Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Caso Crypto AG

Rapporto della Delegazione delle Commissioni della gestione del 2 novembre 2020

Parere del Consiglio federale

del 26 maggio 2021

Onorevoli presidente e consiglieri,

conformemente all'articolo 158 della legge sul Parlamento, vi presentiamo il nostro parere in merito al rapporto del 2 novembre 2020[1] della Delegazione delle Commissioni della gestione concernente il caso Crypto AG.

Gradite, onorevoli presidente e consiglieri, l'espressione della nostra alta considerazione.

26 maggio 2021

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Guy Parmelin
Il cancelliere della Confederazione, Walter Thurnherr

1 FF **2021** 156

Parere

1 Situazione iniziale

Il 10 novembre 2020 la Delegazione delle Commissioni della gestione delle Camere federali (DelCG o Delegazione) ha trasmesso al Consiglio federale il suo rapporto sul caso Crypto AG, invitandolo a esprimere, entro il 1° giugno 2021, il proprio parere in merito alle considerazioni e alle raccomandazioni da essa formulate nel suddetto rapporto.

Il «caso Crypto AG» riguarda un'operazione in materia di attività informative che ha avuto origine negli anni Settanta, quando la società di tale nome e con sede in Svizzera è stata acquisita congiuntamente dai servizi di intelligence americani e da quelli tedeschi. Dal 1993 il nostro Servizio informazioni strategico (SIS) è venuto a conoscenza del fatto che la Crypto AG esportava apparecchi «deboli» la cui cifratura poteva essere decodificata. Nel 2001 il SIS è stato trasformato in un'unità amministrativa civile e, grazie alla collaborazione con i servizi di intelligence statunitensi, mediante siffatti apparecchi della Crypto AG è riuscito a procurarsi maggiori informazioni concernenti l'estero.

L'inchiesta della Delegazione ha mostrato che nessuno dei predecessori dell'attuale capo del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) è mai stato informato di tale operazione dai capi o direttori del Servizio delle attività informative della Confederazione (SIC) o delle organizzazioni che l'hanno preceduto. Il 19 agosto 2019 l'attuale capo del DDPS è stato ragguagliato per la prima volta in modo sommario in merito a questioni critiche intorno alla società Crypto AG dal direttore del SIC, che è stato incaricato di acquisire informazioni attendibili sul caso. Il 31 ottobre 2019 il capo del DDPS è stato quindi informato in modo più approfondito quanto all'interesse dei media per la società e agli effetti che le rivelazioni potevano avere sulla collaborazione in materia di attività informative. La ragione di suddetto interesse è stata l'annunciata pubblicazione, da parte dei servizi di intelligence americani, di un rapporto segreto (MINERVA – A History) sull'operazione condotta circa la Crypto AG.

All'inizio di novembre 2019 il capo del DDPS ha informato il Consiglio federale, che si è poi occupato intensamente del caso Crypto AG. Qui di seguito ci si soffermerà di nuovo sulla cronologia esatta delle attività del DDPS, degli altri dipartimenti, della Cancelleria federale e del Consiglio federale.

Durante la seduta del Consiglio federale del 6 novembre 2019, con una nota informativa segreta il DDPS lo ha informato in merito ai primi elementi acquisiti sul caso Crypto AG. Il giorno successivo si è svolta una riunione con il capo del DDPS, il vicecancelliere e portavoce del Consiglio federale, la segretaria generale del Dipartimento federale di giustizia e polizia (DFGP), il segretario generale del DDPS e rappresentanti del SIC. È stato deciso di istituire un gruppo di lavoro interdipartimentale e di informare le autorità di vigilanza (DelCG e autorità di vigilanza indipendente sulle attività informative [AVI-AIn]). Il 12 novembre 2019 il presidente della DelCG e il capo dell'AVI-AIn sono stati messi al corrente di persona dal capo del DDPS

quanto al contenuto della nota segreta. Il 18 novembre 2019 si è svolta la prima riunione del gruppo di lavoro interdipartimentale. Fino al 3 marzo 2020 ve ne sono state in tutto cinque.

Sulla base di un documento interlocutorio del DDPS, il caso Crypto AG è stato trattato nella seduta del Consiglio federale del 20 dicembre 2019. Quest'ultimo ha deciso il seguito della procedura: il DDPS è stato incaricato di elaborare, in collaborazione con il DFGP, una proposta per la direzione di un organo d'inchiesta indipendente e di presentarla al Consiglio federale nella seduta del 15 gennaio 2020. L'8 gennaio 2020 il segretario generale del DDPS ha chiesto all'ex giudice federale Niklaus Oberholzer se voleva assumersi l'inchiesta sui fatti concernenti la società Crypto AG. Il signor Oberholzer si è detto disposto ad accettare l'incarico.

Il 20 dicembre 2019 la Segreteria di Stato dell'economia (SECO) ha revocato a due società subentrate alla Crypto AG, la TCG Legacy AG e la Crypto International AG, le autorizzazioni generali d'esportazione, sospendendole fino a nuovo avviso. Tale decisione è stata presa dietro istruzioni della Direzione del Dipartimento federale dell'economia, della formazione e della ricerca (DEFR). In tale contesto si è altresì stabilito che la SECO avrebbe continuato a esaminare le domande di autorizzazioni singole all'esportazione.

Il 15 gennaio 2020, su richiesta del DDPS, il Consiglio federale ha affidato a Niklaus Oberholzer la direzione dell'organo di inchiesta sui fatti nel caso Crypto AG. L'ex giudice federale doveva potere accedere rapidamente a tutti i documenti rilevanti presso l'Archivio federale (AFS) e nelle unità amministrative interessate. Al più tardi entro la fine di giugno del 2020 doveva essere presentato un primo rapporto all'attenzione del Consiglio federale. Se dopo una prima consultazione dei documenti disponibili fosse stato necessario precisare il mandato d'inchiesta, il DDPS ne avrebbe informato quest'ultimo.

È stato inoltre deciso che il resoconto sull'inchiesta sarebbe stato presentato al Consiglio federale alla fine di giugno del 2020. In base alle informazioni disponibili in quel momento, esso avrebbe deciso sul da farsi e su un possibile ulteriore approfondimento dell'inchiesta. Il 16 gennaio 2020 il signor Oberholzer ha iniziato il proprio lavoro presso l'AFS.

Il 14 febbraio 2020 la Delegazione ha comunicato per scritto al Consiglio federale di avere avviato un'ispezione formale. Nel contempo, essa ha accolto con favore il mandato d'inchiesta conferito dal Consiglio federale e, ai sensi dell'articolo 154*a* capoverso 1 della legge sul Parlamento (LParl; RS *171.10*), l'ha autorizzato a proseguire tali lavori.

Il 15 febbraio 2020 il capo del DDPS ha ricevuto da Niklaus Oberholzer un primo rapporto succinto sullo stato dei suoi accertamenti provvisori. Il 19 febbraio 2020 il Consiglio federale ha preso atto di tale documento a seguito di una nota informativa segreta del DDPS.

Nell'interesse di un chiarimento rapido ed efficace, alla fine di febbraio 2020 la Delegazione ha deciso che da quel momento avrebbe assunto la responsabilità dell'esame affidato dal Consiglio federale all'ex giudice federale Oberholzer. Tutti gli accertamenti svolti fino ad allora sul caso Crypto AG sono stati quindi riuniti nell'ispezione

della DelCG. Il 21 febbraio 2020 essa ha comunicato la sua decisione al Consiglio federale e il 26 febbraio 2020 ha informato i media.

Il 25 febbraio 2020 la SECO ha sporto denuncia contro ignoti al Ministero pubblico della Confederazione (MPC) fondandola su una possibile violazione del diritto in materia di controllo dei beni a duplice impiego.

Il 5 marzo 2020 la presidente della Confederazione ha comunicato per scritto alla Delegazione che il Consiglio federale ha preso atto della decisione di quest'ultima di revocare l'autorizzazione a proseguire l'inchiesta da parte di Niklaus Oberholzer. Nella lettera il Consiglio federale le ha assicurato che avrebbe garantito il regolare trasferimento dei dossier e sostenuto la sua inchiesta. Fino alla conclusione dell'ispezione della DelCG all'inizio di ottobre 2020, i dipartimenti e gli uffici interessati le hanno fornito molta documentazione. Membri del Consiglio federale e rappresentanti dell'Amministrazione federale hanno partecipato a varie audizioni della Delegazione.

Il 19 giugno 2020, su richiesta del DEFR, il Consiglio federale ha deciso di sospendere, fino alla conclusione dell'inchiesta da parte del MPC, la decisione relativa alle domande di autorizzazioni singole all'esportazione presentate dalla società Crypto International AG. Il Consiglio federale ha mantenuto questa decisione anche il 26 agosto 2020, dopo una richiesta di riesame della suddetta società.

Il 7 ottobre 2020 la DelCG ha trasmesso al Consiglio federale, per parere, la bozza di rapporto sulla propria ispezione. Il Consiglio federale ha fatto pervenire il suo parere del 28 ottobre 2020 alla DelCG con il relativo controllo dei fatti. Il 10 novembre 2020 è stato pubblicato il rapporto definitivo della DelCG sul caso Crypto AG.

2 Parere del Consiglio federale

2.1 In generale

Come descritto in precedenza, vari dipartimenti e il Consiglio federale si sono occupati intensamente del caso Crypto AG. Il Consiglio federale respinge pertanto la critica della DelCG, secondo cui esso non ha riconosciuto la «portata politica» della situazione. Le informazioni immediate fornite dal DDPS al Consiglio federale, l'esame approfondito di quest'ultimo, l'istituzione di un gruppo di lavoro interdipartimentale e il mandato conferito a Niklaus Oberholzer provano che il caso è stato preso sul serio e che il Consiglio federale ha voluto decisamente fare chiarezza. Ciò gli era stato riconosciuto dalla Delegazione nella lettera inviatagli il 14 febbraio 2020, prima di decidere, una settimana dopo, ossia il 21 febbraio 2020, di revocare l'autorizzazione all'inchiesta e di assumersi tutti gli accertamenti sul caso Crypto AG.

Il Consiglio federale capisce l'intenzione della DelCG di svolgere l'inchiesta sotto un'unica direzione e la considera appropriata da un punto di vista metodologico e materiale. Le risulta però difficile comprendere le ragioni dell'inversione di tendenza da una settimana all'altra nel febbraio 2020.

Sul caso Crypto AG sono stati redatti due rapporti: quello della DelCG del 2 novembre 2020 e uno, classificato segreto, redatto da Niklaus Oberholzer su incarico di

quest'ultima. In virtù dell'obbligo di mantenere il segreto, la Delegazione non ha voluto sottoporre il rapporto Oberholzer all'intero Consiglio federale. Gli ha proposto di garantire l'accesso al rapporto per analogia con la procedura di consultazione di cui all'articolo 167 capoverso 3 LParl, ovvero alla consigliera federale competente per il SIC. Con lettera del 6 novembre 2020, il Consiglio federale ha informato la Delegazione di rinunciare a prendere visione del rapporto Oberholzer, classificato segreto, se non avessero potuto farlo anche tutti gli altri membri del Consiglio federale, il cancelliere federale e il direttore del SIC. Il Consiglio federale ritiene infatti che la procedura offerta dalla DelCG renda impossibile esprimere un parere circostanziato sull'insieme delle conclusioni della Delegazione (rapporto della DelCG e rapporto Oberholzer). In questa sede esso si limita quindi a pronunciarsi sul rapporto di quest'ultima.

2.2 In merito agli aspetti legati alle attività informative

Per quanto riguarda la parte del caso Crypto AG propriamente riguardante l'intelligence, il Consiglio federale constata che secondo la valutazione della DelCG l'attività dei servizi di informazione SIS e SIC era legale, innanzitutto in virtù della legge militare (LM, RS *510.10*) e quindi in virtù della legge sulle attività informative (LAIn, RS *121*). Il Consiglio federale concorda con la valutazione della Delegazione, secondo cui l'acquisizione di informazioni connessa a tale attività nel corso degli anni ha dimostrato di essere utile all'intelligence. Nel valutare la «portata politica», occorre tenere conto di tale valutazione quanto alla dimensione informativa.

Risulta problematico il fatto che, come illustrato dalla DelCG, gli esistenti accessi alle informazioni della Crypto AG nella direzione dell'allora SIS siano stati un segreto ben custodito. Essi sono rimasti riservati a questa ristretta cerchia di persone. Di conseguenza, anche ai tempi del SIC a lungo la direzione politica non è stata informata. Si deve infine constatare che dal 1993 la stessa DelCG non è mai stata messa al corrente dal Servizio informazioni in merito all'operazione e che pertanto non ne era a conoscenza fino a quando, nel novembre 2019, il capo del DDPS l'ha informata. Il Consiglio federale condivide l'opinione della Delegazione secondo cui, nel caso in questione, ci sarebbe dovuta essere un'informazione da parte del Servizio informazioni.

Dopo avere ricevuto informazioni confermate sul caso dal direttore in carica del SIC, il capo del DDPS ne ha informato il Consiglio federale e gli organi di vigilanza (DelCG e AVI-AIn). Per il resto, il collegio governativo ritiene che la valutazione dei fatti da parte della Delegazione non sia stata svolta in modo equiparabile. Secondo il Consiglio federale, il rapporto della DelCG avrebbe dovuto valutare subito tutti i direttori che erano a conoscenza dell'operazione e non ne avevano informato la direzione politica.

Dal punto di vista giuridico, per la Delegazione è assolutamente ammissibile che il SIC e un servizio estero si avvalgano congiuntamente di un'impresa con sede in Svizzera per procurarsi informazioni concernenti l'estero. In un siffatto caso, il Consiglio federale condivide la valutazione della DelCG secondo cui le autorità politiche devono essere informate dal Servizio informazioni così da poter valutare possibili im-

plicazioni in termini di politica di sicurezza, politica estera o politica economica. Riguardo alla questione se il caso Crypto AG era problematico quanto al diritto della neutralità, nel suo parere del 17 febbraio 2021 sull'interpellanza 20.4456 Molina il Consiglio federale afferma: «L'articolo 9 della Convenzione dell'Aia del 1907 non è applicabile a questa fattispecie, poiché quest'ultima non rientra nel campo di applicazione delle misure restrittive o proibitive concernenti i belligeranti. Quindi, il Consiglio federale non ravvisa in questo caso nessuna violazione della Convenzione dell'Aia».

Il Consiglio federale constata inoltre che il caso Crypto AG non ha pregiudicato la politica estera della Svizzera né la sua credibilità. Non vi è stata praticamente nessuna reazione da parte di Stati terzi nei confronti del nostro Paese a seguito della rivelazione del caso sui media.

2.3 In merito alle autorizzazioni all'esportazione

Il Consiglio federale contesta l'accusa di tattica dilatoria e l'intenzione attribuitagli di volere evitare la pubblicazione nei media di notizie negative.

A conoscenza di cifrature possibilmente manipolate degli apparecchi della Crypto AG, quale misura immediata il capo del DEFR ha ordinato la revoca della licenza generale di esportazione. La revoca del 20 dicembre 2019 da parte della SECO ha impedito che vi fossero esportazioni senza controlli preliminari. Era tuttavia possibile continuare a presentare le domande di autorizzazioni singole all'esportazione.

A ogni momento la SECO sarebbe stata disposta a emanare in tempi molto brevi, su relativa richiesta, una decisione impugnabile. Mai le società colpite dall'ordine di revoca e patrocinate da un avvocato hanno chiesto che fosse emanata una siffatta decisione. Come mostrano anche i reclami presentati al Tribunale amministrativo federale contro la procedura di sospensione delle domande d'esportazione aperta dalla SECO, esse hanno senz'altro esaminato la possibilità di avvalersi di rimedi giuridici.

Il Consiglio federale non condivide il parere della DelCG secondo cui la revoca della licenza generale di esportazione è stata illegittima. Non sussiste alcun diritto al rilascio di una siffatta autorizzazione che, come rileva anche la Delegazione, può essere rilasciata se sono soddisfatti i requisiti della legge sul controllo dei beni a duplice impiego (LBDI; RS *946.202*) e della relativa ordinanza (OBDI; RS *946.202.1*). L'articolo 7 capoverso 2 LBDI prevede che un'autorizzazione può essere revocata se le condizioni e gli oneri ad essa connessi non sono rispettati. Nel caso oggetto del presente parere, la revoca non si limita ai motivi di rifiuto delle autorizzazioni menzionati nell'articolo 6 LBDI.

All'epoca il DEFR e la SECO disponevano di informazioni tali da suscitare seri dubbi circa la prova di un controllo attendibile, all'interno dell'azienda, del rispetto delle prescrizioni in materia di controlli delle esportazioni, come richiesto dall'articolo 5 capoverso 2 OBDI. A quel momento non è stato di conseguenza né arbitrario né illegittimo revocare le autorizzazioni generali di esportazione sulla base delle circostanze rivelate al DEFR. Tale procedura era tanto più giustificata dal fatto che il rilascio di autorizzazioni singole d'esportazione continuava a essere possibile, senza il quale anzi

non era possibile un controllo delle merci da esportare. La sospensione da parte del Consiglio federale di questo tipo di autorizzazioni fino alla conclusione dell'inchiesta penale del MPC è stato l'ultimo passo in una procedura di autorizzazione nella quale in precedenza già nel gruppo di controllo delle esportazioni interdipartimentale erano state formulate riserve in occasione dell'esame delle domande di autorizzazioni singole all'esportazione.

Ai sensi degli articoli 12 e 13 OBDI, il rilascio delle autorizzazioni generali di esportazione è di esclusiva competenza della SECO. L'accusa del mancato coinvolgimento del gruppo di controllo delle esportazioni interdipartimentale è pertanto infondata.

2.4 In merito alla denuncia

La SECO non ha sporto denuncia con leggerezza ma, laddove possibile, ha preventivamente proceduto a opportuni accertamenti e raccolto informazioni.

L'accusa che la denuncia sia stata sporta per motivi politici è infondata. A causa delle circostanze di fatto, la SECO è stata obbligata, per legge, a denunciare gli elementi di sospetto per possibili atti perseguibili a norma del codice penale presso il Ministero pubblico della Confederazione. In effetti, la denuncia penale è stata presentata basandosi sul sospetto che le domande presentate per l'esportazione di apparecchi di cifratura contenessero informazioni inesatte, soddisfacendo così la fattispecie penale di cui all'articolo 14 capoverso 1 lettera c LBDI. Nella denuncia è poi stata fatta valere una possibile infrazione ai sensi dell'articolo 9 capoverso 1 lettera a dell'ordinanza del 13 maggio 2015 sull'esportazione e la mediazione di beni per la sorveglianza di Internet e delle comunicazioni mobili (OICoM; RS *946.202.3*) a causa di informazioni inesatte o incomplete contenute nelle domande di esportazione.

Dopo avere ricevuto e verificato la denuncia della SECO, su ordine del MPC la Polizia giudiziaria federale (PGF) ha sequestrato circa 400 apparecchi della Crypto International AG e della TCG Legacy. Nella sua richiesta di autorizzazione al Consiglio federale il MPC ha inoltre dichiarato che vi era motivo sufficiente di sospettare un delitto o un crimine ai sensi dell'articolo 14 LBDI e dell'articolo 9 OICoM. Con le misure di salvaguardia, il MPC non soltanto ha condiviso il sospetto della SECO, ma nella richiesta di autorizzazione ha riconosciuto il sufficiente indizio di reato. In questo modo si confuta anche l'accusa secondo la quale la denuncia da parte della SECO è avvenuta a torto.

Inoltre, il MPC ha ripetuto il sospetto di atti perseguibili a norma del codice penale nelle considerazioni relative al decreto d'abbandono. Nella valutazione giuridica del decreto, il MPC ha affermato di ritenere che negli apparecchi esportati dalla Crypto AG fossero state inserite falle, che la cifratura delle comunicazioni straniere avrebbe potuto essere violata da servizi segreti che ne erano a conoscenza e che l'utilità per l'intelligence degli apparecchi di cifratura esportati fosse parte di una cooperazione del SIS e del successivo SIC con servizi segreti stranieri. A tal fine, a partire dal 2002 vi sarebbero state sufficienti basi legali e la cooperazione si sarebbe svolta entro il quadro giuridico.

In nessun momento il DEFR e la SECO disponevano di informazioni che consentissero loro di verificare gli elementi di sospetto addotti quanto a eventuali motivi giustificativi giuridicamente rilevanti.

3 Osservazioni sulle raccomandazioni

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

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.

Il Consiglio federale non è d'accordo con la raccomandazione.

La condotta politica nei confronti del SIC da parte del DDPS e del Consiglio federale è chiaramente disciplinata in numerose basi legali (cfr. segnatamente gli art. 70 e 80 LAIn). In virtù dell'articolo 19 dell'ordinanza sulle attività informative (OAIn; RS *121.1*) il SIC deve presentare «annualmente al capo del DDPS un rapporto su tutte le operazioni e tutte le fonti umane». Conformemente a tale disposizione il SIC avrebbe dovuto imperativamente informare il DDPS sulle sue attività in relazione con la Crypto AG, implicanti una collaborazione con un servizio partner estero.

Il controllo del servizio informazioni da parte del capo del DDPS comprende anche sedute mensili di direzione con la direzione del SIC. Dal gennaio 2014 tali colloqui sono messi a verbale. Tutti i relativi verbali sono stati trasmessi alla DelCG ai fini della sua inchiesta. Le attività operative del SIC sono regolarmente tematizzate in occasione delle sedute.

Nel caso della Crypto AG il problema non è sorto a causa di lacune negli strumenti di controllo a livello di DDPS o di Consiglio federale, ma è stato cagionato dall'intenzione di collaboratori del SIS e, successivamente, del SIC di mantenere segreta l'operazione e di sottrarla al controllo politico. Si è trattato di un'operazione pluriennale di cui non era facile valutare le circostanze e le possibili conseguenze.

In una simile situazione sarebbe una misura ragionevole una verifica da parte dell'AVI-AIn. L'AVI-AIn è un organo di controllo indipendente, ma il DDPS può senz'altro proporle di avviare un'ispezione specifica. Nel caso della Crypto AG ad esempio, l'AVI-AIn ha eseguito, con il previo consenso della DelCG, una verifica non annunciata degli archivi del SIC.

Per contro la DelCG ha respinto l'ispezione proposta dal DDPS all'AVI-AIn in merito alla legalità dell'attività operativa del SIC in collaborazione con il Centro operazioni

elettroniche (COE). Il Consiglio federale non condivide la valutazione della DelCG al riguardo. Il ricorso all'AVI-AIn in tale ambito sarebbe stato ragionevole poiché corrispondente, tra l'altro, al mandato legale dell'autorità di vigilanza (cfr. art. 78 cpv. 1 LAIn); l'AVI-AIn, inoltre, si era detta disposta a integrare tale verifica nella sua pianificazione annuale per il 2020.

In merito a un'eventuale verifica in tal senso da parte dell'AVI-AIn, la DelCG fa valere che il DDPS avrebbe dovuto chiedere una relativa autorizzazione della Delegazione, conformemente all'articolo 154*a* capoverso 1 LParl. Tale disposizione, tuttavia, concerne esplicitamente solo inchieste disciplinari o amministrative. È dubbio che una verifica da parte dell'AVI-AIn rientri in tali categorie.

Nel gennaio 2021 la SG-DDPS ha potenziato il personale addetto alla consulenza in materia di intelligence a favore del capo del DDPS. Tale misura non è dovuta all'elaborazione del caso Crypto AG, ma è stata adottata in relazione con le esperienze maturate negli anni precedenti e con i compiti supplementari risultanti dall'entrata in vigore della LAIn, concernenti soprattutto la valutazione e l'approvazione delle nuove misure di acquisizione del SIC soggette ad autorizzazione.

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.

Il Consiglio federale considera questa raccomandazione come già messa in atto.

La Delegazione Sicurezza del Consiglio federale (DelSic) tratta regolarmente e approfonditamente questioni inerenti ai servizi informazioni. Le tematiche relative all'intelligence rappresentano una parte importante degli affari trattati dalla DelSic. Ciò risulta dagli ordini del giorno e dai verbali della DelSic, trasmessi anche alla DelCG.

Il Consiglio federale non condivide il parere secondo cui un ulteriore organo *ad hoc* sarebbe utile alla sua capacità di condotta. Nel caso Crypto AG il problema principale non è rappresentato da una presunta mancata informazione del Consiglio federale da parte del DDPS, ma è dovuto al fatto che sino al 2019 il Servizio informazioni non ha informato gli organi di direzione politici e le autorità di vigilanza. L'accesso del Servizio informazioni a informazioni della Crypto AG era un segreto ben custodito in seno alla direzione dell'ex SIS ed era noto unicamente a tale ristretta cerchia di persone. L'istituzione di ulteriori organi a livello di Amministrazione o di Consiglio federale non migliorerebbe alcunché segnatamente in una situazione di tal genere.

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.

Il Consiglio federale è parzialmente d'accordo con la raccomandazione.

La DelSic è un organo del Consiglio federale e, pertanto, un organo politico. Si compone dei capi del DDPS, del DFAE e del DFGP ed è diretta dal capo del DDPS. I tre membri della DelSic possono partecipare alle sedute accompagnati da collaboratori dell'Amministrazione federale operanti nei rispettivi dipartimenti. Di regola si tratta dei segretari generali e di collaboratori del Comitato ristretto Sicurezza, che prepara numerosi affari della DelSic. A seconda delle tematiche trattate, i membri della DelSic possono ricorrere per le loro sedute a ulteriori persone, ciò che è regolarmente il caso. Per tematiche concernenti l'esercito può essere fatto ricorso anche al capo dell'esercito (CEs). Una partecipazione permanente del CEs alle sedute della DelSic non sarebbe tuttavia opportuna poiché le tematiche inerenti all'esercito costituiscono un'eccezione.

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.

Il Consiglio federale è parzialmente d'accordo con la raccomandazione.

Dal punto di vista del Consiglio federale la raccomandazione della DelCG va nella giusta direzione. Il Consiglio federale ritiene che l'obbligo di informare e la riserva di decisione riguardo ad attività di intelligence non debbano essere limitati a casi concernenti aziende svizzere e nel cui ambito il servizio informazioni collabora con partner esteri. Anche altre attività di intelligence possono rivestire notevole importanza sul piano politico. Affinché gli organi di direzione politica possano esercitare la loro funzione di condotta e di vigilanza è decisivo che il servizio informazioni avvii un'informazione, per la via di servizio, tempestiva e conforme ai vari livelli. Il fattore determinante per l'avvio dell'informazione deve pertanto essere rappresentato dalla possibile dimensione politica di un fatto. Il coinvolgimento di un'azienda svizzera può fungere da indicatore in tal senso, ma non può costituire l'unico criterio per l'avvio di un'informazione. I casi di semplice coinvolgimento di aziende svizzere, ad esempio nell'ambito di flussi di pagamento usuali in ambito commerciale, o l'osservazione coordinata a livello internazionale di possibili attività di proliferazione ad opera di aziende svizzere rientrano tra i compiti standard di un servizio di intelligence. Dovrebbero essere trattati a livello governativo soltanto nei casi in cui comportino notevoli opportunità o rischi sul piano politico.

Il DDPS informa il Consiglio federale già allo stato attuale in merito a importanti attività o riscontri di intelligence. Il Consiglio federale desidera pertanto accogliere la raccomandazione in via generale e stabilire i criteri atti a determinare le attività di intelligence sulle quali intende essere informato dal DDPS e i casi in cui intende autorizzare esso stesso simili attività. Tali criteri possono essere elaborati e ancorati a livello di legge nel quadro della revisione della LAIn o dell'OAIn.

Nel quadro della LAIn non è tuttavia prevista alcuna competenza decisionale del Consiglio federale riguardo agli aspetti operativi delle attività di intelligence. Nell'articolo 70 LAIn sono disciplinate in primo luogo la direzione politica e la vigilanza del Consiglio federale. All'articolo 70 capoverso 1 lettera e LAIn è previsto tuttavia che il Consiglio federale «ordina le misure necessarie in caso di situazioni di minaccia particolari». All'articolo 12*a* della legge sull'organizzazione del Governo e dell'Amministrazione (LOGA; RS *172.010*) è inoltre stabilito che i dipartimenti «informano regolarmente il Consiglio federale sui loro affari e in particolare sui rischi e gli eventuali problemi connessi» e che il Consiglio federale può esigere che i suoi membri gli forniscano determinate informazioni. Nell'articolo 38 LOGA è sancito il diritto dei capi dei dipartimenti di intervenire personalmente nelle decisioni delle unità amministrative subordinate. L'articolo 13 LOGA, pur costituendo in primo luogo una prescrizione procedurale, menziona che il Consiglio federale prende «decisioni sugli affari preponderanti o di rilevanza politica». Le regolamentazioni vigenti consentono pertanto già allo stato attuale al Consiglio federale di adottare decisioni in merito ad attività di intelligence di rilevanza politica.

Il Consiglio federale condivide il parere della DelCG secondo cui il Servizio informazioni deve informare i responsabili politici in merito a fatti la cui portata è paragonabile a quella del caso Crypto AG. Negli scorsi dieci anni l'informazione da parte del SIC in merito alle operazioni di intelligence è stata sistematizzata e ampliata. Le attività concernenti la Crypto AG non sono tuttavia mai confluite in tali resoconti. Ciò è dovuto al fatto esposto più sopra che l'accesso alle informazioni concernenti la Crypto AG era un segreto ben custodito da una cerchia ristretta di persone in seno alla direzione del SIS nonché, successivamente, del SIC ed era noto esclusivamente a tale ristretta cerchia di persone.

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.

Il Consiglio federale sta mettendo in atto la raccomandazione nei limiti del possibile.

Valutazione generale da un punto di vista pratico

L'Amministrazione federale impiega soluzioni di cifratura in innumerevoli ambiti – ad esempio nel quadro dell'impiego di telefoni cellulari per scopi aziendali (iPhone). Non è possibile sottoporre a relativi controlli l'azienda produttrice Apple. Quanto auspicato nella raccomandazione non può essere realizzato totalmente già soltanto per questo motivo. A ciò si aggiunge che tutte le soluzioni di cifratura impiegate attual-

mente per i livelli di classificazione AD USO INTERNO e CONFIDENZIALE provengono da fornitori esteri. Inoltre, la messa in atto della raccomandazione è problematica nel settore dell'interoperabilità. L'interoperabilità delle attuali cifrature multistrato, ampiamente utilizzate, non è compatibile con quanto auspicato nella raccomandazione. Per di più, soluzioni di cifratura proprietaria prodotte in Svizzera non comportano praticamente alcun vantaggio rispetto alle soluzioni di cifratura *open source*. Per ambedue le soluzioni è necessario convalidare che la tecnologia di cifratura in questione è stata implementata in modo ottimale. In complesso, la raccomandazione pare pertanto poco realizzabile a livello pratico. Le soluzioni di cifratura sono attualmente presenti in una moltitudine di sistemi e componenti. Nella prassi non potrebbe più essere acquistato alcun software all'estero.

Se per contro la raccomandazione dovesse avere per oggetto posti chiave, ad esempio, del DFGP (p. es. nel settore della criminalità organizzata), del DFAE (per la rete esterna) o del DDPS (segnatamente per il SIC), quanto auspicato nella raccomandazione sarebbe in gran parte attuabile.

Va tuttavia osservato che neanche i produttori svizzeri possono garantire totalmente che tutti gli aspetti legati alla sicurezza dello sviluppo e della produzione siano sotto il loro controllo. Ciononostante le aziende svizzere offrono chiari vantaggi rispetto ad aziende estere, ad esempio per quanto concerne la necessaria dichiarazione di sicurezza aziendale o il controllo di sicurezza relativo alle persone. Tali vantaggi sussistono soprattutto nel quadro di una collaborazione pluriennale.

Infine, in Svizzera vi sono fornitori interessanti, tra l'altro per armasuisse, che gestiscono filiali anche in altri Paesi. In alcuni Stati sono in vigore leggi che obbligano i produttori a cooperare con organi statali (p. es. il Patriot act negli Stati Uniti o leggi analoghe in Cina e in Francia). Di conseguenza la collaborazione con aziende svizzere che dispongono di filiali all'estero potrebbe essere altrettanto problematica sotto il profilo della politica di sicurezza.

Valutazione sotto il profilo giuridico

La raccomandazione può essere messa in atto in conformità con la legislazione in materia di acquisti pubblici. Nel quadro della legge federale del 21 giugno 2019 sugli appalti pubblici, più precisamente in virtù della sua revisione entrata in vigore il 1° gennaio 2021 (LAPub; RS *172.056.1*), è previsto che la legislazione in materia di acquisti pubblici non si applica a commesse pubbliche se «ciò è ritenuto necessario per la tutela e il mantenimento della sicurezza esterna o interna o dell'ordine pubblico» (art. 10 cpv. 4 lett. a LAPub). Per l'acquisto di soluzioni di cifratura la Confederazione è pertanto autorizzata ad assegnare in qualsiasi momento e mediante trattativa privata commesse in Svizzera.

Per contro, la Confederazione non può esercitare alcun influsso sull'offerta dei fornitori di servizi. Attualmente esiste soltanto un'azienda in mani svizzere che offre soluzioni di cifratura. Tuttavia, se la Confederazione ricorre a un unico fornitore per un acquisto, tale fornitore acquisisce una posizione di monopolio. Per un simile caso la legislazione in materia di acquisti pubblici prevede appositi strumenti di controllo, tra cui, ad esempio, accordi sul diritto di consultare la contabilità aziendale e di svolgere audit. Non va tuttavia dimenticato che una situazione di monopolio comporta anche

l'assunzione del rischio che l'azienda fallisca e sia oggetto di conseguenti procedimenti esecutivi o che l'azienda sia economicamente distrutta e che il relativo know-how vada perso. A ciò si aggiunge che la vendita di partecipazioni e un eventuale passaggio di proprietà di un'azienda in mani straniere non possono essere impediti per contratto.

Per mettere in atto la raccomandazione si dovrebbe pertanto far sì che l'azienda mantenga un legame con la Confederazione al di fuori dell'ambito ristretto della prestazione contrattuale. Parimenti, nel quadro di contratti di lavoro e in materia di servizi e nell'ambito di progetti di ricerca andrebbe fatto in modo che il potere di disporre dei beni immateriali rimanga in mano alla Confederazione. Come noto, tra gli strumenti utili a tal fine figurano tra l'altro progetti PPP[2], contratti di cooperazione, progetti di ricerca e sviluppo congiunti. Considerate le esperienze maturate sinora, va tuttavia messo in conto che simili misure rendono di regola più oneroso un acquisto. D'altro canto, tali misure consentono di ridurre la dipendenza economica della Confederazione da una simile azienda.

Aspetti di politica di sicurezza

Oltre agli aspetti giuridici e pratici vanno considerate anche le implicazioni a livello di politica di sicurezza, soprattutto per quanto concerne la base tecnologica e industriale rilevante in materia di sicurezza.

Al riguardo il settore Scienza e tecnologia di armasuisse ha allestito un elenco delle tecnologie determinanti in materia di politica di sicurezza[3], in cui la crittologia figura tra le «tecnologie chiave determinanti in materia di politica di sicurezza». La crittologia rappresenta una tecnologia chiave per il nostro Paese e per il mondo intero. Nella realtà odierna, caratterizzata dalla capillare interconnessione digitale, praticamente tutti i meccanismi elettronici di sicurezza sono basati su procedure di crittografia. L'e-banking, l'e-commerce, l'e-government come qualsiasi altro servizio elettronico sarebbero impensabili senza il ricorso alla crittografia. Nel corso della progressiva digitalizzazione la crittografia assumerà una sempre maggiore importanza per l'economia, la società e le autorità. Nei principi da esso definiti in materia di politica d'armamento del DDPS, il Consiglio federale ha preso atto della necessità di rafforzare, in seno alla base tecnologica e industriale svizzera rilevante in materia di sicurezza, le competenze tecnologiche e le capacità industriali chiave determinanti in materia di politica di sicurezza.

Tale esigenza è illustrata anche nel rapporto della DelCG, a conferma del parere del Consiglio federale. Attualmente le pertinenti competenze tecnologiche in Svizzera sono disponibili in particolare presso il settore Sicurezza dell'informazione/Crittologia (SI Critt) della Base d'aiuto alla condotta dell'esercito nonché in seno al settore Scienza e tecnologia di armasuisse. L'acquisto sicuro di sistemi di cifratura rientra nella sfera di competenza di armasuisse. Oltre alle competenze disponibili in seno alla Confederazione sono tuttavia necessari anche partner industriali altamente qualificati.

2 Public private partnership (PPP).
3 L'elenco comprende 213 tecnologie, priorizzate secondo le necessità dell'esercito. Le tecnologie a cui è stato assegnato il massimo livello di priorità sono considerate tecnologie chiave determinanti in materia di politica di sicurezza.

Se questi ultimi si trovano all'estero, non è praticamente possibile esercitare alcun influsso sullo sviluppo degli apparecchi. Il caso Crypto AG illustra in maniera esemplare a quali rischi e conseguenze si espongono gli Stati che per tali sistemi devono ricorrere a offerenti all'estero.

Alla luce di quanto esposto occorrerebbe analizzare in maniera più approfondita le possibilità offerte dalla legge federale concernente le imprese d'armamento della Confederazione (LIAC; RS *934.21*), ad esempio le possibilità di partecipazione ad aziende. Ciò potrebbe condurre a soluzioni praticabili e flessibili per i problemi di sicurezza tematizzati dalla DelCG.

Avendo riconosciuto l'importanza delle summenzionate competenze tecnologiche e capacità industriali, nei suoi Principi del 24 ottobre 2018 in materia di politica d'armamento del DDPS il Consiglio federale ha ribadito la sua intenzione di mantenere e rafforzare, in seno alla base tecnologica e industriale rilevante in materia di sicurezza, in particolare le competenze tecnologiche e le capacità industriali chiave determinanti in materia di politica di sicurezza.

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.

Questa raccomandazione viene messa in atto.

Visti gli imminenti sviluppi tecnologici e le sfide legate alla digitalizzazione nonché le crescenti esigenze in materia di sicurezza, si renderà necessario un ampliamento delle competenze specialistiche in materia di crittologia. Per garantire le necessarie competenze occorrerà promuovere delle forme di partenariato e di collaborazione idonee, senza perdere di vista soluzioni sostenibili sul piano economico.

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.

Questa raccomandazione viene messa in atto.

Affinché la crittoanalisi possa tenere il passo con questi cambiamenti, da un lato sono necessari accessi a punti deboli, sia per poterli comprendere che per poterli poi sfruttare anche a livello di attività informative, dall'altro occorre uno scambio con altri servizi specializzati.

In tal senso lo scambio con altri servizi delle attività informative assume un'importanza particolare. Secondo l'articolo 12 capoverso 3 LAIn, la collaborazione con servizi delle attività informative esteri per l'esecuzione della LAIn (e quindi anche dell'esplorazione radio e dei segnali via cavo) compete al SIC. Esso definisce perciò

annualmente, d'intesa con il COE, la sua strategia relativa ai servizi partner e quindi anche quella in materia di crittologia. La strategia definisce con quali servizi partner e in merito a quali ambiti tematici il COE e il settore Crittologia procedono a uno scambio regolare sul piano specialistico. Il SIC fa in modo di rendere possibili, mantenere e rafforzare in futuro i necessari contatti con i servizi partner.

In questa sede si vuole inoltre richiamare l'attenzione sul fatto che le competenze crittografiche e crittoanalitiche vanno considerate in modo complessivo poiché sono a rischio anche soluzioni teoricamente invulnerabili.

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.

Il Consiglio federale considera questa raccomandazione come già messa in atto. La SG-DDPS presenterà alla DelCG un resoconto relativo alla realizzazione.

La SG-DDPS tiene e documenta i suoi atti conformemente alla legge sull'archiviazione (LAr; RS *152.1*) in modo sistematico nel sistema di gestione degli affari Acta Nova. Secondo le prescrizioni organizzative concernenti la gestione delle informazioni in seno alla SG-DDPS, il Centro di competenza GEVER (CC GEVER SG-DDPS) verifica ogni anno nella Registratura della SG-DDPS, assieme ai competenti settori della SG-DDPS, se sia possibile eliminare determinati atti.

Gli atti per i quali viene definito o è stato definito un valore archivistico vengono consegnati all'Archivio federale (AFS). La consegna ha luogo in forma elettronica mediante il processo d'archiviazione standardizzato dell'AFS. I manoscritti dei massimi livelli della Direzione del Dipartimento sono messi a disposizione per l'archiviazione secondo le raccomandazioni dell'AFS (Promemoria «Documenti di lavoro personali e archivi privati dei magistrati della Confederazione») di regola al termine del mandato. A tale riguardo non occorrono istruzioni supplementari.

Da gennaio 2014 i colloqui regolari tra il capo del DDPS e il direttore del SIC sono messi a verbale (cfr. sopra il parere relativo alla raccomandazione 1). Tali documenti vengono trattati secondo le prescrizioni summenzionate.

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.

Il Consiglio federale è d'accordo con la raccomandazione. La relativa messa in atto solleva tuttavia alcune questioni che occorre chiarire.

Dopo la pubblicazione della raccomandazione della DelCG, il SIC ha sospeso la consegna convenuta con l'AFS per febbraio 2021 di atti operativi delle organizzazioni precedenti al SIC, tra cui figurano segnatamente gli atti «Crypto», per non eludere la messa in atto della raccomandazione.

Conformemente all'articolo 6 LAr, l'Amministrazione federale offre all'Archivio federale di riprendere tutti i documenti dei quali non ha più bisogno in modo permanente, ovvero che non tratta più regolarmente. Sono possibili eccezioni, se l'unità amministrativa è essa stessa competente per la relativa archiviazione. Il SIC archivia tuttavia i suoi documenti nell'AFS secondo la LAr, come viene confermato nell'articolo 68 LAInf.

Il diritto in materia di archiviazione limita l'accesso dei servizi mittenti ai documenti archiviati contenenti dati personali. I servizi mittenti possono consultare documenti durante il termine di protezione soltanto se ne hanno bisogno quali mezzi di prova, vale a dire nell'ambito di un procedimento giudiziario, a fini legislativi o giurisprudenziali, a fini statistici o per una decisione in merito alla concessione, alla limitazione o al rifiuto del diritto alla consultazione o all'informazione delle persone interessate (art. 14 cpv. 2 LAr). L'articolo 68 capoverso 3 LAIn conferisce inoltre al SIC il diritto di consultazione al fine di valutare minacce concrete per la sicurezza interna o esterna oppure per tutelare un altro interesse pubblico preponderante. L'accesso all'archivio del SIC è perciò garantito, tuttavia soltanto mediante gli strumenti esistenti dell'AFS.

La raccomandazione presuppone che il SIC elabori delle nuove panoramiche dei contenuti relative agli atti da consegnare e le conservi al fine di poter determinare rapidamente se ha archiviato documenti relativi a determinate fattispecie o persone. Fintantoché vengono utilizzate in modo permanente, tali panoramiche possono essere conservate più a lungo presso il SIC rispetto ai documenti ai quali si riferiscono. Se viene attribuito loro un valore archivistico, anche tali panoramiche dovranno essere archiviate in una fase successiva. Un simile modo di procedere è pertanto possibile, solleva tuttavia determinate questioni p. es. per quanto riguarda i diritti alla consultazione. Il SIC chiarirà tali questioni con l'AFS.

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.

Questa raccomandazione viene a cadere.

Con decisione dell'8 dicembre 2020, il MPC ha abbandonato la procedura penale aperta per infrazione alla legge sul controllo dei beni a duplice impiego (art. 14 LBDI) nonché per infrazione all'articolo 9 OICoM (art. 319 cpv. 1 lett. b e c del Codice di procedura penale [CPP; RS *312.0*]).

Il 29 dicembre 2020 il Consiglio federale ha preso atto della decisione di abbandono del MPC incaricando la SECO di riesaminare e autorizzare quelle domande che erano oggetto della decisione del 19 giugno 2020 del Consiglio federale, a condizione che fossero soddisfatti i presupposti giuridici. Il 30 dicembre 2020 la SECO ha autorizzato tutte le domande pendenti delle ditte subentrate alla Crypto AG (sia quelle sospese a seguito della decisione del 19 giugno 2020 del Consiglio federale che quelle rimanenti), emettendo il giorno successivo delle nuove autorizzazioni generali d'esportazione.

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.

Questa raccomandazione viene messa in atto.

La Cancelleria federale esaminerà assieme al segretariato della DelCG in che modo mettere in atto in particolare l'esigenza legata alle «Questioni relative agli affari in corso della DelCG». Successivamente il Consiglio federale sottoporrà una proposta alla DelCG per la procedura da adottare.

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.

Il Consiglio federale ritiene problematica questa raccomandazione sia giuridicamente che materialmente, per cui la respinge.

Ha comprensione che la DelCG si preoccupi del fatto che le inchieste da lei condotte potrebbero essere rese difficoltose o subire ritardi e che delle autorità federali sporgano denunce penali in riferimento a procedure o persone che sono oggetto di tali inchieste. Anche se le inchieste penali condotte da autorità di perseguimento penale cantonali o federali da un lato e l'esercizio dei compiti di sorveglianza da parte della DelCG dall'altro non si prefiggono necessariamente i medesimi obiettivi (a tale riguardo vedi anche l'art. 154*a* cpv. 4 LParl secondo cui un'inchiesta della Delegazione delle Commissioni della gestione non impedisce l'esecuzione di procedimenti giudiziari civili e amministrativi né di istruzioni e procedimenti giudiziari in materia penale) e quindi non devono essere armonizzati sul piano temporale, è anche nell'interesse del Consiglio federale che i procedimenti non abbiano un influsso svantaggioso reciproco.

Il Consiglio federale è tuttavia anche del parere che un processo di consultazione istituzionalizzato e, se del caso, addirittura prescritto per legge come è formulato nella prima frase della raccomandazione 12 non sia né necessario né opportuno e questo per i seguenti motivi.

- Le procedure relative alla Crypto AG sono uniche nel loro genere. Il Consiglio federale non è a conoscenza di alcun altro caso in cui le autorità della Confederazione abbiano sporto denunce penali che fossero in contrasto con un oggetto specifico d'inchiesta della DelGC sia sul piano del contenuto che su quello temporale. Neanche il rapporto della DelGC indica casi simili a cui occorrerebbe rimediare mediante l'obbligo di consultazione raccomandato. Il Consiglio federale non ritiene pertanto indicato creare una regola procedurale generale sulla base di questo caso isolato.
- Per principio chiunque è autorizzato a sporgere una denuncia penale (art. 301 CPP). Per le autorità federali esistono inoltre obblighi di denuncia previsti da normative specifiche. Infatti diverse leggi federali – tra cui anche la legge sul controllo dei beni a duplice impiego, di particolare interesse in questo caso – prevedono che le autorità della Confederazione preposte al rilascio delle autorizzazioni e al controllo, ma anche gli organi di polizia cantonali e comunali nonché le autorità doganali sono tenuti a denunciare al MPC le infrazioni alla rispettiva legge «che hanno accertato o di cui hanno avuto notizia nell'esercizio delle loro funzioni» (art. 18 cpv. 2 LBDI, ma anche art. 40 cpv. 2 della legge sul materiale bellico [LMB, RS *514.51*], art. 100 cpv. 3 della legge federale sull'energia nucleare [LENu, RS *732.1*] oppure art. 27 cpv. 2 della legge federale sulle prestazioni di sicurezza private fornite all'estero, [LPSP, RS *935.41*]; in modo analogo anche art. 27*a* della legge sull'assicurazione contro i rischi delle esportazioni [LARE, RS *946.10*]). Laddove le autorità federali hanno un obbligo di denuncia, rimane un margine esiguo per un processo di consultazione formale preliminare.
- Il diritto di consultazione richiesto nella raccomandazione in pratica implicherebbe che l'Amministrazione federale debba essere informata in maniera sistematica e precoce dalla DelGC sulle persone e procedure oggetto di inchieste, il che secondo le circostanze potrebbe contravvenire alle esigenze in materia di inchieste della DelGC. Occorrerebbe inoltre chiarire quali informazioni l'autorità federale che intende sporgere denuncia dovrebbe fornire alla DelGC, affinché quest'ultima possa assumere i suoi diritti di consultazione in maniera sensata. Se inoltre fosse necessario agire celermente, questi processi potrebbero andare a detrimento di un perseguimento penale efficiente come pure di un'alta vigilanza efficace esercitata dalla DelGC.

Nella seconda frase della sua raccomandazione 12 la DelGC propone che il competente dipartimento o la CaF – qui si dovrebbe intendere il dipartimento oppure la CaF di cui fa parte l'autorità federale autorizzata o tenuta a sporgere denuncia (unità amministrativa) – in precedenza debba ottenere una presa di posizione dell'autorità di perseguimento penale. Oltre al fatto che simili fasi procedurali supplementari potrebbero rallentare i processi in modo svantaggioso, il Consiglio federale ritiene che un tale coordinamento con le autorità di perseguimento penale non sia auspicato per una questione di principio.

In linea generale il diritto di denuncia sancito dalla legge non soggiace a una riserva secondo cui in precedenza si debba ottenere una presa di posizione dell'autorità di perseguimento penale su se e come questa intenda reagire a una denuncia. Una denuncia penale permette di portare a conoscenza di un'autorità penale un comportamento giudicato perseguibile penalmente. Successivamente l'autorità penale deve esaminare se il comportamento denunciato costituisce effettivamente un reato e se sono dati ulteriori presupposti per un perseguimento penale. Secondo il risultato di questo esame, l'autorità di perseguimento penale ha diverse possibilità: il decreto di non luogo a procedere, tra l'altro se gli elementi costitutivi di reato o i presupposti processuali non sono adempiuti (art. 310 CPP). Può sospendere il procedimento, in particolare se l'esito del procedimento penale dipende da un altro procedimento di cui appare opportuno attendere l'esito (art. 314 cpv. 1 lett. b CPP). Può aprire l'istruzione oppure trasmettere alla polizia, perché compia indagini supplementari, le denunce penali dalle quali non emergano chiaramente indizi di reato (art. 309 cpv. 1 e 2 CPP). Non può e non deve definire già al momento della denuncia penale se e come intende reagire, ancor meno in una fase precedente.

L'obbligo di ottenere una presa di posizione richiesto dalla raccomandazione finirebbe de facto per sfociare in un esame preliminare dei presupposti di un perseguimento penale o per determinare se il perseguimento appaia opportuno, da parte dell'autorità di perseguimento penale stessa. Si tratterebbe di un obbligo finora sconosciuto nella procedura penale svizzera. Anche se un simile esame preliminare potrebbe apparire sensato, solleverebbe numerose questioni successive complesse: come bisognerebbe gestire la preimplicazione peraltro problematica sul piano giuridico delle persone coinvolte, nell'ottica del perseguimento penale se la denuncia penale viene effettivamente sporta in una fase successiva? In che misura il Consiglio federale e l'Amministrazione federale sarebbero legati al parere espresso dall'autorità di perseguimento penale? Infine sorge la domanda su quale funzione svolgerebbe una simile consultazione preliminare in caso di reati perseguibili d'ufficio, che in seguito dovrebbero essere comunque perseguiti dall'autorità di perseguimento penale, indipendentemente da un'eventuale denuncia penale, non foss'altro che in base alle informazioni preliminari fornite dalle autorità federali? Per tutti questi motivi il Consiglio federale non ritiene né necessario né opportuno approfondire l'idea di una simile consultazione preliminare.