaborato con

22 Iv. Pa. Hofmann del 13 mar. 2007 «Trasferimento dei compiti dei servizi informazioni civili a un dipartimento» (07.404).

i servizi di intelligence stranieri. Dalle note manoscritte su questo incontro risulta la menzione che anche il Servizio informazioni svizzero aveva potuto sfruttare le falle introdotte nelle procedure di cifratura della società.

Il bilancio della situazione chiesto dal direttore del SIC si è concluso a metà settembre del 2019. Uno dei due esemplari del rapporto, che era considerato a uso esclusivo del Servizio, è stato consegnato al direttore del SIC, l'altro al capo della divisione Supporto alla condotta e all'impiego (NDBU). Solo all'inizio di novembre del 2019 sono stati predisposti altri esemplari per il capo in servizio della divisione Ricerca del SIC (NDBB), che nel 1994 aveva diretto le investigazioni della Polfed, e per un altro membro della direzione del SIC. Il documento conteneva tutte le informazioni rilevanti per comprendere le relazioni tra i servizi delle attività informative del DDPS e i servizi americani e il loro operato con la Crypto AG. Per quanto possibile, analizzava anche le conseguenze della scissione della società che aveva avuto luogo l'anno precedente. Al documento non è stato dato seguito all'interno del SIC né le informazioni rilevanti sul piano politico che conteneva sono state trasmesse alla responsabile del DDPS.

A metà ottobre 2019 il SIC è entrato in possesso del rapporto MINERVA (cfr. n. 2.1.1) e il direttore del SIC è stato messo al corrente del contenuto. A partire da fine ottobre, lo scambio di informazioni tra il SIC, i servizi americani e altri servizi stranieri implicati si è intensificato. L'obiettivo era di garantire che tutti disponessero delle stesse informazioni e di anticipare le conseguenze delle rivelazioni dei media sul rapporto MINERVA.

In occasione della seduta di direzione dell'ufficio del 31 ottobre 2019, il direttore del SIC ha nuovamente sollevato la questione Crypto AG, informando la responsabile del DDPS che anche i media svizzeri stavano conducendo un'inchiesta e riferendo dei colloqui intercorsi tra il SIC e i servizi stranieri coinvolti. A seguito di ciò, il DDPS ha elaborato una nota sulle implicazioni della Crypto AG nelle attività informative destinata alla seduta del Consiglio federale del 6 novembre 2019. La nota sottolineava che i servizi informazioni svizzeri non erano mai stati direttamente coinvolti in questa operazione condotta da servizi stranieri, ma che ne avevano beneficiato indirettamente poiché avevano potuto procurarsi le relative conoscenze tecniche. Tuttavia, queste affermazioni riflettevano solo in parte le rilevanti conclusioni sul piano politico e la necessità di intervenire che sono emerse dal bilancio della situazione di metà settembre 2019, poiché il SIC ha sottoposto tale bilancio alla responsabile del DDPS solo a metà febbraio 2020.

4.1.4 Informazioni trasmesse all'organo di alta vigilanza

Se la DelCG si era occupata a più riprese nel 1994 dell'indagine condotta dalla Polfed sulla Crypto AG, fino al 2019 la società stessa non era mai stata oggetto di discussione tra l'organo di alta vigilanza e i servizi del DMF e del DDPS. È stata invece più volte affrontata la sicurezza degli strumenti di comunicazione della Confederazione e l'utilizzo della crittologia. Nel 2007, la DelCG ha appreso dal direttore del SIS che l'ampliata collaborazione in materia di crittologia con un partner europeo aveva conseguenze positive anche sullo scambio di informazioni nell'ambito dell'esplorazione radio.

Sempre nel 2007, la DelCG aveva chiesto di essere informata sull'utilizzo della crittologia nel DDPS e le è stata spiegata l'integrazione della decrittazione nel processo di esplorazione delle comunicazioni. Da una scheda informativa è emerso, tra l'altro, che numerosi produttori di apparecchi di cifratura inserivano intenzionalmente falle per determinati clienti e che i servizi di intelligence degli Stati Uniti e di alcuni loro alleati erano all'origine di questa pratica. Tuttavia, anche altri Paesi che disponevano delle competenze necessarie, tra cui la Svizzera, potevano trarne vantaggio. L'obiettivo principale della decrittazione era scoprire queste backdoor, che consentono di introdursi nei sistemi informatici.

Per approfondire il tema della crittologia, nel maggio 2009 la DelCG ha svolto un'altra audizione, ma neppure in questa occasione è stata informata che procedure di cifratura di società con sede in Svizzera venivano manipolate per conto di servizi di intelligence stranieri e che, con il consenso di questi, la Svizzera era a conoscenza delle falle. La discussione riguardava la questione della sicurezza degli apparecchi acquistati dalla Svizzera.

Il 12 novembre 2019 il DDPS ha informato per la prima volta oralmente il presidente della DelCG (*Claude Janiak*) del caso Crypto AG. In seguito a questo incontro, il presidente della DelCG ha consegnato alla responsabile del DDPS una copia riservata del verbale dell'audizione condotta dalla DelCG nel maggio 2009. Ciò è avvenuto poiché si aveva l'impressione che al DDPS occorressero tutti i dati disponibili per completare le sue scarse conoscenze su questo dossier.

Il 25 novembre 2019 la DelCG è stata ufficialmente informata in qualità di organo di alta vigilanza. Secondo il direttore del SIC, la Svizzera era a conoscenza delle implicazioni dei servizi di intelligence americani nella Crypto AG e ha fatto risalire i fatti rilevanti ancora alla Guerra fredda, senza riferimenti al presente. A suo parere, la Svizzera aveva potuto trarre vantaggio da queste conoscenze nell'ambito delle sue attività informative, ma né il SIC né le organizzazioni che lo hanno preceduto avevano avuto rapporti con la Crypto AG al riguardo. Secondo il direttore del SIC, si trattava di una vecchia questione alla quale non si doveva riservare un'eccessiva importanza.

La responsabile del DDPS, a sua volta, non ha intravisto alcun rischio di reputazione per la Svizzera, poiché la Confederazione non deteneva partecipazioni nella Crypto AG né era in qualche modo collegata con essa. Inoltre, la società non aveva bisogno né di licenze né di autorizzazioni da parte della Confederazione. Sotto la direzione del DDPS è stato quindi costituito un gruppo di lavoro interdipartimentale (GLID) per accertare i fatti in questo caso complesso e garantire una politica di comunicazione coerente verso i media da parte dell'intero Consiglio federale (cfr. n. 6.1.1).

Nella seduta del 25 novembre 2019, il DDPS si è impegnato a consegnare alla DelCG un rapporto di sintesi sulle ulteriori investigazioni svolte, ma questo rapporto non è mai stato redatto. Inoltre, nonostante le ripetute richieste da parte della segreteria della DelCG, la SG-DDPS non è stata in grado di sottoporle una copia della nota informativa elaborata dal DDPS per la seduta del Consiglio federale del 6 novembre 2019. Il documento è stato trasmesso solo dopo che la DelCG ha avviato l'ispezione.

4.2 Valutazione della DelCG

4.2.1 Legalità della ricerca di informazioni (prima del 2002)

Quando, nell'autunno 1993, il SIS ha cominciato a procurarsi informazioni riguardanti gli apparecchi di cifratura «deboli» della Crypto AG, non esistevano ancora basi legali specifiche per il servizio informazioni dell'esercito concernente l'estero. Il Consiglio federale aveva tuttavia già proposto una disposizione in tal senso nel suo messaggio dell'8 settembre 1993[23] sulla nuova legge militare. Intendeva così dare seguito anche agli interventi della commissione parlamentare d'inchiesta DMF (CPI DMF)[24].

Nella nuova legge militare, entrata in vigore il 19 giugno 1995, il compito del SIS era descritto in modo molto vago: «raccogliere [...] informazioni concernenti l'estero rilevanti sotto il profilo della politica di sicurezza» (art. 99 cpv. 1 LM).

Secondo il messaggio sulla LM, erano intese le «informazioni concernenti tutte le minacce provenienti dall'esterno, che potrebbero richiedere l'impiego dell'esercito o di parti di esso». Negli anni successivi, la nozione di politica di sicurezza è stata sempre più ampliata al di là della difesa nazionale militare, come dimostrato anche dalla trasformazione del SIS in un ufficio federale civile nel 2001. Le basi legali del servizio informazioni civile concernenti l'estero sono state invece trasposte dalla LM alla LSIC solo nove anni dopo.

Il messaggio sulla LM precisava inoltre che dovevano essere raccolte «soltanto le informazioni che non possono essere acquisite con i mezzi accessibili al pubblico o che non possono essere raccolte per tempo». Ciò implicava che per la ricerca di informazioni il SIS poteva utilizzare attivamente mezzi specifici ai servizi informazioni, che si trattasse di fonti umane o di strumenti tecnici tra cui l'esplorazione radio o la decrittazione.

Dal punto di vista della DelCG, ai sensi della LM la ricerca di informazioni sugli Stati che avevano acquistato apparecchi «deboli» dalla Crypto AG e l'acquisizione di conoscenze sulle procedure di cifratura in essi utilizzate dovevano essere rese compatibili con il compito del SIS laddove si trattasse di decrittare le trasmissioni di autorità straniere, in particolare nell'ambito delle forze armate e dei servizi di sicurezza.

Occorreva tuttavia considerare che la Crypto AG sviluppava e produceva i suoi apparecchi in Svizzera, da dove li esportava. La ricerca di informazioni sulla società era dunque consentita solo nella misura in cui serviva in seguito ad acquisire informazioni concernenti l'estero mediante la decrittazione di trasmissioni straniere, mentre il SIS doveva evitare di cercare altre informazioni sulle attività della società o dei suoi dipendenti, il che non si è sempre verificato.

Secondo il messaggio summenzionato, la LM prevedeva una scissione tra il SIS e i servizi civili di difesa e di informazioni (all'epoca Polfed). Per quanto riguarda l'attività in Svizzera, il SIS doveva limitarsi al controspionaggio al suo interno. Se, nello

23 Messaggio dell'8 sett. 1993 a sostegno della legge federale sull'esercito e l'amministrazione militare e del decreto federale sull'organizzazione dell'esercito (FF **1993** IV 1).

24 Iv. Pa. Ufficio CN «Avvenimenti nel Dipartimento militare federale. Commissione parlamentare d'inchiesta» del 13 mar. 1990 (90.022).

svolgimento della sua attività, fosse giunto a conoscenza di atti punibili, avrebbe dovuto attivare le autorità di perseguimento penale.

Sulla base delle sue conoscenze in merito all'inserimento di procedure di cifratura «deboli» negli apparecchi della Crypto AG, il SIS era consapevole che i servizi americani se ne servivano per ricercare informazioni su altri Stati. Sebbene non fosse suo compito ricercare informazioni per provare che servizi di intelligence svolgevano attività vietate, il SIS avrebbe dovuto trasmettere quanto scoperto al controspionaggio e alle autorità di perseguimento penale, soprattutto in considerazione del fatto che la Polfed aveva avviato un'indagine al riguardo. Invece non solo non l'ha fatto, ma ha anche comunicato alla Polfed di non avere indizi tali da lasciar supporre che dietro la Crypto AG si celassero servizi di intelligence stranieri.

Il SIS ha quindi attribuito maggiore importanza alla ricerca di informazioni nell'ambito delle attività informative e al mantenimento di buoni rapporti con i servizi di intelligence americani che al perseguimento penale. La DelCG ritiene che il SIS non fosse abilitato a procedere in tal senso e la summenzionata ponderazione dei diversi interessi avrebbe dovuto avere chiaramente luogo a livello politico.

4.2.2 Legalità della collaborazione con i servizi di intelligence americani (dopo il 2002)

A partire dal momento in cui i servizi americani hanno acconsentito a condividere le conoscenze tecniche sugli apparecchi «deboli» della Crypto AG con il loro omologo svizzero, secondo la DelCG il SIS non poteva più considerare l'operazione come una ricerca segreta di informazioni nei confronti della società, ma una collaborazione in materia di attività informative tra il SIS e il servizio di intelligence straniero.

Secondo l'articolo 99 capoverso 3 lettera c LM, il Consiglio federale doveva disciplinare la collaborazione del servizio informazioni con servizi esteri. Dal momento che ciò non è avvenuto, negli anni Novanta la collaborazione tra il SIS e un servizio partner era lasciata alla discrezione del servizio stesso oppure doveva essere approvata dal capo del Dipartimento[25]. In base alla sua prima ispezione riguardante le relazioni tra il Servizio informazioni svizzero e il Sudafrica, la DelCG ha raccomandato che la competenza di decidere in merito all'instaurazione, al mantenimento e al controllo di contatti regolari con l'estero fosse affidata al Consiglio federale[26].

All'inizio del 2001, quando il SIS è stato trasformato in un ufficio federale civile, il Consiglio federale ha sottoposto a una revisione totale l'OSINF[27], che risaliva al 1995. Secondo l'articolo 6 dell'ordinanza riveduta[28], l'avvio di contatti regolari con un servizio straniero necessitava del consenso del Consiglio federale.

25 Rapporto annuale 2001/2002 del 17 mag. 2002 delle CdG e della DelCG, n. 9.1 (FF **2002** 5297, qui 5327).
26 Relazioni fra la Svizzera e il Sudafrica: ruolo dei Servizi d'informazione svizzeri. Rapporto del 12 nov. 1999 della DelCG (FF **2000** 479, qui 486).
27 Ordinanza del 4 dic. 1995 concernente il servizio informazioni (OSINF; RU **1995** 5298).
28 Ordinanza del 4 dic. 2000 sul servizio informazioni del Dipartimento federale della difesa, della protezione della popolazione e dello sport (OSINF; RU **2001** 124).

Il consenso del Consiglio federale in materia di collaborazione copriva un ampio spettro di attività informative, dallo scambio di dati ai colloqui specialistici tra esperti passando per la gestione comune di fonti o la condotta di operazioni congiunte per la ricerca di informazioni. Vi rientrava anche il transfer di conoscenze in merito alle procedure di cifratura «deboli» negli apparecchi della Crypto AG. Il servizio di intelligence americano, che ha acconsentito alla trasmissione di informazioni sugli apparecchi di cifratura della Crypto AG, figurava sin dall'inizio nell'elenco dei contatti con l'estero approvati dal Consiglio federale.

Come spiegato al numero 4.1.1, l'accesso sistematico del SIS alle informazioni sulle procedure di cifratura della Crypto AG è stato reso possibile unicamente dal benestare dei servizi americani. La DelCG ritiene dunque che il flusso di informazioni basato su questo accordo costituiva una collaborazione in materia di attività informative ai sensi dell'articolo 99 capoverso 3 lettera c LM. Ai fini del parere formulato dall'organo di alta vigilanza è determinante l'esistenza accertata di questa collaborazione, di cui la direzione del SIS era a conoscenza. Secondo la DelCG non sono invece rilevanti le circostanze concrete in cui questa collaborazione è sorta e come si è svolta. È altresì opportuno osservare che l'articolo 99 capoverso 3 lettera c LM era l'unica disposizione legale sulla quale si poteva basare il SIS per accedere a queste informazioni. Tali disposizioni della legge militare sono rimaste in vigore anche dopo l'istituzione del SIC e sono state successivamente integrate nella LAIn (cfr. n. 5.1).

La DelCG ritiene incomprensibile e inesatta in un'ottica giuridica la posizione difesa dai responsabili del SIS, secondo cui non c'è stata alcuna collaborazione del genere tra il SIS e i servizi americani. Questa posizione risultava problematica anche perché serviva da pretesto alla direzione del SIS per non informare l'organo incaricato della sua vigilanza diretta.

In base a quanto comunicato alla DelCG dall'attuale direttore del SIC (*Jean-Philippe Gaudin*), i servizi americani partivano dal principio che anche i successivi responsabili all'interno del Servizio informazioni svizzero sarebbero stati informati della collaborazione. Risulta altresì evidente che i servizi americani erano consapevoli dell'utilità di condividere le conoscenze con il servizio svizzero per garantire la buona riuscita delle loro operazioni. Secondo la DelCG, il fatto che il SIS e i servizi americani agissero di comune accordo implica una corresponsabilità delle autorità elvetiche per le attività della Crypto AG.

4.2.3 Opportunità ed efficacia della ricerca di informazioni

La DelCG giunge alla conclusione che le informazioni ottenute dalla Svizzera grazie alle sue conoscenze in merito alle procedure di cifratura «deboli» degli apparecchi della Crypto AG si sono rivelate utili alle attività informative della Svizzera nel corso degli anni.

Tali conoscenze hanno potuto essere utilizzate direttamente per decrittare le comunicazioni provenienti da Paesi stranieri. Questo know-how ha costituito anche una base preziosa per gli scambi di esperienze e di dati con servizi di intelligence stranieri, il

che ha quindi permesso di migliorare ulteriormente le capacità della Svizzera in materia di decrittazione e di rafforzare la sua posizione sulla scena delle attività informative.

La DelCG conosce casi concreti nei quali le suddette capacità hanno prodotto risultati che hanno consentito alle autorità svizzere e all'esercito di trarre notevoli vantaggi. Occorre tuttavia osservare che le procedure di cifratura e l'accesso alle comunicazioni rilevanti erano soggette a un'evoluzione continua, pertanto il know-how acquisito poteva rivelarsi ben presto privo di valore.

Per la sicurezza della Svizzera è necessario che gli apparecchi di cifratura acquistati per le proprie autorità siano sicuri. La capacità di verificarne la sicurezza e quella di sfruttare le loro vulnerabilità sono inevitabilmente legate. Come risultato dall'ispezione condotta dalla DelCG, la Svizzera è riuscita a identificare queste falle in diversi tipi di apparecchi e a eliminarle. È emerso anche quanto sia importante conoscere bene i fornitori nel proprio Paese e poter influenzare la qualità dei loro prodotti. Vi hanno notevolmente contribuito le informazioni ottenute dal servizio delle attività informative.

4.2.4 Opportunità della vigilanza e della condotta esercitate dai capi del DMF e del DDPS.

Prima della sua trasformazione in un ufficio federale civile, il SIS faceva parte del GSI, che era subordinato al capo dello Stato maggiore generale. La ricerca di informazioni sulla Crypto AG ha avuto luogo senza che il comando militare lo sapesse. Ciò solleva interrogativi in particolare in merito al funzionamento interno del GSI che tuttavia non sono stati approfonditi dalla DelCG nell'ambito di questa ispezione.

L'allora capo del DMF (*Kaspar Villiger*) non era direttamente coinvolto nella condotta del SIS militare. Come risulta da una nota informativa del SIS redatta nel marzo 1994 in merito al caso Bühler, non era stato messo a conoscenza dei veri proprietari della Crypto AG sebbene il capo del SIS (*Fred Schreier*) sapesse nel frattempo chi fossero. Nel contempo, il capo del DMF era abbastanza preoccupato delle accuse rivolte alla società, tanto che ha cercato di ottenere informazioni dai competenti specialisti delle truppe di trasmissione in merito alla sicurezza degli apparecchi di cifratura dell'esercito.

In qualità di ufficio federale civile, il SIS era posto sotto la direzione politica del DDPS e, dal 2004, addirittura subordinato direttamente al capo del Dipartimento ai sensi dell'articolo 99 capoverso 5 LM. Dall'ispezione condotta dalla DelCG non sono emerse indicazioni che il direttore del SIS (*Hans Wegmüller*) abbia informato il suo capo Dipartimento (*Samuel Schmid*) delle relazioni esistenti tra i servizi di intelligence americani e la Crypto AG e dei dati ai quali il SIS aveva accesso. Tuttavia, in base alla valutazione giuridica della DelCG secondo la quale il SIS civile ha in ultima istanza collaborato con i servizi americani, il capo del DDPS avrebbe dovuto essere imperativamente informato.

Stando a quanto appreso dalla DelCG nelle note manoscritte del capo del DDPS negli anni dal 2002 al 2008 (cfr. n. 2.1.2), la sicurezza degli apparecchi di cifratura della

Confederazione è stata oggetto di diverse discussioni tra il direttore del SIS e il capo del DDPS. Quando è emerso che un produttore svizzero (non la Crypto AG) aveva fornito apparecchi poco affidabili alla Confederazione e a due grandi società, il DDPS ha adottato le necessarie misure per colmare queste lacune. Il capo del DDPS è stato tenuto regolarmente al corrente degli sviluppi del caso dal SIS.

Il SIC e la sua nuova direzione hanno cominciato a operare nel 2010. Dal punto di vista della DelCG, il primo direttore del SIC (*Markus Seiler*) si è sottratto alle sue responsabilità quando, nel 2017, gli sono stati forniti chiari indizi concernenti la Crypto AG e si è rifiutato di ricevere le informazioni in forma scritta. Con il suo comportamento ha impedito soprattutto che la direzione politica del Dipartimento potesse trattare gli aspetti rilevanti della questione. In retrospettiva, l'omissione del primo direttore del SIC appare tanto più grave poiché all'epoca il SIC avrebbe ancora potuto preparare senza urgenza le necessarie decisioni di condotta e attuarle d'intesa con direzione del Dipartimento e, eventualmente, con il Consiglio federale. Quando, due anni dopo, il SIC ha dovuto affrontare il problema, la situazione era molto più difficile a causa della pressione mediatica.

La DelCG non dispone di indicazioni che il primo direttore del SIC sia stato informato della portata del problema concernente la Crypto AG dal suo sostituto (*Paul Zinniker*), che era stato direttore del SIS e, all'interno del servizio, era stato personalmente coinvolto nella genesi del caso Crypto AG (cfr. n. 4.1.2). Quando il suo superiore gerarchico ha assunto la funzione di segretario generale del Dipartimento degli affari esteri (DFAE), egli ha diretto il SIC ad interim dal dicembre 2017 fino al luglio 2018. Al passaggio delle consegne all'attuale direttore del SIC (*Jean-Philippe Gaudin*), la Crypto AG non era oggetto di discussione. Tuttavia, dal punto di vista della DelCG, il direttore del SIC avrebbe dovuto essere esaustivamente informato dal suo sostituto al più tardi nell'estate del 2019, quando i media hanno cominciato a interessarsi al caso Crypto AG (cfr. n. 4.1.3).

In queste circostanze, gli ex capi del DMF e del DDPS non hanno potuto assumere le proprie responsabilità di condotta. Secondo la DelCG, ciò sarebbe stato tuttavia essenziale e non doveva essere a esclusiva discrezione dei diretti responsabili all'interno del servizio delle attività informative.

4.2.5 Opportunità del modo di procedere dell'attuale SIC e delle informazioni fornite alla responsabile del DDPS

Nella primavera 2019, l'attuale direttore del SIC ha ricevuto sostanzialmente le stesse informazioni del suo predecessore nel 2017. Ha quindi colto l'occasione per chiedere che fosse stilato un bilancio della situazione concernente il caso Crypto AG, che doveva servire anche a mettere in luce la necessità per il SIC di agire. Inoltre, il direttore del SIC ha richiamato in tempo utile l'attenzione della responsabile del DDPS sull'interesse che i media stavano cominciando a riservare alla Crypto AG.

La DelCG deplora, tuttavia, che la direzione del SIC non sia riuscita, dopo aver ricevuto il suddetto bilancio scritto della situazione, a inquadrare correttamente il ruolo del suo proprio servizio in qualità di organo subentrato al SIS e a trarne le debite

conseguenze politiche. In particolare, il direttore del SIC avrebbe dovuto provvedere affinché, in seno al suo servizio, fossero rapidamente raccolte tutte le informazioni disponibili per sottoporle a un'analisi approfondita. Avrebbe dovuto affidare questo compito a una persona competente, dotata della necessaria esperienza.

Dal momento che il nuovo direttore del SIC non era stato informato della situazione dal direttore ad interim e poi sostituto (cfr. n. 4.2.4), quindi la conseguente valutazione è stata incompleta e inadeguata, gli sforzi del servizio e del DDPS erano soprattutto finalizzati, nell'autunno del 2019, ad anticipare le domande e i resoconti dei media e ad elaborare un'appropriata strategia di comunicazione. L'analisi del ruolo del SIC e degli organi che lo avevano preceduto è stata effettuata soltanto sulla scorta di indicazioni che nel tempo erano state trasmesse ai membri dirigenti del servizio e alle quali non era stato riconosciuto alcun carattere di urgenza.

Invece di approfondire la natura delle relazioni che il Servizio informazioni svizzero intratteneva con la Crypto AG e i servizi americani, il direttore del SIC si è accontentato di relativizzarne l'importanza per il suo servizio e di esonerarlo da qualunque responsabilità. L'intenzione di proteggere il proprio servizio e la responsabile del Dipartimento ha caratterizzato la lacunosa valutazione della situazione che è stata sottoposta al Dipartimento e alla DelCG.

Neppure la SG-DDPS ha riconosciuto la portata del problema, nonostante uno dei collaboratori avesse il ruolo di consulente in materia di attività informative della responsabile del Dipartimento.

Nel contempo, il DDPS si è lasciato sfuggire l'occasione di approfondire le questioni strategiche che si ponevano in rapporto con il caso Crypto AG relativamente alla competenza della Svizzera in materia di crittologia, sia nell'ambito delle attività informative, sia in quello dell'esercito o dell'industria. Il comando dell'esercito non è stato consultato, sebbene la sicurezza delle sue reti e il successo di importanti progetti fossero direttamente implicati.

5 Questioni di principio per il futuro

5.1 Operazioni in materia di attività informative in collaborazione con imprese svizzere.

La Svizzera non è membro di alcuna alleanza militare ed è tenuta a osservare il principio della neutralità. In virtù della sua indipendenza politica e delle buone relazioni che intrattiene a livello bilaterale e multilaterale, gli altri Stati non hanno praticamente motivo di pensare che la Svizzera rappresenti una minaccia per loro. Le imprese e le organizzazioni che operano in Svizzera beneficiano all'estero dell'immagine di neutralità del Paese. I servizi di intelligence esteri possono dunque avere interesse a nascondersi dietro imprese svizzere per operare contro Stati terzi.

Se queste attività sono assimilate alla fattispecie dello spionaggio (artt. 272–274 e art. 301 CP)[29], è compito del controspionaggio opporvisi, ossia del SIC e delle autorità di perseguimento penale nei limiti delle loro rispettive competenze. Se si arriva a un

29 Codice penale svizzero (CP; RS **311.0**).

procedimento penale, è il DFGP o il Consiglio federale a decidere in ultima istanza in merito al perseguimento in giudizio delle persone coinvolte.

È altresì ipotizzabile che un servizio di intelligence straniero cerchi di collaborare con il SIC per sfruttare i vantaggi della Svizzera in un'operazione di attività informative e che sia disposto, in cambio, a condividere con la Svizzera i risultati dell'operazione. Dal momento che l'articolo 12 capoverso 1 lettera c LAIn autorizza il SIC a svolgere attività congiunte volte ad acquisire e analizzare informazioni, tale collaborazione con un servizio di intelligence è giuridicamente consentita («Joint Operation»). Conformemente all'articolo 34 LAIn, il SIC può demandare la ricerca di informazioni anche a servizi esteri e privati, siano essi in Svizzera o all'estero.

L'articolo 36 capoverso 1 LAIn sancisce che il SIC possa acquisire segretamente informazioni riguardanti fatti che avvengono all'estero. Sebbene la legge non si pronunci sulle modalità applicabili, secondo l'articolo 36 capoverso 3 LAIn deve essere osservato il principio della proporzionalità. Il vantaggio ottenuto con l'acquisizione di informazioni deve essere dunque proporzionato ai rischi operativi e politici di un'operazione e all'ingerenza nei diritti fondamentali delle persone interessate.

L'acquisizione di informazioni da parte del SIC deve essere orientata alle attuali minacce in materia di politica di sicurezza. Nella missione fondamentale assegnata al SIC, il Consiglio federale decide quali Stati siano per il SIC obiettivi prioritari dell'esplorazione. Approvando i contatti con l'estero, il Consiglio federale definisce i servizi di intelligence esteri con i quali ritiene sia politicamente opportuno collaborare. Il servizio delle attività informative è dunque uno strumento a cui il Consiglio federale può ricorrere in funzione delle minacce e dell'opportunità politica. Una parità di trattamento senza riserve di Stati stranieri nell'ambito delle attività informative non è prevista e contraddirebbe il principio della proporzionalità statuito dalla legge.

Conformemente al diritto in vigore, è dunque ammissibile che il SIC e un servizio estero si avvalgano congiuntamente di un'impresa con sede in Svizzera per procurarsi informazioni concernenti l'estero (cfr. art. 34 cpv. 2 LAIn). Nell'ambito di un'operazione congiunta tra il SIC e un servizio di intelligence straniero, le attività condotte da quest'ultimo non sono più assimilabili alla fattispecie dello spionaggio.

Laddove un'impresa svizzera fosse coinvolta in una collaborazione tra il SIC e un servizio partner, la DelCG ritiene tuttavia assolutamente necessario che le possibili conseguenze politiche siano preliminarmente analizzate a livello politico. In particolare devono essere esaminate le conseguenze per la piazza economica svizzera e per le persone eventualmente colpite nella suddetta impresa. Devono essere altresì considerate le ripercussioni di questa collaborazione sulla politica estera svizzera in generale e sulle relazioni bilaterali interessate in particolare.

La DelCG ritiene dunque necessario che il Consiglio federale esamini a fondo le possibilità che la LAIn offre al SIC. In particolare dovrebbe accertare il margine di manovra politico che è disposto a concedere al DDPS e in quali circostanze vuole essere informato o decidere tali operazioni.

5.2 Una crittografia sicura per la Svizzera

La possibilità di disporre di strumenti di crittografia sicura è una condizione sine qua non per la sicurezza delle infrastrutture informatiche e di comunicazione in Svizzera. Per esempio, i due progetti del DDPS «Rete di condotta Svizzera» e «Telecomunicazione dell'esercito» non possono prescindere da una cifratura sicura dei dati trasmessi, senza la quale il risultato di questo investimento di circa 2,2 miliardi di franchi è compromesso. Inoltre, anche il DFAE e il SIC devono poter disporre di collegamenti sicuri per le loro comunicazioni.

Una delle principali conclusioni a cui è giunta l'ispezione condotta dalla DelCG è che i fornitori di tecnologia di cifratura sono un bersaglio privilegiato dei servizi di intelligence stranieri nei loro tentativi di infiltrazione. La storia della Crypto AG dimostra che anche le società svizzere poste sotto l'influenza di servizi di attività informative stranieri possono produrre apparecchi che utilizzano procedure di cifratura «deboli». L'ispezione della DelCG ha altresì messo in luce che le autorità svizzere sono comunque riuscite a garantire la sicurezza dei propri apparecchi.

Come la DelCG ha potuto accertare, tutte le verifiche effettuate hanno confermato che la Crypto AG non ha mai fornito apparecchi di cifratura «deboli» alle autorità svizzere, a differenza di un'altra società che ne ha venduto di vulnerabili all'Amministrazione federale, compresi i servizi delle attività informative (cfr. n. 4.2.4). È dunque essenziale che la Confederazione disponga di competenze sufficienti nell'ambito della crittologia, poiché solo questo know-how consente di controllare la sicurezza degli apparecchi acquistati e di influenzarne la progettazione. Tale competenza è strettamente legata al know-how necessario per decrittare cifrature straniere, fattore imprescindibile ai fini di una collaborazione tra i servizi delle attività informative, come esposto nel numero 5.1.

Infine, la Confederazione ha tuttavia la possibilità di influenzare in misura sufficiente la sicurezza degli apparecchi di cifratura perché rispondano alle sue esigenze e ai suoi bisogni solo se sono sviluppati e prodotti in Svizzera e il fornitore è chiaramente in mani svizzere. La Confederazione non ha, invece, alcuna possibilità di influenzare l'affidabilità dei fornitori stranieri. Sulla scorta delle considerazioni suesposte, la DelCG giunge alla conclusione che la Confederazione potrà contare su strumenti di crittografia sicuri solo se sono prodotti da un'industria che opera nell'ambito della tecnologia di cifratura con sede in Svizzera.

Nel corso delle sue ispezione, la DelCG ha tuttavia constatato che né il Consiglio federale né tanto meno il Dipartimento federale dell'economia, della formazione e della ricerca (DEFR) avevano compreso l'importanza del fatto che l'affidabilità delle tecniche di cifratura non può prescindere da una collaborazione con fornitori indigeni. Questa tematica non era considerata prioritaria neppure all'interno del DDPS, il quale aveva indicato al Consiglio federale ancora il 6 novembre 2019 che gli attesi comunicati dei media sul caso Crypto AG avrebbero potuto compromettere l'esistenza delle imprese chiamate a subentrare alla Crypto AG.

Secondo le investigazioni condotte dalla DelCG, il capo dell'esercito (CEs) e il segretario generale del DDPS hanno parlato, nel febbraio 2020, delle possibili conseguenze che potrebbe avere per l'esercito la perdita dei suoi fornitori di strumenti di cifratura, tuttavia non si è cercata una strategia che consentisse di trovare possibili alternative

agli apparecchi forniti dalle società subentranti alla Crypto AG. Non c'è mai stato neppure un colloquio tra la responsabile del DDPS e il CEs sulle possibili misure da adottare per assicurare all'esercito l'accesso a strumenti di cifratura sicuri qualora gli attuali fornitori dovessero cessare l'attività.

Il 19 giugno 2020 il Consiglio federale ha autorizzato il MPC ad avviare la procedura penale in rapporto alle precedenti esportazioni della Crypto AG e ha deciso di congelare la decisione in merito alle domande di esportazione presentate dalla Crypto International AG e dalla TCG Legacy AG fino alla conclusione del procedimento penale (cfr. n. 8.4). Prima della decisione del Consiglio federale, il DDPS aveva in realtà segnalato la dipendenza della Svizzera dalle società subentrate alla Crypto AG, in particolare dalla CyOne Security AG. Tuttavia, come è risultato dalla richiesta del DFGP del 17 giugno 2020, non era stato in grado di valutare le conseguenze per l'esercito di un eventuale fallimento della Crypto International AG che era gravemente toccata dal blocco illimitato delle esportazioni. Il DDPS ha avviato investigazioni serie sulla questione solo a partire da settembre 2020. Le informazioni trasmesse dal CEs alla DelCG sulle investigazioni in corso presso le imprese coinvolte erano insufficienti.

Secondo la DelCG, il Consiglio federale non ha tenuto sufficientemente conto degli interessi fondamentali della Svizzera per strumenti di crittografia sicuri nella sua decisione del 19 giugno 2020, tuttavia il DDPS, dal canto suo, non aveva approfondito né era riuscito a dimostrare in modo convincente i rischi ai quali si esponevano la Confederazione e, in particolare, l'esercito.

La DelCG non ritiene di sua competenza procedere, nell'ambito della sua ispezione, alle investigazioni e alle valutazioni dei rischi che avrebbero dovuto essere svolte dall'Esecutivo, né può prevedere l'esito del procedimento penale e della procedura di ricorso che le imprese coinvolte hanno intentato contro la decisione del Consiglio federale di sospendere le autorizzazioni all'esportazione. Di conseguenza, la Delegazione si astiene dall'esprimere un giudizio definitivo in merito a quanto le decisioni del Consiglio federale abbiano messo durevolmente in discussione l'accesso della Svizzera a strumenti di crittografia sicuri.

6 Misure adottate dal DDPS e dal Consiglio federale

6.1 Decisione del Consiglio federale del 20 dicembre 2019

6.1.1 Istituzione di un gruppo di lavoro interdipartimentale

Il 7 novembre 2019, in occasione di una seduta alla quale sono intervenuti la responsabile del DDPS (*Viola Amherd*), il vice-cancelliere della Confederazione, il segretario generale del DDPS, la segretaria generale del DFGP e alcuni rappresentanti del SIC, è stato deciso di istituire un gruppo di lavoro interdipartimentale (GLID) in rapporto con la Crypto AG. In quel momento le informazioni erano poco chiare e diversi dipartimenti avevano ricevuto richieste fondate sulla legge federale sul principio di

trasparenza dell'amministrazione (LTras)[30] e sulla LAr. Il GLID aveva il compito di raccogliere le informazioni disponibili e di procedere a un'analisi sistematica che permettesse tra l'altro di decidere sul da farsi. Dovevano essere approfonditi i fatti concernenti la società Crypto AG. Il gruppo di lavoro si è riunito la prima volta il 18 novembre 2019 sotto la direzione del segretario generale del DDPS. La Cancelleria federale (CaF) era stata invitata a partecipare presupponendo che l'intero Consiglio federale fosse direttamente coinvolto e che la CaF dovesse coordinare le informazioni. Diverse audizioni condotte nell'ambito dell'ispezione hanno rivelato che il compito affidato al GLID non era stato interpretato allo stesso modo da tutti i suoi membri, da cui si evince che non era sufficientemente chiaro.

Nella sua prima seduta il GLID (composto dalla SG-DDPS, dalla SG-DFGP, dal vicecancelliere della Confederazione, dal capo della divisione NDBU, da un rappresentante dell'UFG e da altri rappresentanti del DDPS) ha deciso di trattare il caso in due tappe successive. Da un lato doveva essere condotta una disanima storica, dall'altro il GLID intendeva occuparsi degli sviluppi più recenti. La priorità doveva tuttavia consistere nel mettere a punto una cronologia che consentisse, in un secondo momento, di rispondere a domande concrete nonché di elaborare strategia e comunicazione. Inoltre, a partire dalla sua seconda seduta, avrebbero partecipato anche un rappresentante del DFAE e uno del MPC. Dalla nota relativa alla prima seduta del GLID risulta che nel 2009 la DelCG sarebbe stata messa al corrente dal DDPS su alcuni aspetti del caso Crypto AG, tuttavia questa informazione non corrisponde al contenuto del verbale che il presidente della DelCG ha fatto pervenire alla responsabile del DDPS a seguito del loro incontro del 12 novembre 2019 (cfr. n. 4.1.4).

Il GLID si è riunito in altre quattro occasioni (29 novembre 2019, 9 dicembre 2019, 10 febbraio 2020 e 2 marzo 2020). A partire dalla terza seduta sono intervenuti anche rappresentanti della SG-DEFR e dell'AFS. Sembra che il GLID abbia concentrato la sua attività su due aspetti in particolare: le domande di consultazione dei documenti ai sensi della LTras e l'elaborazione della cronologia da parte del SIC. In occasione della seduta del GLID del 9 dicembre 2019, il SIC gli ha presentato una prima cronologia che tuttavia è stata respinta con la richiesta di rielaborarla perché poco chiara e incompleta. Tra l'altro, mancavano informazioni concernenti gli ultimi 20 anni.

Da ultimo, il GLID ha rinunciato a eseguire per suo conto un'elaborazione dettagliata dei fatti rinviando ai lavori cominciati il 16 gennaio 2020 da Niklaus Oberholzer (cfr. n. 6.2). La DelCG constata che, in base alle sue attuali conoscenze, i risultati del bilancio della situazione stilato nell'autunno 2019 su incarico del direttore del SIC non sono stati considerati nei lavori del GLID. Secondo le spiegazioni fornite dalla responsabile del DDPS, nelle prime quattro sedute del GLID è stato chiesto al capo della divisione NDBU se esistessero altri documenti o informazioni, ma ha sempre negato. Solo poche persone erano a conoscenza del bilancio stilato, e tra queste il capo della NDBU. Infatti, il SIC non voleva rendere nota all'interno del GLID la collaborazione nelle attività informative con il servizio di intelligence americano a proposito della Crypto AG, dunque ha impedito che l'argomento fosse approfondito dal GLID. Per questo motivo non sono stati menzionati neppure i dossier rinvenuti nell'installazione

30 Legge federale del 17 dic. 2004 sul principio di trasparenza dell'amministrazione (legge sulla trasparenza, LTras; RS **152.3**).

K. Se il bilancio della situazione dell'autunno 2019 fosse già stato noto allora alla responsabile del Dipartimento, sarebbe stato secondo lei possibile evitare di istituire il GLID e il mandato conferito al signor Oberholzer sarebbe stato diverso. Il gruppo di lavoro ha deciso di non sciogliersi e di riunirsi in funzione delle esigenze. Il 15 gennaio 2020 il Consiglio federale ha quindi deciso che il GLID avrebbe dovuto sostenere a titolo consultivo il comitato di ricerca nominato per affiancare il signor Oberholzer.

Nel complesso va osservato che, per adempiere i compiti summenzionati, il GLID si è occupato prima di tutto di questioni formali e di garantire le informazioni ai media. Con l'intervento della DelCG e anche con la rivelazione del bilancio stilato dal SIC, il GLID ha assunto soltanto una funzione di coordinamento e i suoi lavori potevano servire al Consiglio federale come base decisionale solo in misura limitata.

6.1.2 Dossier rinvenuti nell'installazione K

Il 12 novembre 2019 il SIC ha ricevuto le prime informazioni, ancora piuttosto vaghe, sulla probabile esistenza di altri documenti concernenti la Crypto AG. È poi trascorso quasi un mese, fino al 10 dicembre 2019, prima che queste informazioni venissero verificate. Il giorno dopo, otto scatole piene di dossier riguardanti la Crypto AG sono state scoperte in un luogo esterno all'AFS (installazione K, cfr. n. 2.1.4). Il 12 dicembre 2019 il direttore del SIC è stato quindi informato di questa scoperta e dei primi elementi riscontrati. Alla domanda sul perché il SIC abbia atteso quasi un mese prima di seguire effettivamente gli indizi ricevuti, il direttore del SIC ha risposto che non si trattava di una questione urgente.

La DelCG è contrariata da questa risposta, dato che la conclusione del bilancio della situazione stilato nell'autunno 2019 (cfr. in proposito il n. 4.1.4) era stata anticipata per dare al direttore del SIC un vantaggio a livello di informazioni in vista dell'eventuale divulgazione di notizie da parte dei media. Secondo la DelCG, il fatto che il SIC non abbia agito con maggiore tempestività in merito ai dossier rinvenuti nell'installazione K con la motivazione che non vi intravedeva alcuna urgenza mostra che i responsabili in seno al SIC non avevano riconosciuto la vera portata della questione.

La conclusione cui è giunta la DelCG trova conferma anche nel fatto che i dossier scoperti nell'installazione K sono stati visionati solo in modo sommario, senza essere oggetto di una catalogazione esaustiva né di alcuna valutazione. Quando, il 17 febbraio 2020, la DelCG ha chiesto un inventario dei documenti, il SIC ha potuto fornire solo qualche parola chiave, che un collaboratore aveva annotato di propria iniziativa e che si riferiva unicamente ad alcuni contenitori.

Il 16 dicembre 2019 il direttore del SIC ha riferito verbalmente alla responsabile del DDPS che in un'installazione K erano stati rinvenuti alcuni documenti, dopodiché il Consiglio federale si è occupato per la seconda volta del caso Crypto AG nella sua seduta del 20 dicembre 2019.

6.1.3 Basi della decisione del Consiglio federale del 20 dicembre 2019

Nella proposta del DDPS indirizzata al Consiglio federale in vista della seduta del 20 dicembre 2019 era precisato che le informazioni conosciute non erano sufficienti per tenere un dibattito sui contenuti in seno al Consiglio federale. Oggi, alla luce degli elementi acquisiti dalla DelCG, questa affermazione risulta pertinente non tanto perché non si disponesse di tutte le informazioni necessarie, ma perché esse non erano state consultate o trattate dal SIC in modo appropriato e con la necessaria celerità. Inoltre, il DDPS non ha informato correttamente il Consiglio federale, altrimenti nella sua proposta non sarebbe stato dichiarato che praticamente non esistevano documenti ufficiali o che erano irreperibili e che il SIC aveva accesso soltanto a pochi documenti. In quel momento il SIC era già a conoscenza dell'esistenza dei dossier scoperti nell'installazione K, anche se non li aveva ancora studiati nel dettaglio; alcune parole chiave relative al contenuto dei dossier erano state trascritte ed erano disponibili in quel momento. In merito ai documenti scoperti, ci si è limitati a comunicare alla responsabile del DDPS che un ex consigliere federale (*Kaspar Villiger*) era a conoscenza dei fatti.

In base agli elementi noti a oggi, si può concludere che il bilancio stilato nell'autunno 2019 conteneva tutte le principali informazioni necessarie a comprendere la portata e le conseguenze del caso Crypto, tuttavia tali informazioni non sono state comunicate adeguatamente al Consiglio federale in vista delle sue sedute del 6 novembre 2019 e del 20 dicembre 2019, di conseguenza questi non disponeva di informazioni sufficienti (cfr. n. 4.1.3). È stato tra l'altro commentato che le fonti a cui si è fatto ricorso per stilare il bilancio della situazione erano molto deboli e che il documento avrebbe dovuto essere completato, ma ciò non è mai avvenuto.

Come già esposto al numero 4.1.3, nell'ottobre 2019 il SIC ha ricevuto il rapporto MINERVA insieme con altri documenti. Il 21 novembre 2019, il vice-cancelliere della Confederazione e due rappresentanti della SG-DDPS hanno esaminato questi documenti per un'ora. Tenendo conto del volume della documentazione, è opportuno osservare che un'ora è ben lungi dall'essere sufficiente per esaminarli seriamente. I rappresentanti della CaF e della SG-DDPS erano stati incaricati di occuparsene dal GLID, di cui erano pure membri. Alla seconda seduta del GLID si è semplicemente comunicato che i documenti erano stati esaminati e che avrebbero avuto un ruolo importante nell'elaborazione della cronologia. Allo stato attuale delle conoscenze, tuttavia, le informazioni evinte da questi documenti non sono state considerate nella decisione adottata dal Consiglio federale in occasione della sua seduta del 20 dicembre 2019.

A causa delle informazioni lacunose trasmesse dal SIC al GLID e della conseguente incertezza (cfr. n. 6.1.1), il 9 dicembre 2019 il GLID ha ritenuto necessario sottoporre al Consiglio federale tre proposte in merito a come procedere, una delle quali consisteva nell'affidare a esterni l'incarico di svolgere investigazioni più approfondite. Su raccomandazione del DDPS, il Consiglio federale ha quindi deciso, nella sua seduta del 20 dicembre 2019, di affidare a un comitato di ricerca l'incarico di studiare il caso Crypto e ha chiesto al DDPS di proporgli, prima della seduta del 15 gennaio 2020, una candidatura per la direzione del comitato e di informarlo sulle tappe successive

entro fine febbraio 2020. Il Consiglio federale è stato così condotto su una strada sbagliata.

In base alla posizione ufficiale adottata in occasione della seduta, emerge che in quel momento il Consiglio federale presupponeva che si trattasse soltanto di una ricerca storica.

6.2 Nomina dell'incaricato dell'inchiesta

Il 23 dicembre 2019 si è svolta una prima riunione nella SG-DDPS durante la quale è stata menzionata la possibilità di nominare l'ex giudice federale Niklaus Oberholzer a capo del comitato di ricerca. L'8 gennaio 2020 si è svolto un primo colloquio con il signor Oberholzer che si è dichiarato pronto a dirigere il gruppo di ricerca.

In occasione della seduta del 15 gennaio 2020, il Consiglio federale ha deciso, su proposta del DDPS, di nominare Niklaus Oberholzer direttore del comitato di ricerca. Secondo la decisione in questione, il comitato era incaricato di procedere a un esame completo dei fatti riguardanti la Crypto AG dal 1945 fino alla scissione della società avvenuta nel febbraio 2018.

Si trattava di chiarire il ruolo svolto dall'Amministrazione federale e dalle autorità politiche. Secondo la proposta del DDPS, le questioni della legalità e dell'opportunità delle attività informative erano di competenza delle autorità ordinarie di vigilanza (autorità di vigilanza indipendente sulle attività informative [AVI-AIn] e DelCG). Il mandato prevedeva inoltre che il Consiglio federale ricevesse un resoconto entro la fine di giugno 2020. Considerata l'urgenza e il gran numero di documenti da consultare, a Niklaus Oberholzer è stata offerta la possibilità di avvalersi di diversi giuristi di un rinomato studio di avvocati, che non sono stati poi interpellati. Il signor Oberholzer è entrato in carica il 16 gennaio 2020.

Per la DelCG, il fatto che il mandato di indagine avesse come termine il mese di febbraio del 2018 dimostra che la possibilità di trovare rapporti con l'attualità non era presa in considerazione in quel momento Inoltre, la proposta di questo mandato era fondata su conoscenze lacunose del GLID.

Quando ha cominciato il suo lavoro il 16 gennaio 2020, Niklaus Oberholzer aveva ricevuto dal DDPS solo la cronologia incompleta che il SIC aveva predisposto per il GLID (cfr. n. 6.1.1). Non era in possesso del rapporto MINERVA né era a conoscenza dei dossier rinvenuti nell'installazione K. Le prime informazioni sul contenuto del rapporto MINERVA le ha apprese dai media. Il 15 febbraio 2020, in risposta al dibattito mediatico sulla possibile connivenza di alcuni consiglieri federali, ha quindi redatto una nota all'attenzione della responsabile del DDPS (*Viola Amherd*). Dal momento che ignorava l'esistenza dei documenti rinvenuti nell'installazione K, ha concluso che i documenti in suo possesso non consentivano di provarlo. Il giorno seguente la stampa domenicale ha riferito dei suddetti documenti che, secondo i giornalisti, avrebbero dimostrato che l'allora capo del DMF (*Kaspar Villiger*) doveva essere a conoscenza dei fatti.

Il modo di procedere del DDPS ha impedito che l'indagine condotta dal signor Oberholzer fornisse rapidamente elementi attendibili utili in vista di future decisioni politiche. Il comitato di ricerca aveva prima di tutto il compito di studiare gli eventi storici e non di sostenere il Consiglio federale nella gestione del caso Crypto AG. In realtà, il Consiglio federale aveva previsto la possibilità di precisare il mandato di indagine dopo una prima consultazione dei documenti disponibili, ma non è stato possibile in quanto il DDPS, a causa del lacunoso scambio di informazioni al suo interno, non concedeva l'accesso ai documenti in suo possesso.

6.3 Ruolo della Delegazione Sicurezza

In occasione della seduta della Delegazione Sicurezza (DelSic) del 18 febbraio 2020, la responsabile del DDPS (*Viola Amherd*) ha comunicato che il giorno successivo avrebbe presentato al Consiglio federale i primi risultati intermedi dell'inchiesta Oberholzer. Il Consiglio federale ha quindi ricevuto la nota che il signor Oberholzer aveva redatto il 15 febbraio 2020 all'attenzione della responsabile del DDPS senza essere a conoscenza dei fascicoli più importanti.

In seguito, il caso Crypto AG non è stato più trattato in seno alla DelSic, che non ha quindi colto l'occasione, nella sua seduta del 5 maggio 2020, di discutere la domanda di autorizzazione depositata dal MPC presso il DFGP il 13 marzo 2020 (cfr. n. 8.4.3). Dal canto suo, il DFAE non ha menzionato le difficoltà diplomatiche che si delineavano con i Paesi amici colpiti dalla sospensione delle forniture da parte delle imprese subentrate alla Crypto AG.

La prevista seduta della DelSic del 20 agosto 2020 è stata annullata in mancanza di temi urgenti da trattare, sebbene in questo momento tutti i membri del Consiglio federale avessero ricevuto una richiesta di riesame da parte della Crypto International AG in merito alla sospensione delle sue autorizzazioni all'esportazione (cfr. n. 8.5). Neanche la domanda se un fallimento della Crypto International AG potesse compromettere la disponibilità per l'esercito di strumenti di crittografia sicuri (cfr. n. 5.2) era evidentemente un oggetto che la DelSic doveva trattare secondo il parere del DDPS, cui è affidata la presidenza permanente della Delegazione. Occorre tuttavia osservare che, dalla riforma[31] degli strumenti di condotta della politica di sicurezza, avvenuta nell'ottobre 2011, il CEs e l'esercito non facevano più parte della cerchia di partecipanti fissi della DelSic, mentre la direttrice dell'Ufficio federale di polizia (fedpol) e il direttore del SIC vi prendono sempre parte, così come, normalmente, i segretari generali dei tre dipartimenti.

31 Istruzioni del 24 ago. 2011 sull'organizzazione della condotta in materia di politica di sicurezza del Consiglio federale (FF **2011** 6093).

7 La DelCG rileva il caso

7.1 Autorizzazione ai sensi dell'articolo 154*a* LParl

Il 13 febbraio 2020, durante una seduta straordinaria, la DelCG ha deciso di avviare un'ispezione. Il Consiglio federale è stato informato per lettera il 14 febbraio 2020.

L'articolo 154*a* capoverso 1 della legge federale sull'Assemblea federale (LParl)[32] sancisce che inchieste disciplinari o amministrative della Confederazione riguardanti fatti o persone che sono oggetto di un'inchiesta della Delegazione delle Commissioni della gestione possono essere avviate o proseguite unicamente con l'autorizzazione di quest'ultima.

Nella sua lettera del 14 febbraio 2020, la DelCG informa il Consiglio federale che lo autorizza, ai sensi dell'articolo 154*a* LParl, a proseguire l'inchiesta Oberholzer. Contestualmente gli ha chiesto di concedere al signor Oberholzer l'accesso incondizionato a tutti i fondi d'archivio e gli ha annunciato di voler coordinare strettamente la propria inchiesta con Niklaus Oberholzer. Ha inoltre informato il Consiglio federale che avrebbe fatto valere la propria priorità nell'audizione delle persone che lavorano o lavoravano per la Confederazione.

La richiesta della DelCG di concedere a Niklaus Oberholzer il pieno accesso agli archivi era motivata dalle restrizioni derivanti dalla decisione del Consiglio federale del 15 gennaio 2020. Secondo la proposta del DDPS del 13 gennaio 2020, il comitato di ricerca doveva disporre degli stessi diritti di consultazione dei dati personali di chiunque altro ne facesse richiesta, ai sensi dell'articolo 11 LAr. Ogni domanda di consultazione di tali dati doveva dunque essere esaminata dall'organo federale competente. In ultima istanza ciò significava che la consultazione di alcuni documenti avrebbe potuto essere rifiutata al signor Oberholzer in presenza di interessi di protezione preponderanti. Questo era tuttavia in contraddizione con l'obiettivo di chiarire senza preclusioni tutti gli aspetti storici del caso Crypto AG.

Dal punto di vista della DelCG, il comitato di ricerca doveva disporre degli stessi diritti di consultazione, ai sensi dell'articolo 14 LAr, dei servizi federali che avevano versato i documenti. Dopotutto, Niklaus Oberholzer operava su mandato del Consiglio federale, al quale gli uffici competenti erano subordinati e, secondo l'articolo 14 LAr, la consultazione dei dati personali archiviati è possibile solo in casi ben definiti, per esempio se sono utilizzati come mezzi di prova. Tale necessità esisteva per l'inchiesta Oberholzer, pertanto la DelCG non vede alcun motivo legale per cui uffici federali avrebbero potuto limitare l'accesso ai propri documenti che essi stessi avevano versato all'AFS. Nell'incontro avuto con la DelCG il 25 febbraio 2020, la responsabile del DDPS (*Viola Amherd*) ha tuttavia ritenuto necessario, dal punto di vista legale, che la procedura di consultazione di cui all'articolo 11 LAr fosse applicata anche al signor Oberholzer.

32 Legge federale del 13 dic. 2002 sull'Assemblea federale (legge sul Parlamento, LParl; RS **171.10**).

7.2 Trasmissione dei documenti

7.2.1 Mancata consegna di documenti alla DelCG

Con una mail del 12 febbraio 2020 la SG-DDPS è stata pregata di mettere a disposizione della DelCG tutti i documenti necessari rapidamente e senza restrizioni La DelCG ha avanzato questa richiesta appellandosi ai suoi ampi diritti di informazione, secondo cui alle delegazioni delle commissioni di vigilanza non può essere sottaciuta alcuna informazione (art. 154 cpv. 1 LParl). Le delegazioni hanno inoltre il diritto di farsi consegnare i verbali delle sedute del Consiglio federale e anche i documenti classificati come segreti (art. 154 cpv. 2 LParl).

In occasione degli incontri che la DelCG o il suo presidente ha avuto con la responsabile del DDPS (*Viola Amherd*) o il direttore del SIC (*Jean-Philippe Gaudin*) prima dell'avvio dell'ispezione, non è stata fatta menzione di altri documenti oltre al rapporto MINERVA. La DelCG è stata quindi indotta a credere che sul caso Crypto AG non esistesse praticamente alcun documento, il che si è poi dimostrato non corrispondere alla realtà. In occasione del primo colloquio in materia tra la DelCG, la responsabile del DDPS e il direttore del SIC svoltosi il 25 novembre 2019, il bilancio della situazione stilato dal SIC nell'autunno 2019 era già disponibile. La DelCG non è stata informata neppure della scoperta dei dossier nell'installazione K.

La Delegazione è perplessa di fronte al fatto di non essere stata informata dell'esistenza dei diversi documenti considerando che, nel corso della seduta del 25 novembre 2019, ha pregato la responsabile del DDPS di comunicarle i risultati delle investigazioni condotte.

Su espressa richiesta del suo presidente, la DelCG ha ottenuto una copia del rapporto MINERVA il 10 febbraio 2020 e il 13 febbraio 2020 è seguita una copia della nota informativa segreta redatta dal DDPS all'attenzione del Consiglio federale all'inizio di novembre 2019 (cfr. n. 4.1.3). Il bilancio della situazione stilato dal SIC nell'autunno 2019 è stato trasmesso alla DelCG solo il 17 febbraio 2020. La responsabile del DDPS è stata informata dell'esistenza di questo bilancio il giorno seguente per la prima volta.

Si osserva inoltre che i diritti d'informazione della DelCG comprendono anche note e documenti redatti all'attenzione di un capodipartimento, un direttore o un capo ufficio esclusivamente a uso interno.

7.2.2 Concessione dell'autorizzazione a consultare i documenti

Con lettera del 14 febbraio 2020, la DelCG ha chiesto al Consiglio federale di concedere a Niklaus Oberholzer pieno accesso agli archivi. Questa richiesta era motivata dalla volontà della DelCG di dare al signor Oberholzer la possibilità di esaminare il caso in modo completo, attingendo a tutti i documenti, e dall'interpretazione della LAr, secondo la DelCG errata, da parte del DDPS (cfr. n. 7.2.1).

Il 17 febbraio 2020 la DelCG ha preso atto per la prima volta del bilancio della situazione stilato dal SIC nell'autunno 2019. Il pomeriggio del 18 febbraio 2020 e la mattina presto del giorno successivo, i membri della DelCG hanno analizzato il summenzionato bilancio e constatato l'importanza del suo contenuto.

Il presidente della DelCG ha quindi immediatamente chiesto alla responsabile del DDPS che il bilancio non fosse messo a disposizione né del signor Oberholzer né del procuratore generale della Confederazione (*Michael Lauber*) e che non fosse intrapresa alcuna azione irreversibile in materia di trasmissione di documenti. Il DDPS non ha tuttavia dato seguito alla richiesta e il giorno stesso ha consentito a Niklaus Oberholzer di consultare il documento nei locali del SIC, apparentemente su ordine della responsabile del dipartimento. Anche il procuratore generale della Confederazione ha potuto prendere visione di diverse parti del documento il 20 febbraio 2020. Secondo le dichiarazioni del DDPS, né il signor Oberholzer né il procuratore generale della Confederazione ne hanno ricevuto una copia.

7.2.3 Valutazione della portata dei fatti

Dopo la divulgazione dei fatti da parte dei media avvenuta a metà febbraio 2020, le persone responsabili in seno al SIC e al DDPS hanno continuato a presupporre che il caso Crypto AG concernesse fatti risalenti a un passato lontano e non avesse alcuna implicazione nel presente. Secondo loro si trattava soltanto di svolgere un lavoro di ricerca storica per fare piena luce su quanto avvenuto. Questa visione emerge in diversi documenti e dichiarazioni dei diversi attori.

Il 18 febbraio 2020, la SG-DDPS è giunta a conoscenza del bilancio della situazione stilato dal SIC nell'autunno 2019. Il giorno successivo è stato concesso al signor Oberholzer di prendere visione del documento e due giorni dopo anche il procuratore generale della Confederazione ha potuto consultarne alcune parti. Sulla base di queste informazioni, il MPC avrebbe dovuto confermare al DDPS se le attività della Crypto AG adempissero la fattispecie dello spionaggio, ma non è stato in grado di farlo. Ciò mostra che la SG-DDPS non riusciva, da sola, a contestualizzare i risultati del bilancio stilato dal SIC. In particolare non ha compreso il ruolo svolto dal Servizio informazioni svizzero nel caso Crypto AG né ha riconosciuto la portata giuridica della collaborazione con i servizi americani (cfr. n. 4.2.2 e 5.1).

In effetti, le modalità e la durata della collaborazione tra i servizi delle attività informative svizzeri e americani emergevano chiaramente dal bilancio della situazione e, in ultima istanza, implicavano anche una corresponsabilità delle autorità svizzere nelle attività della Crypto AG. Se questa operazione di attività informative poteva in linea di principio basarsi sul diritto vigente, il fatto che si svolgesse senza l'approvazione delle autorità politiche competenti imponeva di informare con urgenza il Consiglio federale. La portata dell'operazione riguardava potenzialmente la politica esterna e la politica economica, ma coinvolgeva anche la sicurezza personale di dipendenti della società implicati a loro insaputa. Di fronte a queste sfide, il Governo svizzero è rimasto immobile fino a quando non ha compreso appieno le attività del suo servizio delle attività informative.

È stato solo con l'avvio dell'ispezione e le conseguenti richieste di informazioni da parte della DelCG che il DDPS ha realizzato, il 18 febbraio 2020, fino a che punto il SIC avesse omesso di informare sufficientemente le autorità politiche. In particolare ha cominciato a rendersi conto che il caso Crypto AG non poteva più essere considerato un fatto puramente storico, ma non ha compreso che la situazione attuale non poteva essere inquadrata prescindendo dalla prospettiva storica. Lo stesso 18 febbraio 2020 il DDPS ha deciso di chiedere all'AVI-AIn di verificare, parallelamente all'inchiesta Oberholzer, se la pratica attuale in materia di attività informative nell'ambito dell'esplorazione delle comunicazioni e della decrittazione fosse legale, non considerando che la legalità di queste attività non poteva essere accertata senza un'analisi dettagliata dei documenti rinvenuti nell'installazione K (cfr. n. 4.2.2).

I documenti giunti a conoscenza della DelCG l'hanno indotta a rivalutare il caso Crypto AG nel suo insieme. Sulla base delle nuove informazioni di cui disponeva, ha ritenuto che fosse indispensabile sbrogliare i problematici nessi esistenti tra le due inchieste condotte dall'Esecutivo e la sua ispezione, che avrebbero potuto compromettere il suo lavoro. Ha dunque ritenuto opportuno che le ultime informazioni emerse non fossero trasmesse subito ad altri organi (responsabili dell'inchiesta Oberhlozer e MPC) fino a quando non fosse chiarito come procedere. La DelCG ha altresì ritenuto sbagliato coinvolgere le autorità di perseguimento penale prima che il DDPS avesse compreso la reale portata delle nuove informazioni. Per questo motivo ha pregato il DDPS di rinunciare a intraprendere azioni irreversibili nella trasmissione di informazioni fino a quando non avesse potuto incontrare la responsabile del Dipartimento.

7.3 Revoca dell'autorizzazione ai sensi dell'articolo 154*a* LParl

Quando, il 18 febbraio 2020, è giunta a conoscenza del bilancio della situazione stilato dal SIC, la DelCG si è resa improvvisamente conto che non si trattava affatto di una disamina storica, bensì che alcune attività riguardavano anche il presente e rischiavano di avere un impatto esplosivo e di vasta portata.

Con lettera del 21 febbraio 2020, la DelCG ha informato il Consiglio federale che revocava l'autorizzazione all'inchiesta del Consiglio federale di cui aveva ricevuto mandato il signor Oberholzer[33]. È emerso che la coesistenza di più inchieste avrebbe ostacolato un chiarimento rapido e agevole dei fatti. Da un lato la DelCG ha realizzato che né il SIC né il DDPS avevano a suo tempo riconosciuto la vera portata dei fatti da accertare, di conseguenza si è vista costretta, con decisione unanime, ad assumere la condotta delle investigazioni e a revocare l'autorizzazione del 14 febbraio 2020. Dall'altro, la responsabile del DDPS (*Viola Amherd*) ha proposto all'AVI-AIn, con lettera del 18 febbraio 2020, di verificare la legalità delle attività crittoanalitiche condotte dal DDPS per conto del SIC. Dal momento che questa fattispecie era oggetto di un'inchiesta della DelCG, la responsabile del DDPS avrebbe dovuto chiedere un'autorizzazione alla Delegazione conformemente all'articolo 154*a* capoverso 1 LParl, ma non lo ha fatto. Al fine di esaminare i fatti in modo rapido ed efficiente, la DelCG ha

33 Crypto AG: responsabilità per le indagini alla Delegazione delle Commissioni della gestione, comunicato stampa della DelCG del 26 feb. 2020.

quindi deciso di revocare l'autorizzazione che permetteva all'Esecutivo di proseguire la sua inchiesta. Nel contempo ha comunicato al Consiglio federale che si opponeva all'inchiesta dell'AVI-AIn voluta dal DDPS.

L'articolo 154*a* capoverso 2 LParl prevede che la Delegazione delle Commissioni della gestione decida sull'autorizzazione dopo aver sentito il Consiglio federale, il quale ha quindi fatto valere di non essere stato sentito prima della revoca dell'autorizzazione, in violazione del suddetto articolo. Il 19 febbraio 2020 il presidente della DelCG ha comunicato alla responsabile del DDPS che non doveva essere consentito né al signor Oberholzer né al procuratore generale della Confederazione di consultare il bilancio della situazione stilato dal SIC e ha offerto alla responsabile del Dipartimento di essere sentita prima della seduta del Consiglio federale; tuttavia l'invito non è stato accolto, bensì è stato proposto un incontro il 25 febbraio 2020. La DelCG ritiene che, con la sua offerta di ascoltare la responsabile del DDPS, le condizioni dell'articolo 154*a* capoverso 2 LParl siano state adempiute. D'altronde non poteva attendere dopo la seduta del 25 febbraio 2020 per revocare l'autorizzazione, poiché era estremamente urgente impedire la diffusione delle informazioni sensibili.

L'obbligo di sentire il Consiglio federale è stato introdotto nell'articolo 154*a* LParl per tener conto dei casi in cui il Consiglio federale deve avere il diritto di condurre o proseguire inchieste disciplinari o amministrative[34]. Nella fattispecie in questione non si ravvisa un simile motivo. All'epoca il Consiglio federale aveva proposto di inserire direttamente nella legge eccezioni più ampie, per esempio l'autorizzazione avrebbe dovuto essere concessa per motivi validi, tra i quali il Consiglio federale citava la necessità di farsi il più rapidamente possibile un'opinione in merito all'affare in questione e di rimediare senza indugio ai vizi presunti[35]. L'Assemblea federale aveva rinunciato a iscrivere i motivi esplicitamente nella legge, ma era giunta alla conclusione che un'audizione poteva essere senz'altro giustificata. La DelCG osserva inoltre che il Consiglio federale, nella sua risposta del 5 marzo 2020 concernente la revoca dell'autorizzazione, non menzionava alcun motivo che giustificasse il mantenimento dell'autorizzazione. Considerando la portata e l'urgenza della questione, che sino ad allora erano state misconosciute dal Consiglio federale, la revoca dell'autorizzazione non poteva essere rinviata.

7.4 Ricorso a un inquirente da parte della DelCG

Nella sua lettera del 21 febbraio 2020, la DelCG ha comunicato al Consiglio federale, oltre alla revoca dell'autorizzazione, che intendeva consentire a Niklaus Oberholzer di proseguire l'inchiesta, ma su mandato della Delegazione. In tal modo si voleva garantire il prosieguo dei lavori senza interruzioni.

La DelCG ha quindi fatto valere il suo diritto di far capo a inquirenti ai sensi dell'articolo 166 capoverso 2 in combinato disposto con l'articolo 155 capoverso 6 LParl.

34 Cfr. in proposito il dibattito al Consiglio degli Stati: Boll. uff. **2004** S 409.
35 Procedure della Delegazione delle Commissioni della gestione e inchieste disciplinari o amministrative della Confederazione condotte parallelamente e aventi lo stesso oggetto, parere del 31 mar. 2004 del Consiglio federale sul rapporto del 21 nov. 2003 della Commissione della gestione del Consiglio degli Stati (FF **2004** 1279, qui 1283).

Un inquirente può essere designato per l'assunzione delle prove. Conformemente al rimando di cui all'articolo 155 capoverso 6 LParl, il diritto di far capo a un inquirente non spetta solo alla CPI, ma anche alla DelCG. L'articolo 155 capoverso 6 LParl prevede espressamente che, per le delegazioni delle commissioni di vigilanza, alla procedura e ai diritti degli interessati sono applicabili gli articoli 166–171 LParl. Di conseguenza, la CPI e la DelCG hanno le stesse competenze e gli stessi diritti.

7.5 Attività dell'AVI-AIn e responsabilità del DDPS in materia di vigilanza

Il 12 novembre 2019 la responsabile del DDPS (*Viola Amherd*) ha informato per la prima volta il presidente della DelCG sul caso Crypto AG (cfr. n. 4.1.4) e lo stesso giorno anche il capo dell'AVI-AIn. Allora la responsabile del DDPS e i servizi del Dipartimento direttamente coinvolti avevano ricevuto anche la pianificazione delle ispezioni per il 2020 dell'AVI-AIn per una presa di posizione. In quel momento, né il DDPS né l'AVI-AIn hanno considerato necessario integrare alcuni aspetti del caso Crypto AG nel nuovo programma delle ispezioni dell'autorità di vigilanza.

Tre mesi dopo, la DelCG ha deciso di avviare l'ispezione, dopodiché il capo dell'AVI-AIn ha informato la DelCG di essere disponibile a coadiuvare i suoi lavori nei limiti del possibile. Inoltre, l'AVI-AIn ha comunicato che avrebbe preso in considerazione le eventuali rivelazioni dei media in due delle sue ispezioni in corso, ma che non prevedeva di svolgere essa stessa investigazioni in merito al caso Crypto AG.

La DelCG ha apprezzato la volontà di coordinamento espressa dall'AVI-AIn e ha ringraziato del sostegno offerto nella sua lettera del 24 febbraio 2020. Successivamente l'AVI-AIn è passata, con l'accordo della DelCG, a esaminare l'installazione K e altri depositi di documenti del SIC. Questo controllo non era stato annunciato. Il rapporto d'ispezione, terminato nel luglio 2020, ha confermato l'impressione della DelCG che non esistesse alcun inventario attendibile dei documenti depositati.

Nel suo rapporto l'AVI-AIn ha rinunciato a formulare raccomandazioni e la DelCG l'ha ritenuta una scelta appropriata in considerazione della sua ispezione in corso. In tal modo era infatti possibile evitare sin dall'inizio contraddizioni con le future raccomandazioni espresse dall'alta vigilanza parlamentare.

La Delegazione ha invece giudicato problematica la proposta del DDPS del 18 febbraio 2020 di incaricare l'AVI-AIn di verificare immediatamente la legalità delle attività crittoanalitiche condotte dal DDPS per conto del SIC. La richiesta da parte della responsabile del DDPS è giunta soltanto dopo la divulgazione sui media del caso Crypto AG, l'avvio dell'ispezione della DelCG e l'avvenuto chiarimento delle esigenze di coordinamento con l'AVI-AIn. Il DDPS non aveva dunque utilizzato tutto il tempo che aveva avuto a disposizione da novembre 2019 per assumere autonomamente o con il supporto dell'AVI-AIn il suo ruolo di vigilanza in merito all'impiego delle capacità crittoanalitiche da parte del SIC, sebbene la responsabilità della legalità delle attività informative incomba proprio al DDPS e non all'AVI-AIn.

Di fronte a un caso legato ad attività informative di valenza politica, la DelCG ritiene che la direzione del DDPS sia tenuta a procurarsi autonomamente le informazioni che

le occorrono per assumere il proprio ruolo di condotta politica. La direzione del Dipartimento deve poter svolgere questo compito con le proprie forze e non può delegarlo a un organo di controllo indipendente, non vincolato a istruzioni, come l'AVI-AIn.

7.6 Informazioni intermedie fornite alla presidente della Confederazione

Con una lettera del 10 marzo 2020, la DelCG ha proposto un colloquio alla presidente della Confederazione (*Simonetta Sommaruga*) per due motivi: da un lato, la DelCG voleva esporle ancora una volta in modo dettagliato i motivi della revoca dell'autorizzazione, anche per impedire che la decisione pregiudicasse le relazioni tra il Consiglio federale e la DelCG. Dall'altro, dubitava che in quel momento il Consiglio federale cogliesse la portata e il carattere sensibile del caso. La presidente della Confederazione ha accolto la proposta, quindi il 25 maggio 2020 la DelCG ha avuto un colloquio con lei e con la responsabile del DDPS (*Viola Amherd*). In questa occasione la presidente della Confederazione è stata informata dei principali risultati delle investigazioni condotte dalla DelCG, che le ha esposto le sfide che a suo avviso si sarebbero presentate affinché ne riferisse al Consiglio federale. Una di queste sfide consisteva nella risposta alla domanda di autorizzazione depositata dal MPC presso il DFGP in riferimento alla denuncia penale della SECO (cfr. in proposito n. 8).

8 Sospensione delle autorizzazioni all'esportazione da parte del DEFR e del Consiglio federale e denuncia penale della SECO

8.1 Riepilogo dei fatti

Il 3 dicembre 2019 la SECO ha fornito alla TCG Legacy AG, una delle società subentrate alla Crypto AG, una licenza generale di esportazione.

Il 16 dicembre 2019, la segretaria generale del DEFR e il collaboratore personale del capo del DEFR hanno discusso del caso Crypto AG con il capo della divisione NDBU. Dal colloquio è risultato che per la Svizzera sarebbe stato inopportuno se fosse stata divulgata la notizia secondo cui la società aveva ottenuto una licenza di esportazione poco prima della rivelazione del caso sui media. Secondo il capo della divisione NDBU, l'unico obiettivo sarebbe stato di guadagnare tempo. La sera del 19 dicembre 2019 il capo del DEFR (*Guy Parmelin*) ha informato la responsabile del DDPS (*Viola Amherd*), alla presenza dei due segretari generali, dell'intenzione di sospendere la licenza generale di esportazione.

Il 20 dicembre 2019, in seguito a un'istruzione impartita dalla direzione del Dipartimento, la SECO ha sospeso fino a nuovo avviso questa licenza generale di esportazione insieme a quella della Crypto International AG, un'altra società subentrata alla Crypto AG. Dalla nota redatta in occasione della seduta del GLID del 10 febbraio 2020 risulta che la SECO avrebbe tuttavia continuato a trattare domande di autorizzazioni singole all'esportazione.

Il 25 febbraio 2020 la SECO ha depositato una denuncia penale contro ignoti presso il MPC, fondata sull'articolo 18 della legge federale sul controllo dei beni utilizzabili a fini civili e militari, dei beni militari speciali e dei beni strategici (LBDI)[36] e sull'articolo 10 dell'ordinanza sull'esportazione e l'intermediazione di beni per la sorveglianza di Internet e delle comunicazioni mobili (OICoM)[37]. La denuncia penale era stata precedentemente approvata dalla segretaria di Stato della SECO e il suo deposito era stato sostenuto dalla SG-DEFR.

Il 2 marzo 2020 il presidente e la segretaria della DelCG sono stati informati della denuncia penale da parte del procuratore generale della Confederazione. Due giorni dopo, il 4 marzo 2020, si è riunito il gruppo di controllo delle esportazioni (GCE). I presenti sono giunti alla conclusione che le domande di autorizzazioni singole all'esportazione dovevano essere sottoposte alla decisione del Consiglio federale. Nel gruppo di controllo delle esportazioni sono rappresentati, oltre alla SECO, il DFAE, il DDPS e il Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (DATEC) che decidono dopo aver sentito il SIC (art. 27 cpv. 3 OBDI).

Il 6 marzo 2020 la Polizia criminale federale (PCF) ha sequestrato quasi 400 apparecchi della Crypto International AG e della TCG Legacy AG, gran parte dei quali è stata lasciata nei depositi della Crypto International AG. Il verbale della perquisizione è stato inviato alla società il 9 maggio 2020.

Su richiesta della SECO, il 10 marzo 2020 il delegato federale alla cibersicurezza ha organizzato uno scambio di opinioni sulle possibilità di manipolazione degli apparecchi e sugli elementi probatori.

Il 13 marzo 2020 il Ministero pubblico della Confederazione ha indirizzato al DFGP una richiesta di autorizzazione ai sensi dell'articolo 66 della legge sull'organizzazione delle autorità penali (LOAP)[38].

Fino al 18 maggio 2020 la Crypto International AG e la TCG Legacy AG hanno depositato complessivamente 15 domande di autorizzazioni singole all'esportazione di apparecchi e moduli di cifratura. Nel maggio 2020, sia i rappresentanti del DDPS sia quelli del DATEC in seno al gruppo di controllo delle esportazioni si sono dichiarati a favore dell'autorizzazione di tutte le domande di autorizzazioni singole. I rappresentanti del DFAE erano invece propensi ad approvare solo le domande della TCG Legacy AG e a sottoporre quelle della Crypto International AG alla decisione del Consiglio federale.

La mattina del 25 maggio 2020 la DelCG ha avuto un colloquio con la presidente della Confederazione, la responsabile del DDPS e, nel pomeriggio, con la responsabile del DFGP (*Karin Keller-Sutter*). In quell'occasione la Delegazione è stata informata del disbrigo della richiesta di autorizzazione in seno al DFGP.

36 Legge federale del 13 dic. 1996 sul controllo dei beni utilizzabili a fini civili e militari, dei beni militari speciali e dei beni strategici (legge sul controllo dei beni a duplice impiego, LBDI; RS **946.202**).

37 Ordinanza del 13 mag. 2015 sull'esportazione e l'intermediazione di beni per la sorveglianza di Internet e delle comunicazioni mobili (OICoM; RS **946.202.3**).

38 Legge federale del 19 mar. 2010 sull'organizzazione delle autorità penali della Confederazione (legge sull'organizzazione delle autorità penali, LOAP; RS **173.71**).

In vista della seduta del Consiglio federale del 12 giugno 2020, il DEFR ha avanzato la proposta di autorizzare le 15 domande di autorizzazioni singole della Crypto International AG e della TCG Legacy AG. Nel quadro della procedura di corapporto è stato proposto di rinviare l'esame dell'oggetto. È stata contestata anche l'opportunità di attendere la conclusione delle investigazioni ancora in corso della DelCG e del MPC prima di prendere una decisione.

Il 19 giugno 2020 il Consiglio federale ha stabilito, fondandosi su una proposta modificata del DEFR, di sospendere la sua decisione in merito alle 15 domande presentate dalle due società subentrate alla Crypto AG fino alla conclusione delle investigazioni del MPC. Contestualmente ha autorizzato l'avvio di un procedimento penale contro ignoti.

Il 3 luglio 2020 la SECO ha deciso che l'esame delle domande di autorizzazioni singole all'esportazione della TCG Legacy AG sarebbe stato sospeso fino alla conclusione delle investigazioni da parte del MPC. Nella seduta del 26 agosto 2020, il Consiglio federale ha respinto una richiesta di riesame della Crypto International AG in merito alle singole licenze di esportazione.

8.2 Basi legali

Il caso in esame solleva numerose questioni in merito al diritto relativo al controllo dei beni. Il quadro giuridico applicabile alle misure adottate dalla Confederazione nei confronti delle società subentrate alla Crypto AG è costituito dalla legislazione sul controllo dei beni. Secondo l'articolo 2 capoverso 2 LBDI è il Consiglio federale a determinare quali beni rientrino nel campo d'applicazione della legge. Il Consiglio federale ha precisato i beni in questione tra l'altro con l'ordinanza sul controllo dei beni utilizzabili a fini civili e militari, in particolare dei beni militari speciali e dei beni strategici (OBDI)[39].

L'elenco dei beni, la cui esportazione è soggetta ad autorizzazione, figura negli allegati all'OBDI. La parte 2 dell'allegato 2 menziona sistemi e procedure di cifratura[40] nonché sistemi, attrezzature e componenti[41] volti a neutralizzare, indebolire o eludere la sicurezza dell'informazione, progettati o modificati per effettuare le funzioni crittoanalitiche.

Inoltre, per evitare che sistemi di sorveglianza esportati dalla Svizzera siano utilizzati dai loro destinatari stranieri a fini di oppressione politica, il Consiglio federale ha assoggettato queste esportazioni a una procedura vincolante di autorizzazione specifica. Per questo motivo ha emanato, nel 2015, una pertinente ordinanza, la OICoM, che nell'allegato fa riferimento anche agli apparecchi con funzioni crittoanalitiche.

39 Ordinanza federale del 3 giu. 2016 sul controllo dei beni utilizzabili a fini civili e militari, dei beni militari speciali e dei beni strategici (ordinanza sul controllo dei beni a duplice impiego, OBDI; RS **946.202.1**).
40 Allegato 2 parte 2 OBDI, numero di controllo delle esportazioni (NCE) 5A002.
41 Allegato 2 parte 2 OBDI, NCE 5A004.

8.3 Sospensione della licenza generale di esportazione da parte del DEFR

8.3.1 Legalità della sospensione

Nell'ambito della LBDI sono previsti due tipi di autorizzazioni di esportazione: l'autorizzazione singola o l'autorizzazione generale. Conformemente agli articoli 12 e 13 OBDI, la SECO può rilasciare un'autorizzazione generale ordinaria o straordinaria purché siano soddisfatti i diversi requisiti sanciti nella LBDI e nella OBDI.

Alle società che sono subentrate alla Crypto AG la SECO ha rilasciato complessivamente cinque autorizzazioni generali d'esportazione, ordinarie e straordinarie, tra cui un'autorizzazione generale ordinaria per la Germania il 4 dicembre 2019. Il 16 dicembre 2019 la SECO è giunta a conoscenza, per la prima volta, del caso Crypto AG. I primi elementi che attestano gli sforzi volti a sospendere le autorizzazioni generali d'esportazione delle tre società risalgono al 16 dicembre 2019, quando il capo della divisione NDBU ha informato la SG-DEFR. Il 20 dicembre 2019 le autorizzazioni generali d'esportazione sono state dunque sospese dalla SECO. La decisione è stata presa dal capo del DEFR (*Guy Parmelin*), il cui collaboratore personale ha dato le necessarie istruzioni ai collaboratori della SECO che dovevano mettere in atto la decisione. In queste istruzioni è stato esplicitamente precisato che la decisione non doveva essere ulteriormente motivata alle società in questione e che si doveva tornare alla prassi delle autorizzazioni singole. La SECO ha eseguito questa decisione e la comunicazione è avvenuta sulla piattaforma elettronica ELIC[42]. Per quattro delle cinque autorizzazioni generali d'esportazione è indicato esplicitamente che le autorizzazioni della SECO erano state revocate e sospese fino a nuovo avviso. Per quanto riguarda la domanda della TCG Legacy AG, manca la nozione di revoca e la decisione non è motivata per alcuna domanda, secondo le istruzioni della SG-DEFR. Alla TCG Legacy AG, che domandava il motivo della sospensione della licenza, la SECO ha risposto che l'autorizzazione generale d'esportazione sarebbe stata sottoposta a una nuova valutazione. Sia la Crypto International AG sia la TCG Legacy AG hanno presupposto che avrebbero ricevuto per posta una motivazione o una decisione scritta, ma ciò non è mai avvenuto.

Il diritto vigente, che si tratti della LBDI o della OBDI, non prevede la sospensione dell'autorizzazione e la SECO aveva segnalato questo punto alla SG-DEFR, ma la sospensione è stata mantenuta. Non essendo prevista, la sospensione deve essere trattata come una revoca ai sensi dell'articolo 7 LBDI, secondo cui l'autorizzazione è revocata se, dopo il rilascio, le circostanze si sono modificate in modo tale che sono adempiute le condizioni di un rifiuto secondo l'articolo 6 (art. 7 cpv. 1 LBDI). L'autorizzazione può essere revocata anche se le condizioni e gli oneri ad essa connessi non sono rispettati (art. 7 cpv. 2 LBDI).

42 E-licensing, sistema di autorizzazioni elettronico.

8.3.2 Valutazione da parte della DelCG

Secondo le spiegazioni fornite dalla SECO, le autorizzazioni generali d'esportazione sono state revocate ai sensi dell'articolo 7 capoverso 2 LBDI in combinato disposto con l'articolo 5 capoverso 2 OBDI. La DelCG giunge alla conclusione che queste basi legali sono in realtà soltanto un pretesto che, per diversi motivi, non regge di fronte a un'analisi fattuale e giuridica.

- Prima di tutto, la DelCG dispone di documenti dai quali emerge che non esisteva alcun motivo ai sensi dell'articolo 7 LBDI e che si è cercato accanitamente di ritardare la procedura ricorrendo ad atti burocratici per guadagnare tempo e costruire una motivazione della revoca. Il risultato è stato il nesso instaurato tra l'articolo 7 capoverso 2 LBDI e l'articolo 5 capoverso 2 OBDI.
- Secondariamente, il fatto di riferirsi all'articolo 5 capoverso 2 OBDI non convince, poiché almeno un'autorizzazione generale d'esportazione è stata rilasciata ancora il 3 dicembre 2019. Il fatto che le condizioni richieste fossero adempiute solo 17 giorni prima della revoca della licenza convalida ulteriormente la conclusione a cui è giunta la DelCG, ossia che si tratta di un motivo pretestuoso, costruito a posteriori, altrimenti l'autorizzazione non avrebbe dovuto essere rilasciata il 3 dicembre 2019.
- In terzo luogo, per quanto riguarda le domande di autorizzazioni singole all'esportazione che il 19 giugno 2020 il Consiglio federale ha respinto e per le quali ha rinviato la decisione, il DEFR è giunto alla conclusione che in realtà un'autorizzazione avrebbe dovuto essere rilasciata. Se la condizione sancita nell'articolo 5 capoverso 2 OBDI fosse stata veramente non adempiuta, la SECO avrebbe dovuto pronunciarsi a favore di una reiezione delle domande, cosa che non ha fatto.

La SECO voleva inoltre evitare di dover emanare una decisione impugnabile. Fa altresì valere che le società coinvolte avrebbero potuto esigere una tale decisione, ma che si sono astenute. Sebbene dal punto di vista giuridico non si possa muovere alcun rimprovero alla SECO al riguardo, queste affermazioni sono in linea con il quadro qui delineato: tanto la Crypto International AG quanto la TCG Legacy AG hanno affermato di aver presupposto che avrebbero ricevuto la decisione e la motivazione della revoca per posta. La DelCG constata in proposito che il principio della buona fede, garantito dalla Costituzione[43] (art. 9 Cost.), viene messo a dura prova.

Inoltre, la DelCG si stupisce che il capo del DEFR, secondo quanto da lui stesso affermato, abbia incaricato di chiarire la situazione giuridica solo dopo il 20 dicembre 2019, quindi dopo la revoca delle autorizzazioni generali d'esportazione. La questione della revoca non è stata sottoposta neppure al GCE.

La DelCG constata che la revoca delle autorizzazioni generali d'esportazione decisa dalla SECO il 20 dicembre 2019 su istruzioni del capo del DEFR non era fondata su basi legali, quindi era illecita. Costituisce una violazione del principio della legalità secondo l'articolo 5 Cost. e del diritto d'essere trattato senza arbitrio secondo l'articolo 9 Cost.

43 Costituzione federale della Confederazione Svizzera (Cost.; RS **101**).

La DelCG ritiene tuttavia che ai responsabili presso la SECO non deve essere espresso alcun biasimo poiché si sono ritrovati nella situazione delicata di dover eseguire e motivare la decisione del capo del DEFR. La responsabilità della procedura deve essere attribuita unicamente al capo del DEFR e alla SG-DEFR.

8.4 Denuncia penale della SECO

Il 25 febbraio 2020 la SECO ha sporto denuncia penale contro ignoti presso il MPC. Nella denuncia indica che gli apparecchi di cifratura esportati, quindi soggetti al controllo svizzero delle esportazioni, fino al 2018 avrebbero potuto essere manipolati, con conseguente violazione del diritto in materia di controllo delle esportazioni. La SECO fonda la denuncia in particolare su una possibile violazione dell'articolo 14 capoverso 1 lettera c LBDI e dell'articolo 9 capoverso 1 lettera a OICoM.

8.4.1 Decisioni prese in seno al DEFR

In seguito alla sospensione delle autorizzazioni generali d'esportazione da parte del DEFR, la SECO si è chiesta se l'attività della Crypto AG fosse punibile. I primi elementi che attestano tale ipotesi risalgono al 12 febbraio 2020, quando il capo del settore Controlli all'esportazione/Prodotti industriali (BWIP) presso la SECO ha asserito che il MPC doveva essere messo immediatamente a conoscenza della possibile violazione del diritto in materia di controlli delle esportazioni. Il capo stesso del BWIP ha proceduto alla necessaria interpretazione del diritto. Il contatto con il MPC è stato accolto con favore sia dai superiori diretti in seno alla SECO sia dalla SG-DEFR. Il giorno stesso è stato chiesto un colloquio con il MPC.

Parallelamente, il capo del BWIP è stato pregato dalla SG-DEFR di chiarire al più presto se la SECO doveva depositare una denuncia penale. Il 17 febbraio 2020 è stato quindi comunicato alla SG-DEFR che, dal punto di vista della SECO, sussisteva almeno una presunta violazione della LBDI (art. 14 cpv. 1 lett. c LBDI).

Il 21 febbraio 2020 si sono incontrati i rappresentanti della SECO e quelli del MPC. Secondo la nota redatta dalla SECO in quell'occasione emerge che il MPC non aveva identificato alcuna violazione del diritto in materia di controllo delle esportazioni in quel momento e in considerazione degli elementi conosciuti. Il MPC sospettava che gli apparecchi in questione presentassero una cifratura «debole» senza funzioni crittoanalitiche. In questo caso gli istanti non avrebbero fornito indicazioni errate o inesatte. Nell'insieme, il MPC ha ritenuto che non si imponesse una denuncia formale da parte della SECO, tuttavia la denuncia dava l'occasione al MPC di disporre il sequestro a titolo preventivo degli apparecchi di cifratura di cui era richiesta l'autorizzazione d'esportazione. In occasione della sua audizione di fronte alla DelCG, il procuratore generale della Confederazione (*Michael Lauber*) ha confermato che il MPC aveva sconsigliato la SECO di sporgere denuncia. A suo avviso, lo scopo della denuncia era passare «la patata bollente» dal DEFR al MPC. Secondo il MPC, l'opportunità di sporgere una denuncia penale dipendeva anche dal risultato dell'esame politico del caso Crypto AG, in particolare da parte della DelCG.

Dopo l'incontro con il MPC, si è svolto un altro colloquio tra la SECO e la SG-DEFR, dal quale emerge che la decisione di sporgere una denuncia penale era stata presa dalla SECO e non dalla SG-DEFR, che tuttavia l'aveva incoraggiata a farlo. La bozza del testo della denuncia è stata sottoposta alla segretaria di Stato che si è dichiarata favorevole, ma non ha voluto figurare tra i firmatari. Il capo del DEFR (*Guy Parmelin*) ha poi dichiarato alla DelCG che la situazione giuridica era chiara e che la SECO non poteva esimersi dal presentare una denuncia penale. Anche se non lo avesse fatto, la SECO avrebbe rischiato di essere criticata comunque. La denuncia penale è stata depositata ufficialmente il 25 febbraio 2020.

8.4.2 Valutazione della denuncia da parte della DelCG

Secondo quanto indicato nella sua denuncia, la SECO sospettava la Crypto AG di aver esportato apparecchi manipolati, ossia che utilizzavano procedure di cifratura «deboli». Secondo la SECO, il sospetto era fondato sulle rivelazioni apparse nei media sul caso Crypto AG.

Dalla presunta esistenza di una procedura di cifratura «debole», la SECO ha dedotto che gli apparecchi non servissero solo alla cifratura, ma anche alla crittoanalisi[44]. Avrebbero dunque consentito di analizzare procedure di cifratura e, avvalendosi dei risultati dell'analisi, di decrittare le informazioni cifrate con questa procedura.

Tuttavia, la SECO non ha tenuto conto del fatto che il destinatario di un apparecchio dotato di una cifratura «debole», controllato nell'ambito del controllo delle esportazioni, non può trarne alcun vantaggio in termini di crittoanalisi. Avendo cifrato lui stesso le informazioni, non ha bisogno di decrittarle per conoscerle. Procedure di cifratura «deboli» possono invece consentire più facilmente a terzi di violare la cifratura degli apparecchi esportati dalla Svizzera.

Oltre al sospetto espresso, la denuncia della SECO non conteneva indicazioni concrete di «falle» nelle procedure di cifratura utilizzate o in riferimento a funzioni crittoanalitiche presunte. Non menzionava neppure informazioni concrete nei media che avrebbero confermato l'esistenza di queste funzioni.

All'epoca i media avevano tuttavia rivelato che l'esistenza di procedure di cifratura «deboli» erano state tenute segrete ai destinatari degli apparecchi, i quali non potevano dunque essere in alcun caso a conoscenza delle funzioni crittoanalitiche presunte dalla SECO.

Secondo le informazioni che i media hanno tratto dal rapporto MINERVA e pubblicato, gli stessi servizi di intelligence americani avevano sviluppato le procedure di cifratura «deboli» per gli apparecchi della Crypto AG e le avevano impostate in modo

44 Cfr. EKN 5A004 nell'allegato 2 parte 2 dell'elenco dei beni a duplice impiego.

tale da poter violare le cifrature in tempo utile servendosi di queste conoscenze preliminari e potendo avvalersi di sufficienti capacità di calcolo[45]. I servizi americani e i loro partner disponevano dunque sin dall'inizio delle capacità crittoanalitiche necessarie per farlo. L'esportazione di queste funzioni, sviluppate all'estero, era quindi impossibile con un apparecchio della Crypto AG fabbricato in Svizzera.

Evidentemente, sia la SECO sia il DEFR hanno basato la denuncia penale sulle informazioni pubblicate dai media, senza averne analizzato né compreso il contenuto. Neppure altri servizi dell'Amministrazione sono stati interpellati per verificare la plausibilità dei sospetti della SECO prima di presentare la denuncia penale. Nell'accertamento dei fatti la SECO non ha quindi dato prova della diligenza che sarebbe stata indispensabile in considerazione delle conseguenze di vasta portata della sua denuncia. Sembra inoltre che la SECO si sia accontentata di una valutazione giuridica approssimativa, senza averne mai verificato la plausibilità, come conferma il fatto che solo dopo aver presentato la denuncia ha preso contatto con il delegato federale alla cibersicurezza.

La SECO ha altresì supposto che le esportazioni della Crypto AG fossero assoggettate all'obbligo d'autorizzazione ai sensi dell'OICoM, ma questo sarebbe stato plausibile solo se lo Stato a cui erano destinati gli apparecchi della Crypto AG avesse potuto utilizzare le procedure di cifratura «deboli» anche per sorvegliare le attività digitali dei suoi abitanti. Tuttavia, la crittologia «debole» degli apparecchi comprometteva solo le cifrature delle autorità dello Stato repressivo che li utilizzava, ma non quella dei suoi cittadini, di conseguenza l'ipotesi che gli apparecchi di cifratura della Crypto AG potessero essere assoggettati alla OICoM non può, di fatto, essere corretta e non consente di dedurne che la società abbia violato i suoi obblighi di dichiarazione previsti dall'ordinanza.

Non sono convincenti neppure gli argomenti avanzati dalla SECO per suffragare i suoi sospetti di violazione della LBDI, secondo cui le esportazioni di beni dotati di funzioni crittoanalitiche sono soggette all'obbligo d'autorizzazione. Dal momento che la Crypto AG non aveva dichiarato tali funzioni nelle sue domande d'esportazione, la SECO sospettava che fosse colpevole di aver fornito informazioni incomplete.

In proposito va osservato che solo le procedure di cifratura «forti» sottostanno al controllo delle esportazioni[46]. Dall'ipotesi astratta della SECO, secondo cui una cifratura «debole» implica necessariamente funzioni crittoanalitiche, scaturisce che dalla caratteristica stessa di un apparecchio, ossia la cifratura «debole», deriva da un lato l'obbligo di ottenere un'autorizzazione a causa delle funzioni crittoanalitiche, dall'altro l'esenzione da tale obbligo poiché la crittologia è «debole». Si applicherebbero dun-

45 Cfr. The intelligence coup of the century. In: Washington Post, 11. Febr. 2020: la National Security Agency (NSA) non ha installato «backdoor» né ha programmato gli apparecchi in modo che potessero fornire la loro chiave di cifratura. La NSA doveva inoltre continuare a intercettare le comunicazioni di altri Paesi. (...) Tuttavia, le manipolazioni degli algoritmi della Crypto AG hanno agevolato il processo di decrittazione in quanto alcuni compiti che avrebbero richiesto mesi di lavoro potevano essere svolti in pochi secondi [trad.].

46 L'elenco dei beni a duplice impiego, che figura nell'allegato 2 parte 2 LBDI, definisce con il numero di controllo delle esportazioni 5A002 i tipi di procedure di cifratura e la lunghezza minima delle chiavi utilizzate che sono soggetti all'obbligo di autorizzazione.

que prescrizioni contraddittorie all'esportazione di un apparecchio che presenti la duplice caratteristica presunta dalla SECO. Dal momento che l'errore non può essere insito nel diritto in materia di controllo delle esportazioni, alla luce di questa normativa deve essere sbagliata l'ipotesi astratta della SECO secondo cui gli apparecchi con procedure di cifratura «deboli» debbano possedere anche funzioni crittoanalitiche.

8.4.3 Richiesta di autorizzazione del MPC e colloquio della DelCG con la presidente della Confederazione e la responsabile del DFGP

L'articolo 66 capoverso 1 LOAP (reati politici) prevede che i reati politici possano essere perseguiti previa autorizzazione del Consiglio federale, che può negarla per tutelare gli interessi del Paese.

Nella sua richiesta di autorizzazione del 13 marzo 2020, il MPC dichiara che esiste motivo sufficiente di sospettare un delitto o un crimine ai sensi dell'articolo 14 LBDI e dell'articolo 9 OICoM. Il MPC asserisce che l'applicabilità dell'articolo 66 LOAP non è chiaramente disciplinata e che l'articolo non si limita al titolo tredicesimo del Codice penale. Il MPC conclude che le diverse condizioni sono adempiute con la denuncia penale presentata dalla SECO, quindi sottopone al Consiglio federale la decisione concernente l'autorizzazione ad avviare un perseguimento giudiziario. In questa sede non è necessario esporne i diversi motivi.

Nella richiesta di autorizzazione sottoposta al Consiglio federale, il MPC ha dichiarato che non era urgente accordare un'autorizzazione e che era comunque poco sensato farlo prima che la DelCG valutasse la questione in un'ottica politica.

Il 25 maggio 2020, anche in considerazione della richiesta di autorizzazione del MPC, la DelCG ha avuto un colloquio con la presidente della Confederazione (*Simonetta Sommaruga*) e la responsabile del DFGP (*Karin Keller-Sutter*), alla quale era stata indirizzata la richiesta d'autorizzazione. Come esposto nel capitolo 7.5, all'epoca la DelCG non sapeva se il Consiglio federale avesse compreso il carattere sensibile e la vera portata della questione. Proprio a causa della richiesta di autorizzazione rivolta dal MPC al DFGP, la Delegazione desiderava informare la presidente della Confederazione e la responsabile del DFGP degli ultimi elementi acquisiti, sulle cui basi il Consiglio federale avrebbe quindi potuto valutare la richiesta. Inoltre, la responsabile del DFGP aveva auspicato un colloquio con la DelCG per valutare se si trattasse di un caso di particolare importanza, che doveva essere sottoposto alla decisione del Consiglio federale. La responsabile del Dipartimento ha asserito che, secondo la prassi corrente, un'autorizzazione era rifiutata solo in rari casi e unicamente se appariva inopportuna per importanti motivi istituzionali.

Con lettera del 28 maggio 2020 la DelCG ha messo al corrente l'intero collegio governativo dei principali risultati intermedi delle sue investigazioni, segnalandogli nel contempo i rischi che, a suo avviso, la denuncia penale rappresentava per la sicurezza della Svizzera. Ha tuttavia sottolineato chiaramente che la decisione in merito alla richiesta di autorizzazione del MPC fosse una questione politica, alla quale solo il Consiglio federale doveva rispondere.

In occasione della seduta del 19 giugno 2020, il Consiglio federale ha quindi deciso di autorizzare l'MPC ad avviare un perseguimento penale. Le principali conclusioni della DelCG sono state riprese nella proposta che il DFGP ha sottoposto al Consiglio federale.

8.5 Domande di esportazione specifiche delle società subentrate alla Crypto AG

Dalla decisione del DEFR del 20 dicembre 2019 di revocare le autorizzazioni generali d'esportazione scaturisce quella di valutare eventuali domande future nel quadro di una procedura di autorizzazione singola. Fino al 10 giugno 2020 erano state presentate 13 domande di esportazione della Crypto International AG e due della TCG Legacy AG.

Il 4 marzo 2020 il gruppo di controllo delle esportazioni si è riunito in virtù dell'articolo 27 capoverso 3 OBDI per deliberare in merito alle diverse domande di esportazione. Il GCE ha deciso di sottoporre le domande in questione alla decisione del Consiglio federale conformemente all'articolo 47 capoverso 4 della legge sull'organizzazione del Governo e dell'Amministrazione (LOGA)[47], giungendo tuttavia alla conclusione che non esistevano motivi legali tali da impedire il rilascio dell'autorizzazione all'esportazione. Nel maggio 2020 il DATEC e il DDPS si sono pronunciati a favore del rilascio. Il DFAE voleva sottoporre le domande della TCG Legacy AG e della Crypto International AG alla decisione del Consiglio federale.

Il 10 marzo 2020 la SECO e il delegato federale alla cibersicurezza si sono incontrati per un colloquio in seguito a un mandato della SECO volto a stabilire chi potesse coadiuvarla nell'analisi degli apparecchi di cifratura eventualmente manipolati in caso di future domande d'esportazione. Il delegato ha risposto alle domande della SECO il 30 marzo 2020 con una nota informativa nella quale affermava che un esame degli apparecchi era certamente possibile, tuttavia avrebbe richiesto molto tempo e non avrebbe praticamente fornito indicazioni fondate. Ha precisato che, senza ricorrere al know-how degli esperti di crittologia dell'esercito, un esame tecnico non era realistico. La SG-DDPS ha tuttavia rifiutato una collaborazione in materia, di conseguenza il delegato ha proposto di rinunciare all'esame degli apparecchi prima dell'esportazione. La DelCG constata che si tratta dei primi sforzi compiuti dalla SECO, dopo la decisione di revocare le autorizzazioni generali d'esportazione e la presentazione della denuncia penale, di acquisire la competenza necessaria a valutare le domande.

Nella sua prima proposta al Consiglio federale del 10 giugno 2020, il DEFR ha chiesto che tutte le domande fossero autorizzate. Ne consegue che, secondo il GCE, non c'era alcun motivo legale in grado di giustificare il rifiuto dell'esportazione. Il DEFR ha poi operato una sorprendente inversione di rotta sottoponendo al Consiglio federale una proposta rielaborata nella quale chiedeva di rimandare la decisione in merito alle domande di esportazione fino alla conclusione dell'inchiesta del MPC. La DelCG non

47 Legge del 21 mar. 1997 sull'organizzazione del Governo e dell'Amministrazione (LOGA; RS **172.010**).

si spiega questo mutamento, considerando che né la valutazione del delegato alla cibersicurezza né quella del GCE erano cambiate. A suo avviso, la sola spiegazione plausibile poteva risiedere nella procedura di corapporto, nella quale un dipartimento aveva manifestato l'auspicio che il Consiglio federale non decidesse in merito alle domande di esportazione prima della conclusione delle inchieste del MPC e della DelCG. La richiesta è stata accolta dal Consiglio federale nella sua seduta del 19 giugno 2020. Il DEFR ha inoltre sottolineato nella motivazione della sua proposta che non era da escludere che le domande di autorizzazioni singole all'esportazione riguardassero anche gli apparecchi appartenenti agli stock dell'ex Crypto AG. La posizione iniziale del DEFR favorevole ad autorizzare le domande sorprende anche per questo. Gli argomenti con cui il DEFR ha motivato la sua proposta al Consiglio federale non sono stati modificati nonostante quest'ultima sia stata oggetto di una profonda rielaborazione.

La DelCG ignora se le domande riguardassero anche gli apparecchi sequestrati dal MPC o se questo aspetto sia stato chiarito dal DEFR.

Il 7 agosto 2020 la Crypto International AG ha presentato una richiesta di riesame della sua domanda di esportazione, respinta dal Consiglio federale nella sua seduta del 26 agosto 2020.

8.6 Denuncia penale e rinvio della trattazione delle domande d'esportazione singole: valutazione della DelCG

La DelCG non capisce l'approccio seguito dal Consiglio federale, dal DEFR e dalla SECO in riferimento alle domande di esportazione singole delle due società Crypto International AG e TCG Legacy AG. Da un lato va osservato che è passato molto tempo tra la presentazione delle domande e la decisione del Consiglio federale del 19 giugno 2020 o, meglio, il momento in cui la proposta è stata sottoposta per decisione al Consiglio federale. È opportuno menzionarlo soprattutto perché il 4 marzo 2020 il GCE aveva già deliberato che non esistevano motivi legali tali da opporsi all'esportazione. D'altro canto, e proprio con le suddette premesse, la DelCG critica le decisioni prese dal Consiglio federale il 19 giugno 2020 e il 26 agosto 2020 di sospendere la decisione relativa alle domande fino alla conclusione del procedimento del MPC. Anche se in questo caso, come affermato dal Consiglio federale, la legge non fissa termini per il trattamento di una domanda, l'approccio seguito dal Consiglio federale potrebbe violare il principio della buona fede, poiché in linea di massima ogni impresa svizzera ha diritto a un trattamento rapido delle sue domande di autorizzazione all'esportazione a meno che non vi si oppongano motivi giuridici.

Non è accettabile che la SECO applichi ormai ad altre domande di autorizzazioni singole all'esportazione le decisioni del Consiglio federale del 19 giugno 2020 e del 26 agosto 2020, riguardanti invece domande d'esportazione specifiche.

In riferimento alla denuncia penale, la DelCG è sorpresa che una denuncia penale sia presentata per motivi politici da un ufficio federale o da una segreteria di Stato e che non rientri nella competenza della massima autorità politica (capodipartimento o Consiglio federale), tanto più che la denuncia in questione è giustificata da motivi politici.

La DelCG desidera sottolineare in particolare che la SECO aveva una conoscenza puramente frammentaria dei fatti e che nella formazione della propria opinione si è basata in primo luogo sulle rivelazioni dei media. Secondo la DelCG, queste circostanze hanno indotto la SECO ad assoggettare erroneamente l'esportazione degli apparecchi di cifratura all'obbligo di autorizzazione secondo l'OICoM. Un tale modo di procedere ha impedito di comprendere correttamente la vera portata dei fatti. Alla luce di quanto suesposto, la presentazione di una denuncia penale da parte della SECO è più che problematica per motivi politici.

In ultima istanza, la procedura di controllo dei beni è stata utilizzata dal dipartimento competente per fare fronte alle pressioni politiche scaturite dal dibattito nell'opinione pubblica sul caso Crypto AG, ma la legislazione in materia di controllo dei beni non era lo strumento adeguato per dare una risposta politica a una questione che riguardava le attività informative come il caso Crypto AG. Con la denuncia penale della SECO, in primo luogo il DEFR, ma anche il Consiglio federale si sono sottratti alle loro responsabilità di condotta politica.

8.7 Conseguenze dell'ispezione della DelCG

L'approccio seguito dalla SECO e dal DEFR hanno avuto conseguenze rilevanti anche sull'operato del Consiglio federale e sul lavoro della DelCG. Già nella sua richiesta di autorizzazione al DFGP, il MPC aveva evocato un possibile legame tra il procedimento penale e i risultati dell'ispezione della DelCG. Il Consiglio federale, quando ha deliberato che non si sarebbe pronunciato sull'autorizzazione delle domande di esportazione delle società subentrate alla Crypto AG prima della chiusura del procedimento del MPC, ha accettato di non poter prendere una decisione neppure prima che la DelCG concludesse i suoi lavori.

Quando ha realizzato che le decisioni del Consiglio federale del 19 giugno 2020 implicavano un rinvio, a data da destinarsi, della decisione finale sulle domande di esportazione delle società che erano subentrate alla Crypto AG, la DelCG si è vista costretta a estendere la sua ispezione a questo nuovo aspetto del caso Crypto AG. Le decisioni del Consiglio federale hanno dunque reso più onerosa l'ispezione della DelCG, il che ha a sua volta ritardato i lavori del MPC. Infine, il Consiglio federale ha associato il suo trattamento delle domande di esportazione in sospeso all'ispezione dell'alta sorveglianza parlamentare, il che costituisce un problema dal punto di vista della separazione dei poteri.

Nell'ottica della DelCG è necessario precisare che il 28 maggio 2020 aveva informato per scritto il Consiglio federale di tutti i fatti rilevanti concernenti i legami tra la Crypto AG, il servizio di intelligence americano e il Servizio informazioni svizzero. Dal 26 febbraio 2020 ogni consigliere federale era inoltre in possesso di una copia del bilancio interno della situazione stilato dal SIC a metà settembre 2019 (cfr. n. 4.1.3). Il 19 giugno 2020 il Consiglio federale era dunque in possesso di tutte le informazioni necessarie per procedere a una propria valutazione degli aspetti importanti in merito al caso Crypto AG. Avrebbe dunque potuto dotarsi di tutte le basi decisionali necessarie per prendere una decisione finale riguardo ai due oggetti (domanda di autorizza-

zione e domanda d'esportazione) ancora in sospeso in seguito alla reazione non concertata del capo del DEFR (*Guy Parmelin*) al caso Crypto AG. Non c'era alcun motivo di attendere la conclusione del procedimento penale del MPC né dell'ispezione della DelCG.

Nella sua riposta a diversi interventi parlamentari depositati durante la sessione primaverile, il Consiglio federale ha spiegato che avrebbe atteso il rapporto della DelCG dopo che quest'ultima aveva revocato, il 21 febbraio 2020, la sua autorizzazione all'inchiesta del Consiglio federale condotta dal signor Oberholzer[48]. Ha inoltre dichiarato che non avrebbe preso alcuna decisione che potesse nuocere all'ispezione della DelCG o pregiudicarla. Depositando la denuncia penale il 25 febbraio 2020, la SECO aveva già agito in contraddizione con questa linea di condotta definita dal Consiglio federale, prima che venisse comunicata all'Assemblea federale. Pur senza mettere in discussione l'indipendenza della giustizia, la DelCG ritiene quindi necessario un coordinamento delle denunce penali presentate dall'Esecutivo se rischiano di nuocere a un'ispezione decisa dalla Delegazione.

9 Raccomandazioni

Raccomandazione 1: la responsabile del DDPS e la sua Segreteria generale si dotano degli strumenti necessari per essere in grado, da un lato, di procurarsi immediatamente e in modo autonomo le informazioni di cui necessitano in un caso che riguardi le attività informative e, dall'altro, per assicurare la condotta politica nei confronti del SIC e la capacità d'azione a livello di Consiglio federale. Sintanto che ciò non sarà garantito, i mandati conferiti all'AVI-AIn o a inquirenti esterni non sono da considerarsi opportuni.

Raccomandazione 2: il DDPS ricorre alla DelSic in modo mirato per garantire lo scambio di informazioni riguardanti i dossier nell'ambito delle attività informative, rafforzando così la capacità di condotta del Consiglio federale in materia. La DelSic o una delegazione ad hoc del Consiglio federale dovrà intervenire in particolare laddove il DDPS non voglia o non possa comunicare informazioni segrete in seno agli organi dell'Amministrazione.

Raccomandazione 3: il DDPS provvede affinché il CEs partecipi in linea di principio alle sedute della DelSic in qualità di rappresentante dell'Amministrazione. Se fosse necessario per preparare i dossier della DelSic, il CEs dovrà prendere parte anche alle sedute del Comitato ristretto Sicurezza.

Raccomandazione 4: il DDPS informa il Consiglio federale se una collaborazione in materia di attività informative tra il SIC e un servizio partner implica una società svizzera. Il Consiglio federale dovrà stabilire i criteri in base ai quali intende decidere autonomamente su una tale collaborazione.

48 Per es. interpellanza urgente del gruppo socialista «Caso Crypto. Il Consiglio federale è invitato ad agire invece di stare a guardare» (20.3034).

Raccomandazione 5: la Confederazione non acquista soluzioni di cifratura da fornitori esteri. I fornitori indigeni devono garantire alla Confederazione di poter controllare gli aspetti legati alla sicurezza dello sviluppo e della produzione.

Raccomandazione 6: il DDPS garantisce che l'esercito conservi, come avvenuto finora, sufficienti competenze specialistiche in materia di crittologia per riuscire a valutare la sicurezza delle soluzioni di cifratura acquistate dalla Confederazione. Occorre garantire che le sinergie tra le competenze crittografiche e quelle crittoanalitiche siano sfruttate in modo ottimale.

Raccomandazione 7: il DDPS garantisce che le capacità di crittoanalisi siano in linea con le esigenze nell'ambito dell'esplorazione delle comunicazioni, le cui possibilità sono state estese nella LAIn all'esplorazione di segnali via cavo.

Raccomandazione 8: il DDPS disciplina le modalità di archiviazione sicura e legale dei documenti dei massimi livelli della sua direzione che si riferiscono alla sua attività diretta di condotta e sorveglianza nelle attività informative. Inoltre, la SG-DDPS assicura l'archiviazione della documentazione personale degli ex capi del DDPS e ne rende conto alla DelCG.

Raccomandazione 9: la DelCG ritiene necessario che, in caso di necessità, il SIC possa accedere rapidamente alle conoscenze disponibili in merito alle attività informative passate. Parallelamente all'archiviazione dei documenti provenienti dalla ricerca operativa e dagli scambi condotti tra le organizzazioni che l'hanno preceduto e i servizi stranieri, a tal fine il SIC appronta una visione d'insieme delle operazioni e delle fonti per le quali esistono ancora dossier.

Raccomandazione 10: la DelCG invita il Consiglio federale a revocare la sua autorizzazione al procedimento penale che il MPC ha avviato sulla base della denuncia penale della SECO. In seguito, il DEFR dovrà autorizzare tutte le domande d'esportazione presentate dalle società subentrate alla Crypto AG per le quali nessun motivo giuridico chiaro possa giustificare un rifiuto.

Raccomandazione 11: la DelCG riceve man mano le note segrete riguardanti le attività informative o aventi un rapporto con gli oggetti in corso di esame da parte della Delegazione, di cui il Consiglio federale giunge a conoscenza. Il Consiglio federale sottopone alla DelCG una proposta in merito alla procedura da seguire.

Raccomandazione 12: la DelCG è preliminarmente consultata in merito alle denunce penali della Confederazione riguardanti fatti o persone che sono oggetto di un'ispezione condotta dalla Delegazione. A tal fine, il dipartimento competente o la CaF chiedono un parere scritto all'autorità di perseguimento penale in questione.

10 Seguito della procedura

La DelCG invita il Consiglio federale a prendere posizione in merito al presente rapporto e alle raccomandazioni ivi formulate entro il 1° giugno 2021. Il MPC è invitato a pronunciarsi riguardo alla raccomandazione n. 12 entro il 1° giugno 2021.

2 novembre 2020

In nome della Delegazione
delle Commissioni della gestione:

Il presidente, Alfred Heer
La segretaria, Beatrice Meli Andres

Le Commissioni della gestione del Consiglio nazionale e del Consiglio degli Stati hanno preso atto del presente rapporto e ne hanno approvato la pubblicazione.

10 novembre 2020

In nome della Delegazione
delle Commissioni della gestione:

Il presidente della Commissione
della gestione del Consiglio nazionale,
Erich von Siebenthal, consigliere nazionale

La presidente della Commissione
della gestione del Consiglio degli Stati,
Maya Graf, consigliera agli Stati

La segretaria, Beatrice Meli Andres

Elenco delle abbreviazioni

AFS	Archivio federale svizzero
AGFA	Abteilung für Genie und Festung Anlageverzeichnis (Divisione del genio e delle fortificazioni – elenco delle installazioni)
AVI-AIn	Autorità di vigilanza indipendente sulle attività informative
BAC	Base d'aiuto alla condotta
Boll. uff.	Bollettino ufficiale dell'Assemblea federale
BWIP	Settore Controlli all'esportazione/Prodotti industriali
CaF	Cancelleria federale
CdG	Commissioni della gestione delle Camere federali
CEs	Capo dell'esercito
Cost.	Costituzione federale della Confederazione Svizzera del 18 aprile 1999 (RS *101*)
CP	Codice penale (RS *311.0*)
CPI	Commissione parlamentare d'inchiesta
DATEC	Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DEFR	Dipartimento federale dell'economia, della formazione e della ricerca
DelCG	Delegazione delle Commissioni della gestione
DelSic	Delegazione Sicurezza del Consiglio federale
DFAE	Dipartimento federale degli affari esteri
DFF	Dipartimento federale delle finanze
DFGP	Dipartimento federale di giustizia e polizia
DMF	Dipartimento militare federale
Elic	E-licensing (sistema di autorizzazioni elettronico)
fedpol	Ufficio federale di polizia
FF	Foglio federale
GCE	Gruppo di controllo delle esportazioni
GLID	Gruppo di lavoro interdipartimentale
GSI	Gruppo servizio informazioni
Installazione K	Installazione protetta

ISIS	Prima del 2010 Sistema informatizzato per il trattamento dei dati relativi alla protezione dello Stato («informatisiertes Staatsschutz-informationssystem»); ora Sistema d'informazione sicurezza interna («Informationssystem Innere Sicherheit»)
Iv. Pa.	Iniziativa parlamentare
LAIn	Legge federale del 25 settembre 2015 sulle attività informative (RS *121*)
LAr	Legge federale del 26 giugno 1998 sull'archiviazione (RS *152.1*)
LBDI	Legge federale del 13 dicembre 1996 sul controllo dei beni utilizzabili a fini civili e militari, dei beni militari speciali e dei beni strategici (legge sul controllo dei beni a duplice impiego, RS *946.202*)
LM	Legge federale del 3 febbraio 1995 sull'esercito e sull'amministrazione militare (legge militare, RS *510.10*)
LMSI	Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (RS *120*)
LOAP	Legge federale del 19 marzo 2010 sull'organizzazione delle autorità penali della Confederazione (legge sull'organizzazione delle autorità penali, RS *173.71*)
LOGA	Legge del 21 marzo 1997 sull'organizzazione del Governo e dell'Amministrazione (RS *172.010*)
LParl	Legge federale del 13 dicembre 2002 sull'Assemblea federale (legge sul Parlamento; RS *171.10*)
LSIC	Legge federale del 3 ottobre 2008 sul servizio informazioni civile, abrogata il 1° settembre 2017 (RU *2009* 6565)
LTras	Legge federale del 17 dicembre 2004 sul principio di trasparenza dell'amministrazione (legge sulla trasparenza, RS *152.3*)
mia.	miliardo/miliardi
MPC	Ministero pubblico della Confederazione
NCE	Numero di controllo delle esportazioni
NDBB	Divisione Ricerca del SIC
NDBU	Divisione Supporto alla condotta e all'impiego del SIC
OBDI	Ordinanza federale del 3 giugno 2016 sul controllo dei beni utilizzabili a fini civili e militari, dei beni militari speciali e dei beni strategici (ordinanza sul controllo dei beni a duplice impiego, RS *946.202.1*)
OlCoM	Ordinanza del 13 maggio 2015 sull'esportazione e l'intermediazione di beni per la sorveglianza di Internet e delle comunicazioni mobili (RS *946.202.3*)
OMSI	Ordinanza del 27 giugno 2001 sulle misure per la salvaguardia della sicurezza interna, abrogata il 1° gennaio 2010 (RU *2001* 1829)

O-SIC	Ordinanza del 4 dicembre 2009 sul Servizio delle attività informative della Confederazione, abrogata il 1° settembre 2017 (RU *2009* 6937)
OSINF	Ordinanza del 4 dicembre 1995 concernente il servizio informazioni, abrogata il 1° gennaio 2001, citata nelle versioni del 4 dicembre 1995 (RU *1995* 5298), del 4 dicembre 2000 (RU *2001* 124) e con il nuovo titolo di ordinanza del 26 settembre 2003 sui servizi d'informazione del DDPS (RU *2003* 4001)
PCF	Polizia criminale federale
Polfed	Polizia federale
RS	Raccolta sistematica del diritto federale
RU	Raccolta ufficiale delle leggi federali
SA	Società anonima
SAP	Servizio di analisi e prevenzione
SECO	Segreteria di Stato dell'economia
SG	Segreteria generale
SIC	Servizio delle attività informative della Confederazione
SIS	Servizio di informazioni strategico
UFG	Ufficio federale di giustizia
UFTRM	Ufficio federale delle truppe di trasmissione

Allegato 1

Elenco delle persone ascoltate

Tra il 19 febbraio e il 26 agosto 2020 la DelCG ha condotto audizioni e colloqui con i rappresentati ed ex rappresentanti della Confederazione elencati di seguito:

Amherd, Viola	Consigliera federale, responsabile del DDPS (dal 2019)
Boehler, Jürgen	Capo del settore Controlli alle esportazioni/Prodotti industriali, SECO, DEFR
Brossard, Jean-Claude	Capo Supporto alla condotta e all'impiego, SIC, DDPS
Bühler, Jürg	Vicedirettore e capo Ricerca SIC a.i., DDPS, ex secondo sostituto del capo della Polfed (dal 1993), capo Ricerca SAP (dal 2001), capo Coordinamento/Situazione SIC (dal 2010), capo Analisi SIC (dal 2015)
Eckmann, Nils	Assistente procuratore federale, divisione Protezione dello Stato/Organizzazioni criminali, MPC
Eder, Toni	Segretario generale del DDPS
Gaudin, Jean-Philippe	Direttore del SIC, DDPS (dal 2018)
Haefelin, Rainer	Ex capo Sicurezza dell'informazione / Crittologia (2005–2018), BAC, DDPS
Keller-Sutter, Karin	Consigliera federale, responsabile del DFGP (dal 2019)
Koller, Arnold	Ex Consigliere federale, capo del DMF (1987–1989) e del DFGP (1989–1999)
Lauber, Michael	Procuratore generale della Confederazione (2012–2020)
Leuthold, Christian	Capo del Centro di operazioni elettroniche, BAC, DDPS
Maurer, Ueli	Consigliere federale, capo del DFF (dal 2016), ex capo del DDPS (2009–2015)
Nydegger, Kurt	Ex capo BAC (2003–2010)
Nyffeler, Peter	Ex capo sezione Crittologia e cifratura (1982–2004), UFTRM/sottogruppo Aiuto alla condotta/BAC
Oberholzer, Niklaus	Ex giudice federale, capo del comitato di ricerca del Consiglio federale, incaricato dell'inchiesta DelCG
Parmelin, Guy	Consigliere federale, capo del DEFR (dal 2019), ex capo del DDPS (2016–2018)
Regli, Peter	Ex sottocapo di stato maggiore informazioni (1991–2000), ex sostituto sottocapo di Stato maggiore informazioni (1989–1991), ex capo della sezione Informazioni dell'aviazione e della difesa contraerea (1981–1988)
Schmid, Samuel	Ex consigliere federale, capo del DDPS (2001–2008)

Schöttli, Thomas	Vicedirettore e capo Coordinamento/Situazione SIC, DDPS
Schreier, Fred	Ex capo SIS (1990–1999), ex capo della sezione Analisi (1978–1989), Gruppo informazione e sicurezza
Seiler, Markus	Segretario generale del DFAE (dal 2017), ex direttore del SIC, DDPS (2010–2017) e segretario generale del DDPS (2004–2009)
Sommaruga, Simonetta	Presidente della Confederazione, responsabile del DATEC (dal 2019), ex responsabile del DFGP (2010–2018)
Süssli, Thomas	Capo dell'esercito (dal 2020), ex capo BAC (2018–2019)
Villiger, Kaspar	Ex consigliere federale, capo del DMF (1989–1995) e del DFF (1996–2003)
von Daeniken, Urs	Ex capo SAP (2001–2008), ex capo Polfed (1990–2000)
Walter, René	Capo Sicurezza dell'informazione / Crittologia (dal 2018), BAC, DDPS
Wegmüller, Hans	Ex capo SIS (2001–2008), ex capo della sezione Ricerca (1987–1993) nel Gruppo servizio informazioni
Wüger, Daniel	Segretario generale aggiunto DFGP
X	Persona attualmente al servizio del DDPS
Y	Persona precedentemente al servizio del DDPS
Zinniker, Paul	Ex direttore aggiunto del SIC e capo Ricerca SIC (2010–2019), ex direttore del SIC ad interim (2017–2018), direttore del SIS (2008–2009) e capo Ricerca SIS (dal 1996)