Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Centro nazionale per la cibersicurezza (NCSC)

Berna, 12 gennaio 2022

Procedura di consultazione

relativa alla modifica della legge federale del 18 dicembre 2020 sulla sicurezza delle informazioni in seno alla Confederazione (Legge sulla sicurezza delle informazioni, LSIn)

(Introduzione dell'obbligo di notifica di ciberattacchi a infrastrutture critiche)

Rapporto esplicativo

Indice

1 Situazione iniziale 4
1.1 Necessità di agire e obiettivi 4
1.2 Alternative esaminate e opzione scelta 4
1.2.1 Potenziamento dello scambio di informazioni su base volontaria 4
1.2.2 Rapporto con gli altri obblighi di notifica e scambio di informazioni tra le autorità 5
1.2.3 Applicazione dell'obbligo di notifica attraverso incentivi e sanzioni 6
1.3 Rapporto con il programma di legislatura e il piano finanziario, nonché con le strategie del Consiglio federale 7
2 Diritto comparato, in particolare rapporto con il diritto europeo 8
3 Punti essenziali del progetto 9
3.1 La normativa proposta 9
3.2 Compatibilità tra compiti e finanze 9
3.3 Attuazione 9
3.3.1 Necessità di una base legale 9
3.3.2 La LSIn come base giuridica adatta 10
3.3.3 Disposizioni di esecuzione 10
3.3.4 Attuabilità dell'obbligo di notifica 10
4 Commento ai singoli articoli 12
5 Ripercussioni 27
5.1 Ripercussioni per la Confederazione 27
5.2 Ripercussioni per i Cantoni e i Comuni 27
5.3 Ripercussioni sull'economia e sulla società 27
6 Aspetti giuridici 29
6.1 Costituzionalità 29
6.2 Compatibilità con gli impegni internazionali della Svizzera 29
6.3 Forma dell'atto 29
6.4 Subordinazione al freno alle spese 30
6.5 Rispetto del principio di sussidiarietà e del principio dell'equivalenza fiscale 30
6.6 Delega di competenze legislative 30
6.7 Protezione dei dati 30

Compendio

Negli ultimi anni sempre più spesso privati, imprese e autorità sono stati vittime di ciberincidenti che, in alcuni casi, hanno avuto conseguenze gravi. Il presente progetto posto in consultazione prevede l'introduzione dell'obbligo di notifica di ciberattacchi a infrastrutture critiche, grazie al quale sarebbe possibile individuare precocemente i ciberattacchi, analizzare le modalità con cui vengono sferrati e avvisare tempestivamente gli altri gestori di infrastrutture critiche. L'obbligo di notifica permetterebbe dunque di aumentare notevolmente la cibersicurezza in Svizzera.

L'11 dicembre 2020 il Consiglio federale ha incaricato il Dipartimento federale delle finanze (DFF) di elaborare un progetto da porre in consultazione corredato da basi giuridiche per l'introduzione dell'obbligo di notifica di ciberattacchi a infrastrutture critiche.

Il presente progetto prevede che la base legale per l'obbligo di notifica venga introdotta nella legge sulla sicurezza delle informazioni (LSIn) adottata dal Parlamento il 18 dicembre 2020. Oltre all'obbligo di notifica, nella LSIn dovrebbero essere definiti anche i compiti del Centro nazionale per la cibersicurezza (NCSC) e la sua funzione in qualità di servizio centrale di notifica.

A livello di contenuto l'obbligo di notifica riguarderebbe soltanto i ciberattacchi che potenzialmente possono arrecare notevoli danni e verrebbe applicato ai gestori di infrastrutture critiche, ovvero di processi, sistemi e installazioni essenziali per il funzionamento dell'economia e per il benessere della popolazione. La funzione di servizio centrale di notifica verrebbe assunta dal NCSC, che raccoglie anche le segnalazioni volontarie di ciberincidenti e vulnerabilità riscontrate negli strumenti informatici.

Rapporto esplicativo

1 Situazione iniziale

1.1 Necessità di agire e obiettivi

Nel suo rapporto del 13 dicembre 2019 sul postulato 17.3475 «Obbligo di segnalazione di gravi incidenti legati alla sicurezza delle infrastrutture critiche» il nostro Consiglio ha constatato che in Svizzera non esiste un obbligo di segnalazione di ciberincidenti nelle infrastrutture critiche e ha conferito al Centro nazionale per la cibersicurezza (NCSC) il compito di verificare la possibilità di introdurre un obbligo di questo tipo[1].

Questo mandato di verifica trovava fondamento in vari documenti precedenti, tra cui la strategia per la protezione delle infrastrutture critiche (Strategia PIC 2018–2022, misura 2), la strategia per la protezione della Svizzera contro i cyber-rischi (SNPC 2018–2022, misura 9) nonché il rapporto del gruppo di esperti per il futuro del trattamento e della sicurezza dei dati[2]. Inoltre, la questione dell'obbligo di notifica è stata affrontata anche nel corso dei dibattiti parlamentari sulla revisione totale della legge federale sulla protezione della popolazione e sulla protezione civile (LPPC, dibattito del Consiglio nazionale del 14.6.2019) e sull'emanazione della legge sulla sicurezza delle informazioni (LSIn, dibattito del Consiglio nazionale del 4.6.2020). Dopo un'approfondita verifica delle possibili basi legali e, in particolare, della competenza federale[3], il nostro Collegio l'11 dicembre 2020 ha incaricato il DFF di elaborare entro la fine del 2021 un progetto sull'introduzione dell'obbligo di notifica di ciberattacchi a infrastrutture critiche da porre in consultazione.

Lo scopo del progetto era chiarire chi fosse tenuto a segnalare quali tipi di attacchi, quando e a chi. Nel corso delle verifiche effettuate per chiarire questi aspetti si è appurato che il Centro nazionale per la cibersicurezza (NCSC) istituito nel 2019, che nel progetto viene designato come servizio centrale di notifica di ciberattacchi, non disponeva delle basi legali necessarie per assumere i suoi compiti in qualità di centro di competenza della Confederazione per la cibersicurezza così come richiesto dal Parlamento[4]. Attraverso il progetto sull'introduzione dell'obbligo di notifica anche i compiti e le competenze del NCSC dovrebbero quindi essere disciplinati a livello di legge.

1.2 Alternative esaminate e opzione scelta

1.2.1 Potenziamento dello scambio di informazioni su base volontaria

In Svizzera lo scambio di informazioni tra infrastrutture critiche e Confederazione è ben consolidato. Dal 2004 le infrastrutture critiche si scambiano informazioni, prima mediante l'ex Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) e oggi con il NCSC. Questo modello, però, sta dimostrando sempre di più i propri limiti. Per fare in modo che funzioni, uno scambio su base volontaria deve essere fondato su un rapporto di fiducia ben consolidato, che però può essere costruito soltanto se il numero delle parti coinvolte è limitato e se vi è periodicamente la possibilità di confrontarsi in modo diretto. Oggi, però, dal momento che i ciberattacchi sono diventati una minaccia per un gran numero di imprese operanti in settori critici, non è più possibile garantire l'instaurarsi di sufficienti rapporti di fiducia con tutti i soggetti interessati. Negli ultimi anni, quindi, lo scambio di informazioni con alcune imprese e organizzazioni con cui vi era un rapporto di

1 Rapporto del Consiglio federale del 13.12.2019 sulle varianti per l'attuazione di un obbligo di notifica in caso di gravi incidenti legati alla sicurezza delle infrastrutture critiche, in adempimento del postulato 17.3475 Graf-Litscher del 15.06.2017 (rapporto sul postulato).

2 Rapporto del gruppo di esperti per il futuro del trattamento e della sicurezza dei dati del 17.8.2018 (raccomandazione 28). Il gruppo di esperti è stato istituito dal DFF in adempimento della mozione Rechsteiner (13.3841) «Commissione di esperti per il futuro del trattamento e della sicurezza dei dati» il 27.8.2015 per tre anni.

3 Cfr. rapporto «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen» del 25.11.2020, allegato 01 alla proposta del Consiglio federale dell'11.12.2020.

4 17.3508 mozione Eder «Creazione di un centro di competenza per la cyber-sicurezza a livello di Confederazione».

collaborazione già ben consolidato è continuato, ma non è più realistico pensare di espandere questo modello.

Tuttavia, concentrandosi su un numero ristretto di imprese, le segnalazioni restituiscono un'immagine incompleta, se non distorta, della situazione reale. Non è possibile stabilire quali effetti stia scatenando in Svizzera quale minaccia informatica. Inoltre, lo scambio su base volontaria può portare anche a comportamenti indesiderati. Le imprese che non partecipano allo scambio di informazioni ricevono comunque avvertimenti e suggerimenti di tipo tecnico grazie alle segnalazioni degli altri, perché il NCSC non può tenere nascoste informazioni così importanti ai gestori di infrastrutture critiche. In questo modo, però, vi è il rischio che per le imprese sia più semplice adottare un atteggiamento passivo, sapendo che riceveranno comunque le principali segnalazioni, piuttosto che partecipare attivamente allo scambio di informazioni.

Riassumendo, quindi, piuttosto che proseguire con il modello dello scambio di informazioni su base volontaria sarebbe preferibile l'introduzione di un obbligo di notifica, perché in questo modo si potrebbe ottenere una panoramica completa della situazione e garantire che nessuno possa sottrarsi all'obbligo di preallerta reciproca. Tuttavia sarebbe opportuno portare avanti la collaborazione e i rapporti di fiducia reciproca sviluppati attraverso lo scambio di informazioni. In questo senso l'elemento discriminante sarà la possibilità per le imprese e le organizzazioni di ottenere anche un vantaggio dall'introduzione dell'obbligo di notifica.

1.2.2 Rapporto con gli altri obblighi di notifica e scambio di informazioni tra le autorità

L'introduzione di un obbligo di notifica di ciberattacchi ha un impatto sugli obblighi di notifica già esistenti e pone quindi il problema di come e quando le notifiche pervenute al NCSC possano essere inoltrare ad altre autorità.

Per quanto riguarda il rapporto con gli obblighi di notifica già esistenti, è stato verificato se fosse possibile inserire al loro interno anche l'obbligo di notifica di ciberattacchi, in modo da evitare di introdurre un obbligo generale valido per tutti i settori. Questa possibilità è stata però esclusa perché i regolamenti in materia di incidenti legati alla sicurezza attualmente in vigore nei diversi settori non sono omogenei e in alcuni casi non esistono neppure. Mantenendo quindi come possibile soluzione l'introduzione di un obbligo di notifica di ciberattacchi a un servizio centrale di notifica, è necessario però stabilire quali notifiche devono essere effettuate, quando e da chi. L'obbligo di notifica di ciberattacchi, quindi, non sostituirebbe gli altri obblighi di segnalazione in vigore, ma semplicemente li integrerebbe. Contemporaneamente si è cercato di fare in modo che le basi legali permettano di adempiere contemporaneamente a più di un obbligo di notifica. L'impegno richiesto per assolvere i diversi obblighi, infatti, dovrebbe essere il minore possibile, in particolare, ma non soltanto, rispetto all'obbligo di notifica di violazioni della sicurezza dei dati ai sensi dell'articolo 24 della nuova legge federale sulla protezione dei dati (di seguito: nLPD)[5], perché spesso i ciberattacchi provocano anche una perdita di dati. La soluzione scelta permette alla persona che effettua la notifica di inoltrare la notifica del ciberattacco anche ad altri servizi simil nel momento in cui la trasmette al NCSC, adempiendo così contemporaneamente a più obblighi di notifica. Allo stesso tempo il NCSC riceverà anche segnalazioni di ciberattacchi inviate per adempiere ad altri obblighi di notifica, purché contengano i dati richiesti. In questo modo quindi non dovrebbe essere necessario segnalare lo stesso evento a più servizi attraverso procedure diverse.

A questo riguardo dovranno essere chiarite anche le modalità di scambio di informazioni tra le autorità. Quando imprese e organizzazioni segnalano al NCSC un ciberattacco volontariamente o per assolvere un obbligo, devono sapere come verrà trattata la loro notifica e chi riceverà queste informazioni. Anche qui si intendono mantenere i principi su cui si basava il precedente modello dello scambio di informazioni. Per poter inoltrare le notifiche, o parti di esse, è necessario il consenso del gestore dell'infrastruttura critica interessata oppure tali informazioni devono essere rese anonime.

Tuttavia, in due casi il NCSC deve poter inoltrare informazioni che permettono di risalire alla persona che ha effettuato la notifica o alla persona interessata anche senza il loro consenso. Il primo

5 Legge federale del 25 settembre 2020 sulla protezione dei dati (LPD), FF **2020** 6695

caso è dato se la notifica contiene informazioni relative a un reato grave: il NCSC può infatti inoltrare queste informazioni alle autorità di perseguimento penale. Sebbene il NCSC sia esonerato dall'obbligo di denuncia di cui all'articolo 22*a* della legge del 24 marzo 2000[6] sul personale federale, il responsabile del NCSC può inoltrare alle autorità di perseguimento penale delle informazioni se lo ritiene necessario in considerazione della gravità del reato. L'inoltro delle informazioni alle autorità di perseguimento penale non avrà conseguenze penali per il gestore dell'infrastruttura critica, perché solitamente la procedura viene avviata soltanto contro gli autori dell'attacco. Tuttavia, nel raro caso in cui il gestore dell'infrastruttura critica dovesse essere oggetto del perseguimento penale, l'obbligo di notifica non deve fare in modo che la segnalazione si trasformi in un'autoaccusa. Per questo motivo è stata inserita una disposizione per tenere conto del divieto di autoaccusarsi come principio cardine del perseguimento penale. Tale disposizione si ispira a quella relativa all'obbligo di notifica di violazione della sicurezza dei dati della legge rivista in materia di protezione dei dati (cfr. art. 24 cpv. 6 nLPD).

Il secondo caso che esonera dal consenso riguarda l'inoltro di informazioni utili al Servizio delle attività informative della Confederazione (SIC) per individuare tempestivamente e sventare minacce per la sicurezza interna o esterna, per valutare la situazione di minaccia o per il servizio di preallerta informativa ai fini della protezione di infrastrutture critiche ai sensi dell'articolo 6 capoverso 1 lettera a, capoverso 2 e 5 della legge federale del 25 settembre 2015[7] sulle attività informative (LAIn). In questo modo si assicura che il SIC riceva le informazioni di cui ha bisogno in qualità di autorità competente per la preallerta delle infrastrutture critiche e la valutazione della situazione di minaccia.

1.2.3 Applicazione dell'obbligo di notifica attraverso incentivi e sanzioni

Direttamente collegata all'introduzione dell'obbligo di notifica è anche la scelta degli strumenti da adottare per la sua applicazione. La disponibilità ad assolvere l'obbligo di notifica può essere influenzata da tre fattori.

Innanzitutto la notifica deve essere resa il più facile possibile. Tale requisito viene soddisfatto dal NCSC mettendo a disposizione un modulo elettronico attraverso il quale sia possibile registrare rapidamente la notifica e inviarla in modo semplice.

In secondo luogo è necessario che vi siano degli incentivi alla notifica. Questi incentivi sono principalmente il servizio di valutazione e il supporto tecnico offerto dal NCSC per contrastare l'attacco. Questi devono essere intesi come un servizio di pronto intervento e non devono avere una portata tale da entrare in concorrenza con altri servizi disponibili sul mercato. Per i gestori delle infrastrutture critiche, però, può essere molto utile poter contare su un servizio federale che ha una panoramica completa sulla situazione di minaccia e che può fornire aiuto e supporto per una valutazione iniziale e per l'adozione di misure immediate.

Infine, l'ultimo fattore che influisce sulla disponibilità ad assolvere l'obbligo di notifica sono i deterrenti, ovvero le multe. Se, nonostante il confronto con l'infrastruttura critica, si dovesse arrivare comunque a una violazione dell'obbligo di notifica o di informazione, il NCSC, come ultima ratio, può emanare una decisione con comminatoria della multa. L'importo massimo della multa è pari a 100 000 franchi, ma all'azienda che gestisce l'infrastruttura critica può essere comminata direttamente una multa fino a 20 000 franchi. Questa possibilità di comminare una sanzione amministrativa si ispira alla legge sulla protezione dei dati rivista, che all'articolo 63 e seguente prevede una disposizione simile in caso di inosservanza dei provvedimenti disposti dall'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).

Dato il lungo e consolidato rapporto di collaborazione con le infrastrutture critiche, tuttavia, il NCSC ritiene che questa disposizione abbia principalmente un valore simbolico e che serva soprattutto a conferire la necessaria considerazione all'obbligo di notifica.

6 RS **172.220.1**
7 RS **121**

1.3 Rapporto con il programma di legislatura e il piano finanziario, nonché con le strategie del Consiglio federale

Il progetto posto in consultazione era stato annunciato nel messaggio del 29 gennaio 2020[8] sul programma di legislatura 2019–2023 e nel decreto federale del 21 settembre 2020[9] sul programma di legislatura 2019–2023. Nel messaggio sul programma di legislatura si fa riferimento in particolare alla necessità di individuare e superare in modo tempestivo gli incidenti informatici di infrastrutture critiche e di aumentare la resilienza nell'ambito TIC. L'articolo 19 del decreto federale sul programma di legislatura stabilisce quanto segue all'obiettivo 18: «la Confederazione affronta i ciberrischi e sostiene e adotta provvedimenti volti a proteggere la cittadinanza e le infrastrutture critiche». Inoltre, sia nel messaggio che nel decreto federale sul programma di legislatura si fa riferimento alla Strategia nazionale del 18 aprile 2018 per la protezione della Svizzera contro i cyberrischi 2018–2022 e al relativo piano di attuazione.

Nel preventivo per il 2022 con piano integrato dei compiti e delle finanze 2023-2025 il miglioramento della cibersicurezza a livello di Confederazione e nazionale viene inserito tra le priorità strategiche e l'obbligo di notifica è menzionato tra gli affari. Inoltre, viene sottolineato che il NCSC contribuisce attivamente alla protezione della Svizzera contro i ciber-rischi[10].

Nella Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022, con la misura 9 vengono forniti i chiarimenti e la decisione circa l'introduzione di un obbligo di notifica di ciberincidenti. Tale misura è stata completamente attuata con il presente progetto posto in consultazione[11].

8 FF 2020 **1565**, pag. 1653.
9 FF 2020 **7365**, pag. 7372.
10 Preventivo 2022 con PICF 2023–2025, volume 2B, pag. 11 e segg., consultabile sul sito www.efv.admin.ch > Pagina iniziale > Rapporti finanziari > Rapporti finanziari > Preventivo con piano integrato dei compiti e delle finanze (https://www.efv.admin.ch/dam/efv/it/dokumente/Finanzberichte/finanzberichte/va_iafp/2022/va2b-2022.pdf.download.pdf/VA2B-6-8-i.pdf).
11 Cfr. Rapporto sullo stato di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022, agosto 2021, pag. 10, 15 seg., www.ncsc.admin.ch > Pagina iniziale NCSC > Strategia SNPC > Rapporti (https://www.ncsc.admin.ch/dam/ncsc/it/dokumente/strategie/Bericht-Umsetzungsstand_NCS_2021_IT.pdf.download.pdf/Bericht-Umsetzungsstand_NCS_2021_IT.pdf).

2 Diritto comparato, in particolare rapporto con il diritto europeo

Dal mese di luglio del 2016, quando è stata approvata la direttiva UE volta a garantire una maggiore sicurezza delle reti e dei sistemi informativi (direttiva NIS), tutti i Paesi membri dell'UE sono stati obbligati a implementare un obbligo di notifica di ciberincidenti. Il termine fissato per tale attuazione è scaduto a maggio 2018. L'obbligo di notifica riguarda gli «operatori di servizi essenziali» e, ai sensi dell'articolo 4, rientrano in questa definizione le imprese private e le istituzioni pubbliche che svolgono un ruolo importante per la garanzia della sicurezza in settori quali settore sanitario, trasporti, energia, settore bancario e infrastrutture dei mercati finanziari, infrastrutture digitali e fornitura e distribuzione di acqua[12]. I destinatari corrispondono quindi in larga parte alle infrastrutture critiche che, in base al progetto posto in consultazione, sarebbero assoggettate all'obbligo di notifica.

Per quanto riguarda la portata dell'obbligo di notifica la direttiva NIS lascia agli Stati membri dell'EU uno spazio di manovra relativamente ampio. L'obbligo di notifica si applica agli incidenti più gravi e all'articolo 14 viene stabilito che per determinare l'impatto di un incidente dovranno in particolare essere presi in considerazione il numero di utenti interessati, la durata dell'incidente e la diffusione geografica. A differenza del presente progetto posto in consultazione, però, la direttiva NIS non si limita all'introduzione di un obbligo di notifica, ma impone agli operatori di servizi essenziali di adottare anche misure di sicurezza, tra cui rientrano la prevenzione dei rischi, misure a garanzia della sicurezza delle reti e dei sistemi informativi e misure che riducano il più possibile l'impatto degli incidenti che riguardano la sicurezza (art. 14).

Il progetto posto in consultazione, invece, si limita a creare le basi legali per simili requisiti nel settore dell'energia. Uno studio commissionato dall'Ufficio federale dell'energia (UFE) ha constatato che in questo settore, decisivo per l'approvvigionamento economico e la sicurezza del Paese, vi è un forte bisogno di intervenire in materia di cibersicurezza[13]. Nei restanti settori è necessario innanzitutto chiarire se la Confederazione abbia la competenza necessaria per fissare norme giuridicamente vincolanti in materia di cibersicurezza e quali requisiti debbano essere fissati in quali settori.

12 DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO - del 6.7.2016 - recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (L 194/1).

13 «Cyber Security und Cyber Resilienz für die Schweizer Stromversorgung», rapporto del 28.6.2021, www.bfe.admin.ch > Pagina iniziale > Approvvigionamento > Digitalizzazione del mondo dell'energia https://www.bfe.admin.ch/bfe/de/home/news-und-medien/publikationen.exturl.html/aHR0cHM6Ly9wdWJkYi5iZmUuYWRtaW4uY2gvZGUvcHVibGljYX/Rpb24vZG93bmxvYWQvMTA1MjQ=.html

3 Punti essenziali del progetto

3.1 La normativa proposta

L'introduzione dell'obbligo di notifica di ciberattacchi a infrastrutture critiche viene proposto innanzitutto al fine di creare un sistema di preallerta e ottenere una panoramica migliore sulla situazione di minaccia. Dal momento che gli hacker spesso ricorrono a strategie e modalità simili per sferrare attacchi a svariate infrastrutture critiche operanti in settori diversi, l'obbligo di notifica, permettendo la rapida individuazione dei metodi d'attacco e la diffusione di informazioni a riguardo, potrebbe aumentare notevolmente la cibersicurezza delle infrastrutture critiche.

L'obbligo di notifica riguarda soltanto i ciberattacchi che possono arrecare notevoli danni. I ciberattacchi provocati un comportamento errato, ad esempio un'operazione sbagliata compiuta involontariamente da un collaboratore, non sono invece sottoposti a obbligo di notifica. Infine si è rinunciato anche alla possibilità di estendere l'obbligo di notifica alle vulnerabilità riscontrate negli strumenti informatici. Tuttavia, a prescindere dall'introduzione dell'obbligo di notifica di ciberattacchi, chiunque potrà continuare a segnalare volontariamente ciberincidenti e vulnerabilità. Questa opportunità non è riservata soltanto alle infrastrutture critiche e chiunque può ricorrervi.

Con l'introduzione dell'obbligo di notifica di ciberattacchi vengono inoltre regolamentati a livello di legge i compiti del NCSC, attualmente definiti unicamente nell'ordinanza sui ciber-rischi (OCiber)[14]. Tale regolamentazione è necessaria sia perché il NCSC assumerà la funzione di servizio centrale di notifica, sia per tenere conto della riorganizzazione delle autorità federali preposte alla cibersicurezza, e in particolare dell'istituzione del NCSC, avvenuta soltanto durante il dibattito parlamentare sulla LSIn.

3.2 Compatibilità tra compiti e finanze

Il NCSC gestisce già oggi un servizio di contatto che raccoglie le segnalazioni volontarie di ciberincidenti. Tale servizio basa la sua attività sulla pluriennale esperienza maturata con MELANI, la centrale che dal 2004 ha raccolto le segnalazioni effettuate da infrastrutture critiche e popolazione.

Per la raccolta delle segnalazioni il NCSC utilizza un apposito modulo elettronico che può essere adattato per poter raccogliere anche quelle inviate per assolvere l'obbligo di notifica qui proposto. All'inizio l'armonizzazione necessaria con gli altri servizi che già raccolgono segnalazioni di questo tipo (ad es. IFPDT, FINMA, IFSN) e la configurazione del modulo di notifica richiederanno del lavoro aggiuntivo, che potrà però essere coperto con le risorse già a disposizione del NCSC. Per attuare il progetto, però, il NCSC deve poter garantire che le notifiche inviate in adempimento all'obbligo di notifica vengano registrate, quietanzate e documentate correttamente e che vengano inoltrate al giusto servizio ai fini della preallerta, un impegno ulteriore di cui si dovrà tenere conto in fase di potenziamento del NCSC.

Il Centro nazionale per la cibersicurezza in futuro avrà anche il compito di fornire supporto all'infrastruttura critica interessata per la gestione dell'incidente, un servizio già fornito e ben rodato grazie alla pluriennale esperienza maturata dal NCSC (e prima ancora da MELANI) ma che sicuramente dopo l'introduzione dell'obbligo di notifica richiederà un impegno maggiore. Questo perché, molto probabilmente, il NCSC riceverà più segnalazioni e, in più, sarà anche tenuto a fornire almeno una prima valutazione e raccomandazioni su come contrastare l'attacco. Di conseguenza anche il team del NCSC addetto all'analisi tecnica (GovCERT) dovrà essere potenziato.

3.3 Attuazione

3.3.1 Necessità di una base legale

In base al principio di legalità (art. 5 cpv. 1 Cost.[15]) e alle disposizioni in materia di legislazione di cui all'articolo 164 capoverso 1 Cost., l'obbligo di notifica di ciberattacchi deve essere regolamentato a livello di legge almeno nei suoi elementi fondamentali. Il progetto posto in consultazione,

14 RS **120.73**
15 RS **101**

quindi, contiene gli elementi fondamentali dell'obbligo di notifica di ciberattacchi, ovvero il fattore scatenante e l'entità dell'obbligo di notifica (ciberattacchi che possono potenzialmente arrecare danni), chi sarà assoggettato all'obbligo di notifica (gestori di infrastrutture critiche operanti in determinati settori), il contenuto delle notifiche e il loro utilizzo da parte del NCSC. L'obbligo di notifica per i gestori di infrastrutture critiche rappresenta un'ingerenza nei diritti di soggetti privati o, in caso di istituzioni cantonali o comunali, nella loro autonomia federalistica. Tuttavia non si tratta di un'ingerenza grave; inoltre non ha ripercussioni finanziarie sull'impresa o sull'istituzione interessata.

3.3.2 La LSIn come base giuridica adatta

Nell'ambito dei lavori preparatori si è valutato se le nuove regole dovessero essere introdotte in una legge separata o in una esistente, il cui scopo, oggetto e ambito di applicazione fosse compatibile con un obbligo di notifica di ciberattacchi a infrastrutture critiche[16]. Le leggi prese in considerazione come possibili basi legali per l'introduzione di un obbligo di notifica sono state quelle che contengono già disposizioni in materia di tutela delle infrastrutture critiche e che sono incentrate sulla protezione dell'ordine pubblico (LPPC[17], LAP[18], LMSI[19], LAIn e LSIn[20]). Dopo un esame approfondito, però, soltanto la LSIn si è dimostrata adatta. Il suo scopo, garantire la sicurezza delle informazioni trattate dalla Confederazione e dei mezzi informatici impiegati, è direttamente collegato alla cibersicurezza (anche se nella legge non viene utilizzato questo termine). Inoltre la LSIn contiene già disposizioni che prevedono un supporto alle infrastrutture critiche da parte della Confederazione. Questo compito del NCSC, quindi, era già regolamentato a livello di legge da queste disposizioni. La LSIn, dunque, si è rivelata non soltanto adatta, ma pure la base legale ideale all'interno della quale introdurre l'obbligo di notifica di ciberattacchi. Un altro elemento a favore è rappresentato dal fatto che nei dibattiti parlamentari sul disegno di legge si era discusso dell'introduzione dell'obbligo di notifica per i gestori di infrastrutture critiche in caso di «incidenti gravi», ma a giugno 2020 tale proposta era stata rifiutata dalla maggioranza del Consiglio nazionale dopo che il nostro Consiglio aveva fatto notare che si stava elaborando un progetto da porre in consultazione su questo argomento.

3.3.3 Disposizioni di esecuzione

Le disposizioni legali saranno concretizzate attraverso un'ordinanza nella quale verranno descritti più nel dettaglio i compiti del NCSC e la collaborazione con altri servizi e sarà specificato chi dovrà notificare quali ciberattacchi seguendo quale procedura e quando. L'ordinanza integrerà le disposizioni dell'attuale OCiber che disciplinano il rapporto tra la Confederazione e il pubblico e in particolare i gestori di infrastrutture critiche. Per quanto riguarda le disposizioni relative ai destinatari sarà necessario verificare singolarmente se sia preferibile inserire una precisazione nell'ordinanza sull'obbligo di notifica o nelle ordinanze specifiche dei singoli settori.

3.3.4 Attuabilità dell'obbligo di notifica

Ad aprile 2021 il NCSC ha condotto un sondaggio sulla prevista introduzione dell'obbligo di notifica di ciberattacchi intervistando i gestori di infrastrutture critiche e le autorità. Dai risultati è emerso che in generale i soggetti coinvolti sono favorevoli alla proposta, purché venga implementata richiedendo un impegno ridotto a livello burocratico. La figura 1 illustra l'elevato consenso generale tra gli intervistati.

16 Cfr. rapporto «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen» del 25.11.2020, allegato 01 alla proposta del Consiglio federale dell'11.12.2020.
17 RS **520.1**
18 RS **531**
19 RS **120**
20 Legge federale sulla sicurezza delle informazioni in seno alla Confederazione (Legge sulla sicurezza delle informazioni, LSIn) del 18.12.2020, FF **2020** 8755

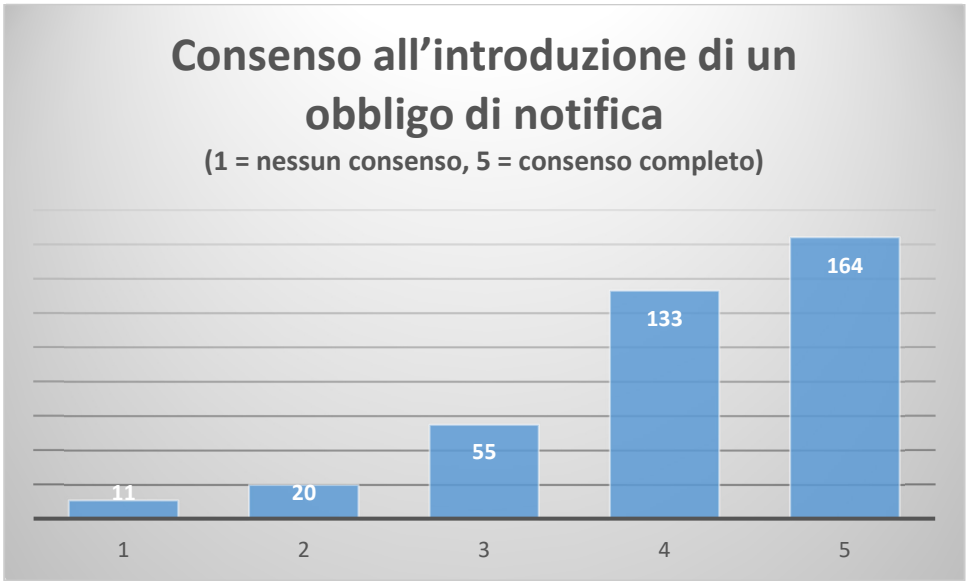

Figura 1 Valutazione della proposta di introdurre un obbligo di notifica

Un ciberattacco a un'infrastruttura critica può comportare, oltre all'obbligo di notifica al NCSC, l'avvio di altri processi sottoposti a obbligo di segnalazione e quindi imporre contemporaneamente svariati obblighi di notifica. Possono per esempio presentarsi i seguenti casi:

- le infrastrutture critiche che operano nel settore dei mercati finanziari sotto la vigilanza della FINMA già da maggio 2020 sono sottoposte all'obbligo di notifica alla FINMA in caso di ciberincidenti[21]. Nel caso subiscano un ciberattacco, quindi, queste imprese dovrebbero segnalare l'evento sia alla FINMA che al NCSC;

- un ciberattacco a un'infrastruttura critica può comportare una violazione della sicurezza dei dati, che, a seconda della gravità, può prevedere un obbligo di notifica all'IFPDT[22];

- se un ciberattacco provoca un malfunzionamento di un'infrastruttura critica, ad esempio un incidente radioattivo in una centrale nucleare, anche questo evento deve essere segnalato (IFSN, CENAL, ecc.).

Il nuovo obbligo di notifica di ciberattacchi che si intende introdurre non sostituirà gli obblighi di segnalazione già in vigore, che rimarranno validi e inalterati. È quindi importante che l'impegno richiesto ai destinatari dell'obbligo di notifica sia sostenibile anche nel caso in cui debbano contemporaneamente assolvere altri obblighi di segnalazione. Per questo motivo il NCSC metterà a disposizione un sistema per la registrazione elettronica della notifica (modulo, maschera di notifica o strumento simile). Gli assoggettati all'obbligo potranno decidere autonomamente se inviare la notifica registrata elettronicamente ad altri servizi di segnalazione inserendo eventuali informazioni aggiuntive. Se gli altri servizi di segnalazione forniranno il proprio supporto, il modulo potrebbe essere anche strutturato in modo tale che, oltre a informazioni generali sull'infrastruttura critica, permetta di inserire informazioni aggiuntive specifiche destinate unicamente a un determinato servizio di segnalazione per l'assolvimento del relativo obbligo di notifica. In questo modo al momento della registrazione e dell'inoltro i soggetti che sottostanno all'obbligo potrebbero decidere quali informazioni inviare a quale servizio.

21 Cfr. art. 29 LFINMA. L'obbligo generale di notifica riguarda anche i ciberincidenti (cfr. Comunicazione FINMA sulla vigilanza 05/2020 del 7.5.2020).
22 art. 24 nLPD

4 Commento ai singoli articoli

Le basi legali dell'obbligo di notifica di ciberattacchi, fatti salvi alcuni adeguamenti al capitolo 1, verrebbero introdotte nel capitolo 5 della LSIn. Il capitolo 5 è stato completamente rielaborato in modo da integrare anche i compiti del NCSC che vanno oltre l'obbligo di notifica e non riguardano esclusivamente le infrastrutture critiche. Per questo motivo è stato modificato anche il titolo del capitolo («Capitolo 5: Misure della Confederazione per la protezione della Svizzera contro i ciber-rischi»).

I principali contenuti delle disposizioni di legge in parte sono già stati descritti in modo esaustivo e giustificati nel messaggio concernente la legge sulla sicurezza delle informazioni (FF *2017* 2675 segg.) e ai punti precedenti. Il commento ai seguenti articoli contiene quindi soltanto integrazioni.

Capitolo 1: Disposizioni generali

Nel primo capitolo sono state apportate modifiche soltanto agli articoli 1, 2 e 5. I restanti articoli non sono stati modificati.

Articolo 1 Scopo

L'articolo della LSIn concernente lo scopo è stato integrato al *capoverso 1* e per questo è stata introdotta una suddivisione nelle lettere a e b. Alla *lettera a* è stata ripresa la formulazione originale, mentre alla *lettera b* è stato specificato lo scopo della legge per quanto concerne i ciber-rischi. L'articolo è stato quindi ampliato per tenere conto degli aspetti inseriti con l'introduzione dell'obbligo di notifica di ciberattacchi e con la regolamentazione a livello di legge dei compiti del NCSC.

Articolo 2 Autorità e organizzazioni assoggettate

È stato modificato il rimando nel capoverso 5 alle disposizioni valide per le infrastrutture critiche perché ora il capitolo 5 inizia con l'articolo 73*a* e termina con l'articolo 79. Non sono state apportate modifiche a livello di contenuto.

Articolo 5 Definizioni

Le definizioni alle lettere a, b e c non sono state modificate.

Lettera d

A questa lettera è stata inserita la definizione di «ciberincidente», ripresa dall'articolo 3 lettera b OCiber e leggermente adeguata. La definizione comprendere anche l'abuso di mezzi informatici, che può avvenire, ad esempio, in caso di tentativi di phishing.

Lettera e

È stata inserita la definizione di «ciberattacco», ovvero un possibile tipo di ciberincidente. La definizione di «ciberattacco», che ne specifica il significato rispetto all'iperonimo «ciberincidente», è importante perché soltanto gli attacchi a infrastrutture critiche sono sottoposti all'obbligo di notifica, mentre i ciberincidenti e le vulnerabilità possono essere segnalate volontariamente e da chiunque.

Capitolo 5: Misure della Confederazione per la protezione della Svizzera contro i ciber-rischi

Al secondo, terzo e quarto capitolo non sono state apportate modifiche. Nel capitolo quinto, oltre all'obbligo di notifica di ciberattacchi a infrastrutture critiche, sono state inserite anche le disposizioni di base relative ai compiti del NCSC. Per renderlo più chiaro il capitolo 5 è quindi stato suddiviso in 3 sezioni.

Sezione 1: Disposizioni generali

Articolo 73a Principio

In questo articolo sono descritti i compiti del NCSC dalla lettera a alla lettera f. Si tratta di un elenco non esaustivo. Riguardo alla ricezione e al trattamento di notifiche (*lettera e*) va precisato che sono intese sia le notifiche volontarie di ciberincidenti e vulnerabilità sia le notifiche di ciberattacchi nei confronti di infrastrutture critiche soggetti all'obbligo di notifica.

I singoli compiti e la collaborazione con le autorità nazionali ed estere sono oggetto di altri articoli che ne concretizzano il contenuto.

Articolo 73b Trattamento delle notifiche di ciberincidenti e vulnerabilità

Dal 1° gennaio 2020 il NCSC gestisce un servizio nazionale di contatto per le questioni legate ai ciber-rischi (cfr. art. 12 cpv. 1 lett. a OCiber), che raccoglie ed elabora le segnalazioni di ciberincidenti e vulnerabilità. Il servizio del NCSC è stato realizzato sulla base di MELANI, la centrale che ha raccolto questo tipo di segnalazioni dal 2004. Questo servizio offerto dal NCSC viene utilizzato attivamente dalle imprese e dalla popolazione. Nel 2020 ha raccolto 10 834 segnalazioni[23].

Dal 28 settembre 2021 il NCSC fa parte della rete mondiale per la gestione delle vulnerabilità nei sistemi informatici ed è autorizzato ad assegnare alle vulnerabilità segnalate un numero d'identificazione univoco in conformità con il sistema di riferimento internazionale[24]. È importante quindi precisare che il NCSC non raccoglie soltanto le notifiche di ciberincidenti ma anche quelle relative alle vulnerabilità.

Capoverso 1

I ciberincidenti e le vulnerabilità possono essere notificati al NCSC non soltanto dai soggetti interessati ma anche da soggetti terzi ed, eventualmente, anche in modo anonimo. Il NCSC analizza gli incidenti e ne valuta la rilevanza per la protezione della Svizzera contro i ciber-rischi. Nel caso in cui la notifica non sia anonima e se la persona che la effettua lo richiede, il NCSC può fornire sulla base di queste analisi anche valutazioni sull'evento e raccomandazioni su come procedere. Il NCSC, inoltre, utilizza le notifiche per scopi statistici e per allertare il pubblico circa le minacce informatiche senza però fornire dati sulla persona che ha effettuato la notifica o sui soggetti interessati dalle minacce.

Il NCSC tratta in modo riservato le notifiche ricevute. La riservatezza è un presupposto fondamentale per garantire che le notifiche vengano effettuate e per favorire la fiducia verso il servizio di notifica.

Capoverso 2

Il NCSC è autorizzato a pubblicare le informazioni sui ciberincidenti o a inoltrarle a autorità e organizzazioni interessate soltanto se queste non contengano dati personali o dati di persone giuridiche. Non è consentito pubblicare dati personali in caso di ciberincidenti. Rimane invece possibile pubblicare con il consenso della persona o dell'organizzazione interessate informazioni contenute in una notifica, ad esempio in caso di abuso di un logo mediante attacchi di phishing.

Capoverso 3

In caso di vulnerabilità, al contrario, può essere necessario rendere nota la vulnerabilità in tempi brevi citando il software o l'hardware interessati per scongiurare ulteriori ciberattacchi. Lo sfruttamento delle vulnerabilità è una delle strategie più utilizzate per sferrare ciberattacchi. Soltanto attraverso la pubblicazione di queste informazioni gli utenti del software o dell'hardware possono adottare tempestivamente le misure necessarie per proteggersi dai ciberattacchi connessi. Il capo-

23 Cfr. Rapporto sullo stato di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022 redatto ad agosto 2021, pag. 5 (www.ncsc.admin.ch > Pagina iniziale NCSC > strategia SNPC > Rapporti, https://www.ncsc.admin.ch/dam/ncsc/it/dokumente/strategie/Bericht-Umsetzungsstand_NCS_2021_IT.pdf.download.pdf/Bericht-Umsetzungsstand_NCS_2021_IT.pdf).

24 Cfr. comunicato stampa del NCSC del 28.9.2021(www.ncsc.admin.ch > Pagina iniziale NCSC > Documentazione > Comunicati stampa > Newslist > L'NCSC fa ora parte della rete mondiale per la gestione delle vulnerabilità nei sistemi informatici; https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/medienmitteilungen/newslist.msg-id-85280.html).

verso 3 costituisce la base legale ai sensi della quale pubblicando le vulnerabilità il NCSC è autorizzato a rendere noto il nome dell'hardware e del software interessati e quindi, implicitamente, anche il loro produttore.

Articolo 73c Inoltro di informazioni

L'articolo 73*c* stabilisce i presupposti che devono essere soddisfatti affinché il NCSC possa inoltrare al SIC o alle autorità di perseguimento penale determinate informazioni contenute in una notifica (capoversi 1 e 2). Infine vengono disciplinate anche le modalità con cui possono essere utilizzate le informazioni nel caso in cui dovesse essere avviato un procedimento penale contro la persona che ha presentato la notifica (capoverso 3).

Capoverso 1

Il capoverso 1 stabilisce che il NCSC è autorizzato a inoltrare informazioni al SIC se queste sono rilevanti per individuare tempestivamente e sventare minacce per la sicurezza interna o esterna, per valutare la situazione di minaccia o per assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche ai sensi dell'articolo 6 capoversi 1 lettera a, 2 e 5 LAIn. L'inoltro è necessario per consentire al SIC di assolvere anche i propri compiti in materia di minacce informatiche, ma è limitato alle informazioni necessarie a tale fine.

Capoverso 2

Il capoverso 2 disciplina l'inoltro di informazioni alle autorità di perseguimento penale. L'obbligo di denuncia a cui è soggetto il personale federale non si applica per le informazioni che il NCSC riceve nell'ambito di una notifica di un ciberincidente o della sua analisi, perché tale obbligo di denuncia è in conflitto con il principio del trattamento confidenziale della notifica. Il responsabile del NCSC è però autorizzato a inoltrare informazioni alle autorità di perseguimento penale, valutando se prevalga l'interesse dello Stato al perseguimento penale o l'interesse alla riservatezza della notifica per la persona che l'ha effettuata. La possibilità di inoltrare la notifica dopo un'opportuna valutazione degli interessi è stata introdotta per permette al NCSC di rivolgersi alle autorità di perseguimento penale in caso di reati gravi.

Capoverso 3

La disposizione di cui al capoverso 3 garantisce che, nel corso di un procedimento penale contro la persona che ha inviato la notifica, le informazioni in essa contenute non possano essere usate contro questa persona senza il suo consenso. Di norma un procedimento penale viene avviato contro chi ha provocato il ciberattacco, quindi contro l'hacker, e non contro la persona che ha inviato la notifica. Nel caso in cui, però, eccezionalmente, dovesse essere avviato un procedimento penale contro la vittima del ciberattacco, è stata introdotta una disposizione analoga a quella di cui all'articolo 24 capoverso 6 nLPD. Questa disposizione, quindi, sancisce il principio secondo cui nessuno può essere obbligato ad affermare la propria responsabilità (nemo tenetur se detegere) in relazione all'obbligo di notifica di ciberattacchi ed è quindi particolarmente rilevante nel caso delle notifiche effettuate per assolvere l'obbligo di notifica di ciberattacchi. Lo stesso privilegio, però, sarà applicabile anche alle notifiche volontarie.

Capoverso 4

Nei casi eccezionali per i quali è previsto l'inoltro di informazioni al SIC o alle autorità di perseguimento penale di cui ai capoversi 1 e 2, laddove le informazioni rappresentino segreti protetti dalla legislazione penale Il NCSC deve essere esonerato dal rispetto del segreto d'ufficio conformemente alle disposizioni dell'articolo 320 CP.

Articolo 74 Sostegno ai gestori di infrastrutture critiche

Oltre ai compiti generali sanciti all'articolo 73*a* e al trattamento delle notifiche di ciberincidenti e vulnerabilità di cui all'articolo 73*b*, il NCSC fornisce ai gestori di infrastrutture critiche anche ulteriori servizi per la protezione contro i ciber-rischi (*capoverso 1*). A questo riguardo bisogna sottolineare che la definizione di infrastrutture critiche fornita all'articolo 5 LSIn è formulata in modo molto ampio e quindi non chiarisce quando un'organizzazione debba essere considerata o meno un'infrastruttura critica. Il NCSC a questo riguardo fa riferimento ai settori e ai sottosettori elencati nella Strategia nazionale per la protezione delle infrastrutture critiche (PIC)[25].

Capoverso 2

A tale scopo il NCSC mette a disposizione dei gestori di infrastrutture critiche vari strumenti. I principali vengono elencati a titolo esemplificativo in questo capoverso. L'elenco non è quindi esaustivo.

Lettera a

Lo scambio reciproco di informazioni è uno strumento molto importante per la protezione dai ciber-rischi. L'elevato dinamismo con cui si evolvono le situazioni di minaccia e la necessità di possibili misure di protezione impone ai responsabili di essere costantemente aggiornati sulle ultime novità e il modo più efficace per raggiungere questo obiettivo è il confronto con altri responsabili. Il NCSC, al fine di portare avanti la consolidata collaborazione stretta tramite MELANI, offre ai gestori di infrastrutture critiche una piattaforma attraverso la quale scambiarsi tali informazioni.

Lettera b

Le informazioni su ciber-rischi e vulnerabilità attuali e le raccomandazioni per l'adozione di misure preventive si limitano a indicazioni utili in modo generale a qualsiasi infrastruttura critica. Non viene fornita una consulenza specifica per la singola impresa.

Lettera c

Parte degli strumenti e delle istruzioni per l'individuazione tempestiva vengono concepiti in modo tale da risultare utili in generale a tutte le infrastrutture critiche. Ma possono essere anche specifici per determinati gruppi di infrastrutture critiche o pensati per determinati settori di attività. Essi non sostituiscono i dispositivi di protezione delle singole imprese, ma devono essere integrati al loro interno.

Capoverso 3

In caso di ciberincidenti il NCSC fornisce supporto ai gestori di infrastrutture critiche attraverso una consulenza tecnica. Nel caso di gestori privati, il sostegno tecnico offerto dal NCSC è sussidiario rispetto ai servizi IT disponibili sul mercato. A questo proposito non è determinante la forma giuridica bensì il soggetto che detiene la responsabilità. Il NCSC, inoltre, fornisce questo supporto solo ed esclusivamente se è necessario intervenire rapidamente e vi è il rischio di conseguenze gravi.

Capoverso 4

In caso di ciberincidenti, in particolare sotto forma di ciberattacchi, il NCSC dovrebbe avere la possibilità di accedere ai sistemi dell'infrastruttura critica interessata per gestire l'incidente o limitare i danni. Ciò, ovviamente, a condizione che il gestore dell'infrastruttura critica fornisca il proprio consenso. Il gestore nei confronti del NCSC è liberato da eventuali obblighi di tutela del segreto. Il *secondo periodo* rappresenta la base legale che permette ai gestori di concedere al NCSC l'accesso

25 Strategia nazionale del Consiglio federale per la protezione delle infrastrutture critiche 2018 – 2022 (www.babs.admin.ch > Pagina iniziale > Altri campi d'attività > Protezione delle infrastrutture critiche > Strategia nazionale PIC; https://www.babs.admin.ch/it/aufgabenbabs/ski/nationalestrategie.html).

alle loro informazioni e ai loro mezzi informatici senza violare obblighi contrattuali o legali di tutela del segreto.

Sezione 2: Obbligo di notifica di ciberattacchi a infrastrutture critiche

Articolo 74a Obbligo di notifica

In questo articolo vengono definiti gli elementi principali dell'obbligo di notifica. In esso viene stabilito che i gestori di infrastrutture critiche sono assoggettati all'obbligo di notifica in caso di ciberattacchi e che questi devono essere segnalati il prima possibile al NCSC una volta individuati. Ai fini della preallerta e della prevenzione, infatti, è fondamentale che gli attacchi vengano segnalati subito dopo la loro scoperta. All'articolo 74*e* si precisa inoltre che il requisito della tempestività non è applicabile a tutte le informazioni richieste, ma soltanto per la prima notifica, effettuata sulla base delle informazioni disponibili in quel momento.

Articolo 74b Settori

La definizione di infrastrutture critiche fornita all'articolo 5 è formulata in modo molto ampio. Non è sufficientemente specifica da permettere di determinare quali imprese o organizzazioni sono considerate infrastrutture critiche e dunque assoggettate all'obbligo di notifica. All'articolo 74*b* vengono quindi elencate nel dettaglio le imprese e le organizzazioni alle quali si applicherebbe l'obbligo di notifica. Tale elenco fa riferimento ai sottosettori critici indicati nella Strategia nazionale per la protezione delle infrastrutture critiche. Quando possibile l'ambito di applicazione dell'obbligo di notifica per questi settori viene definito facendo riferimento a basi legali esistenti. Nei casi in cui questo riferimento non può essere inserito perché non esiste una base legale adeguata per una simile delimitazione, invece, il settore viene definito nel modo più preciso possibile. In questo modo si garantisce che venga specificato in modo sufficientemente chiaro quali soggetti sono sottoposti all'obbligo di notifica.

Lettera a: scuole universitarie

Le scuole universitarie sono molto importanti per la piazza formativa ed economica svizzera. La loro attività di ricerca, in particolare, rappresenta uno dei motori dell'innovazione. Questo però rende le scuole universitarie anche un bersaglio interessante per gli hacker. Sono dunque assoggettate all'obbligo di notifica le università cantonali, i politecnici federali, le scuole universitarie professionali e le alte scuole pedagogiche.

Lettera b: autorità

I ciberattacchi alle autorità, a tutti i livelli federali, sono sottoposti all'obbligo di notifica, perché è importante sapere con quale frequenza e chi sferra attacchi a queste istituzioni. In questo modo possono essere predisposte misure di difesa mirate in base alla minaccia. L'obbligo di notifica è applicabile soltanto alle attività che implicano l'esercizio dell'autorità sovrana di queste autorità e organizzazioni.

Lettera c: organizzazioni cui sono affidati compiti di diritto pubblico

Le organizzazioni che svolgono compiti di interesse pubblico in determinati settori sono assoggettate all'obbligo di notifica. Per chiarire meglio quali attività concrete si intendano, alla lettera c è proposto un elenco. Nel settore della sicurezza e del salvataggio si tratta in particolare delle organizzazioni di primo intervento (polizia, vigili del fuoco, servizi sanitari e di salvataggio). Sono inoltre tenute alla notifica le organizzazioni attive nell'approvvigionamento di acqua potabile, nel trattamento delle acque di scarico e nello smaltimento dei rifiuti.

Lettera d: imprese attive nel settore dell'approvvigionamento energetico, nel commercio, nella misurazione e nella gestione dell'energia

L’approvvigionamento energetico è essenziale per l’economia e la società. Svariati attacchi alle imprese attive nel settore dell’approvvigionamento energetico o alle condutture in altri Stati hanno dimostrato come queste infrastrutture possano essere prese di mira per motivi politici o per cercare di estorcere elevate somme di denaro. Le imprese che svolgono attività importanti per l’approvvigionamento energetico sono quindi sottoposte all’obbligo di notifica.

Lettera e: banche, assicurazioni e infrastrutture del mercato finanziario

Le imprese del settore finanziario sono spesso vittime di ciberattacchi, perché gestendo ingenti quantità di denaro rappresentano un obiettivo interessante per i criminali. Per assicurare l’affidabilità della piazza finanziaria svizzera è quindi importante che questi attacchi vengano segnalati. L’obbligo già vigente di notifica di ciberattacchi alla FINMA rimane in vigore parallelamente. La FINMA e il NCSC si accorderanno in modo da ridurre il più possibile l’onere per i soggetti sottoposti all’obbligo.

Lettera f: servizi digitali

Sono considerati fornitori di servizi digitali tutte le imprese che offrono servizi su Internet che in Svizzera sono utilizzati da un gran numero di utenti, rivestono un’importanza notevole per l’economia digitale o includono servizi di sicurezza o fiduciari. Rientrano quindi in questa definizione in particolare i fornitori di piattaforme per il commercio elettronico di dimensioni significative, di servizi di cloud computing e di motori di ricerca. L’elenco non è esaustivo. Tra gli «altri servizi digitali» sono intesi in particolare servizi nei settori della gestione dell’identità digitale, delle firme o del voto elettronico. Sono inoltre menzionati i centri di registrazione di nomi di dominio e i gestori di centri di calcolo. A livello di ordinanza per specificare quali sono i servizi digitali assoggettati all’obbligo di notifica verranno stabiliti come criteri il numero di utenti, il numero di collaboratori, il fatturato e il tipo di attività.

Lettera g: ospedali

I Cantoni allestiscono elenchi degli ospedali, in cui sono menzionati gli ospedali cantonali ed extracantonali che garantiscono la copertura del fabbisogno di cure mediche di base nel rispettivo territorio cantonale. L’obbligo di notifica di ciberattacchi dovrebbe essere esteso anche a questi ospedali per scongiurare che a causa di attacchi di questo tipo non possano essere garantite le cure mediche di base.

Lettera h: laboratori medici

I laboratori che eseguono analisi microbiologiche per individuare malattie trasmissibili sono importanti per il sistema sanitario. Per svolgere le loro analisi e collaborare con i fornitori di cure mediche di base dipendono in larga misura da infrastrutture IT funzionanti. Per questo i ciberattacchi a questi laboratori sono sottoposti all’obbligo di notifica.

Lettera i: fabbricazione, immissione in commercio o distribuzione, nonché importazione di medicamenti o dispositivi medici

La fabbricazione, la distribuzione e l’importazione di medicamenti sono molto importanti per garantire le prestazioni mediche alla popolazione. Per questo le imprese che operano in questi settori sono sottoposte all’obbligo di notifica. Allo stesso modo anche i produttori e i distributori di dispositivi medici sono assoggettati all’obbligo di notifica.

Lettera j: assicurazioni sociali

Le prestazioni delle assicurazioni sociali sono descritte sulla base dei rischi definiti nelle disposizioni generali della legge federale sulla parte generale del diritto delle assicurazioni sociali (LPGA; RS *830.1*), in modo tale da coprire il più possibile tutti i rami delle assicurazioni sociali. Si è deciso di non elencare le singole leggi (ad es. LAI, LAVS) in modo da coprire non soltanto le prestazioni di legge ma anche quelle sovraobbligatorie, come ad esempio la previdenza professionale o l’assicu-

razione complementare all'assicurazione malattie obbligatoria. Nel caso della previdenza professionale sono considerati tutti gli istituti di previdenza e di libero passaggio, siano essi registrati o non registrati, tuttavia non la previdenza individuale vincolata o volontaria (pilastri 3a e 3b). Queste ultime possibilità previdenziali in genere sono offerte da istituti bancari e assicurativi, che sottostanno all'obbligo di notifica.

A livello di ordinanza anche nel caso delle assicurazioni sociali il nostro Consiglio può introdurre limitazioni alla cerchia dei soggetti sottoposti all'obbligo di notifica, stabilendo criteri adeguati.

Lettera k: fornitori di servizi di telecomunicazione

Una trasmissione mediante telecomunicazione è l'emissione o la ricezione elettrica, magnetica, ottica oppure elettromagnetica di altro tipo, di informazioni su linea o via radioonde (art. 3 lett. c della legge del 30.4.1997[26]sulle telecomunicazioni, LTC). È considerata quale trasmissione mediante telecomunicazione anche l'offerta di capacità di trasmissione e i cosiddetti servizi Over the Top (OTT). In quest'ultimo caso si tratta della trasmissione di informazioni tramite servizi Internet. Si tratta ad esempio di servizi come Skype (Microsoft), WhatsApp (Facebook), Facetime (Apple), Hangouts (Google), Signal e Threema.

Lettera l: Società svizzera di radiotelevisione (SSR)

La SSR ha il compito di fornire programmi radiofonici e televisivi completi e di pari valore a tutta la popolazione nelle tre lingue ufficiali (art. 24 cpv. 1 lett. a della legge federale del 24.3.2006[27] sulla radiotelevisione, LRTV). Inoltre ha il compito di contribuire alla libera formazione delle opinioni del pubblico mediante un'informazione completa, diversificata e corretta, in particolare sulla realtà politica, economica e sociale (art. 24 cpv. 4 lett. a LRTV). Il suo mandato, quindi, va bene oltre gli obblighi di diffusione cui sono sottoposti i restanti media concessionari. I ciberattacchi alla SSR possono minacciare lo svolgimento di questi compiti.

Lettera m: agenzie di stampa d'importanza nazionale

Ai sensi dell'articolo 44*a* dell'ordinanza del 9 marzo 2007[28] sulla radiotelevisione un'agenzia di stampa è considerata d'importanza nazionale se diffonde informazioni sulle quattro regioni linguistiche e pubblica regolarmente informazioni in almeno tre lingue nazionali (cfr. art. 18 lett. a della legge del 5.10.2007[29] sulle lingue in combinato disposto con l'art. 13 cpv. 2 dell'ordinanza del 4.6.2010[30] sulle lingue). Nello specifico in Svizzera è rimasta soltanto l'agenzia di stampa Keystone-ATS (v. ordinanza COVID-19 media elettronici)[31].

Lettera n: fornitori di servizi postali

Le imprese che offrono ai clienti servizi postali a proprio nome sono anch'esse sottoposte all'obbligo di notifica se registrate presso la Commissione delle poste secondo l'articolo 4 capoverso 1 della legge del 17 dicembre 2010[32] sulle poste (LPO). Il nostro Collegio può esonerare dall'obbligo di notifica imprese di dimensioni ridotte a livello di ordinanza, ad esempio analogamente all'esonero delle imprese che realizzano una cifra d'affari economicamente modesta previsto all'articolo 4 capoverso 2 LPO.

Lettera o: trasporto pubblico (trasporto di passeggeri e trasporto ferroviario di merci)

Con il richiamo alla legge federale del 18 giugno 2010[33] sugli organi di sicurezza delle imprese di trasporto pubblico viene preso in considerazione soltanto il settore più importante del trasporto

26 RS **784.10**
27 RS **784.40**
28 RS **784.401**
29 RS **441.1**
30 RS **441.11**
31 RS **784.402**
32 RS **783.0**
33 RS **745.2**

pubblico, ovvero il trasporto di passeggeri in concessione, nonché il trasporto di merci e l'infrastruttura ferroviaria.

Lettera p: imprese dell'aviazione civile

La disposizione sottopone all'obbligo di notifica di ciberattacchi tutte le imprese che dispongono di un'autorizzazione dell'Ufficio federale dell'aviazione civile.

Lettera q: navigazione sul Reno

I porti renani svizzeri costituiscono l'accesso della Svizzera ai mari di tutto il mondo e rivestono un ruolo molto importante per l'approvvigionamento nazionale di merci di ogni tipo. L'obbligo di notifica di ciberattacchi si applica quindi alle imprese che trasportano merci sul Reno secondo la legge federale del 23 settembre 1953[34] sulla navigazione marittima sotto bandiera svizzera e ai processi rilevanti per la gestione e il funzionamento dei porti basilesi.

Lettera r: approvvigionamento di beni indispensabili di uso quotidiano

Nell'approvvigionamento della popolazione con beni indispensabili di uso quotidiano, in particolare generi alimentari, sono coinvolti numerosi soggetti. Oltre ai produttori e agli importatori, infatti, vi sono anche i trasformatori, i centri di distribuzione e i commercianti al dettaglio. Non tutti questi soggetti hanno la stessa importanza per la sicurezza dell'approvvigionamento del nostro Paese. L'obbligo di notifica di ciberattacchi dovrebbe quindi valere soltanto per quei soggetti che svolgono un ruolo importante in questa ottica. Il nostro Consiglio quindi restringerà l'obbligo di notifica nel settore dell'approvvigionamento di beni indispensabili di uso quotidiano applicando i criteri di cui all'art. 74*c*.

Lettera s: produttori di hardware e software

Sempre più spesso si nota che gli attacchi a infrastrutture critiche avvengono utilizzando i loro fornitori di hardware e software. Gli hacker, per garantirsi l'accesso ai sistemi in un secondo momento, compromettono hardware e software prima ancora che siano consegnati ai clienti finali. I produttori di hardware e software sono quindi molto importanti per la cibersicurezza.

Particolarmente rilevanti sono soprattutto i ciberattacchi ai produttori di software che forniscono assistenza ai propri clienti attraverso un sistema per la manutenzione remota. In questi casi, infatti, gli hacker possono cercare di infiltrarsi direttamente nei sistemi delle infrastrutture critiche attraverso questi accessi legittimi. Oltre al criterio legato alla manutenzione remota, i produttori di hardware e software sono sottoposti all'obbligo di notifica se offrono prodotti utilizzati in settori particolarmente delicati. Nello specifico (*n. 1*) hardware e software impiegati per la tecnica di comando e il monitoraggio di sistemi (industrial control systems), utilizzati nell'esercizio di dispositivi medici e impianti di telecomunicazione (*n. 2*) oppure impiegati per attività di garanzia della sicurezza pubblica (*n. 3*). Si tratta in particolare della comunicazione di organizzazioni di primo intervento o dei sistemi utilizzati nelle indagini dalla polizia. Inoltre dovrebbero essere assoggettati all'obbligo di notifica anche i produttori di hardware e software (*n. 4*) con funzioni particolarmente delicate (sicurezza informatica, crittografia, identificazione, attribuzione di diritti di accesso a sistemi o luoghi). Un'eventuale manipolazione di questi prodotti, che vengono impiegati proprio in caso di accresciuta necessità di protezione, sarebbe infatti molto problematica.

Articolo 74c Eccezioni all'obbligo di notifica

All'articolo 74*b* la cerchia dei destinatari è definita in modo molto ampio e può comprendere anche imprese che, nonostante operino in un sottosettore critico, di per sé non sono di fondamentale importanza per il funzionamento dell'economia o per il benessere della popolazione. All'articolo 74*c* si stabilisce quindi che il Consiglio federale limita la cerchia dei soggetti sottoposti all'obbligo facendo ricorso ai criteri elencati. Un'impresa o una categoria di imprese possono essere esentate dall'obbligo di notifica se sono esposte solo in modo ridotto al rischio di ciberattacchi, in quanto si ritiene improbabile che possano esserne vittime, o perché l'impresa nella sua attività dipende solo

34 RS **747.30**

in minima parte dai mezzi informatici (*lettera a*). L'esclusione dall'obbligo di notifica è possibile anche nel caso in cui un eventuale guasto o malfunzionamento avrebbero ripercussioni minime sull'economia o sul benessere della popolazione. L'entità delle ripercussioni viene misurata sulla base del numero di persone interessate, della possibilità che i servizi vengano svolti da altri soggetti e del potenziale di danno per l'economia (*lettera b*).

Articolo 74d Ciberattacchi da notificare

Capoverso 1

La portata dell'obbligo di notifica, ovvero quali tipi di ciberattacchi devono essere notificati, è ora sancita a livello di legge. Alle *lettere dalla a alla d* del capoverso 1 sono elencati i criteri da prendere in considerazione per stabilire se un ciberattacco possa arrecare notevoli danni o possa essere particolarmente rilevante per la tutela di altre infrastrutture critiche. Se il ciberattacco soddisfa uno di questi criteri allora vige l'obbligo di notifica. Questi criteri, se necessario, potranno essere ulteriormente precisati a livello di ordinanza.

Capoverso 2

Il capoverso 2 stabilisce che in caso di concomitanza con circostanze penalmente rilevanti il ciberattacco deve sempre essere notificato. Molti hacker fanno ricorso a minacce e attacchi per cercare di ricattare i gestori di infrastrutture critiche o singoli collaboratori di queste imprese (ad esempio crittografando i dati dell'impresa attraverso ransomware, minacciando di limitare la disponibilità tramite attacchi DDoS o minacciando di pubblicare informazioni compromettenti su singole persone). Questi attacchi devono essere notificati in modo tale che si possa valutare l'entità della minaccia rappresentata dai cibercriminali per le infrastrutture critiche.

Articolo 74e Contenuto della notifica

Al *capoverso 1* vengono disciplinate a livello di legge le informazioni essenziali necessarie per assolvere l'obbligo di notifica. Il contenuto concreto delle singole informazioni da fornire sarà specificato nelle disposizioni di esecuzione.

Nel *capoverso 2* viene precisato che la tempestività con cui deve essere notificato l'evento *(«il prima possibile»*), come stabilito all'articolo 74*a*, riguarda soltanto le informazioni di cui si è già in possesso. Quando si verificano dei ciberattacchi molto spesso per diverso tempo non è chiaro quanto l'attacco sia grave e cosa sia effettivamente accaduto. Se al momento della notifica queste informazioni sono disponibili solo in parte, gli interessati devono quindi avere la possibilità di trasmettere le indicazioni richieste al capoverso 1 soltanto una volta in possesso di maggiori dettagli sull'accaduto.

Articolo 74f Trasmissione della notifica

Capoverso 1

Per permettere di assolvere l'obbligo di notifica con un impegno il più possibile ridotto, il NCSC è tenuto a mettere a disposizione un modulo elettronico di notifica sicuro. Tenuto conto dello sviluppo tecnologico, nel testo della legge il modulo di notifica viene indicato in modo generico come un «sistema sicuro con cui trasmettergli le notifiche». A prescindere da questo modulo di notifica, in ogni caso è comunque possibile informare il NCSC del ciberattacco attraverso altre modalità (per posta elettronica, telefonicamente).

Capoverso 2

Il sistema di segnalazione offre la possibilità a chi effettua la notifica di tramettere contemporaneamente la totalità o una parte della notifica del ciberattacco o delle sue ripercussioni (ad es. le riper-

cussioni sulla sicurezza dei dati o sul funzionamento dell'infrastruttura critica) ad altri servizi e autorità. Il sistema del NCSC non è però riservato unicamente alla trasmissione di notifiche volte ad assolvere un obbligo di legge, esso può essere utilizzato anche per segnalazioni volontarie a servizi terzi. La notifica, però, può essere trasmessa soltanto dal gestore dell'infrastruttura critica interessata. Soltanto il gestore, infatti, può stabilire quali servizi o autorità, fatto salvo il NCSC, possono ricevere la notifica del ciberattacco (o delle sue ripercussioni). Il NCSC non inoltrerà alcuna notifica ad altri servizi o autorità, fatti salvi i casi eccezionali illustrati all'articolo 73*c* capoversi 1 e 2.

Capoverso 3

Il NCSC, su richiesta e in collaborazione con altri servizi di segnalazione, può strutturare il sistema di notifica in modo tale che il gestore di un'infrastruttura critica sottoposto all'obbligo di notifica possa aggiungere eventuali informazioni supplementari, che non sono necessarie per la notifica al NCSC, per trasmetterle a uno o più servizi di segnalazione diversi. Questa funzione dovrebbe servire a ridurre il più possibile l'onere richiesto alle persone assoggettate all'obbligo di notifica. In particolare, nei casi in cui si deve adempiere a più obblighi di notifica contemporaneamente, questo sistema dovrebbe aiutare a informare i relativi servizi e autorità in modo rapido e tempestivo e senza eccessivo dispendio. Queste informazioni supplementari, inserite nel sistema del NCSC dai soggetti che effettuano la notifica e destinate ad altri organismi e autorità, vengono soltanto inoltrate dal sistema ma non archiviate. Il NCSC non ha facoltà di accedere a queste informazioni.

Articolo 74g Obbligo d'informazione

L'obbligo d'informazione è limitato alle informazioni che servono per identificare il modello e il metodo di un ciberattacco per cui è stata inviata una notifica (preallerta) e, in questo modo, a evitare che il ciberattacco abbia ripercussioni anche su altre infrastrutture critiche.

Articolo 74h Violazione dell'obbligo di notifica o d'informazione

Capoverso 1

In caso di violazione dell'obbligo di notifica o d'informazione, inizialmente il NCSC informa il gestore dell'infrastruttura critica, dandogli così nuovamente la possibilità di assolvere i propri doveri. Inoltre, nel caso vi fossero dei malintesi, è possibile chiarirli. Il NCSC è tenuto a questa prima informazione perché è un requisito per l'emanazione della decisione di cui al capoverso 2.

Capoverso 2

Se, nonostante l'evidente violazione dei propri obblighi, il gestore non prende alcun provvedimento, il NCSC emana in un secondo tempo una decisione con comminatoria della pena. Nella sua decisione il NCSC specifica quali obblighi sono stati violati in modo tale che il gestore dell'infrastruttura critica non abbia dubbi su cosa debba fare od omettere. In più, in questo modo si facilita anche il lavoro delle autorità di perseguimento penale che, in caso di inosservanza di questa decisione devono condurre indagini sui fatti denunciati dal NCSC ed emettere una sentenza o un decreto d'accusa (cfr. articolo 74*i*).

Articolo 74i Infrazioni contro le decisioni del NCSC

Questo articolo riprende in gran parte le regole stabilite all'articolo 63 e seguenti nLPD in caso di mancato rispetto delle decisioni del NCSC da parte dell'impresa. Come viene spiegato nel messaggio concernente la legge sulla protezione dei dati rivista[35], anche in questo caso è passibile di pena la persona che all'interno dell'infrastruttura critica avrebbe dovuto preoccuparsi di dare seguito alla decisione del NCSC (cfr. art. 29 CP[36]). L'obbligo violato che incombe all'impresa è imputato alla persona fisica. Il rimando all'articolo 6 della legge federale del 22 marzo 1974[37] sul diritto

35 Messaggio del 15.9.2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati, FF **2017** 5939, 5976, 6088 seg.
36 RS **311.0**
37 RS **313.0**

penale amministrativo indica la responsabilità penale della dirigenza dell'impresa, quindi dei dirigenti e delle persone autorizzate a prendere decisioni e dare istruzioni. In questo modo è possibile definire in modo chiaro su chi ricade la responsabilità penale all'interno delle infrastrutture critiche.

Capoverso 1

L'importo massimo della multa è stato fissato a 100 000 franchi, per tenere debitamente conto del significato delle infrastrutture critiche per il corretto funzionamento dell'economia e dello Stato e per sottolineare la loro responsabilità per la garanzia della cibersicurezza di questi ultimi. L'importo massimo della multa è giustificato anche dal fatto che questa rappresenta l'ultima ratio e viene comminata solo dopo che una serie di altre misure non ha portato alcun risultato. Tenuto conto dei diversi livelli di cibersicurezza nei singoli settori e dei requisiti aggiuntivi imposti con il nuovo obbligo di notifica di ciberattacchi, si è deliberatamente evitato di riprendere il limite massimo della multa pari a 250 000 franchi previsto dalla legge sulla protezione dei dati rivista. La minaccia di una multa di 100 000 franchi dovrebbe essere sufficiente per spingere i responsabili delle infrastrutture critiche a un comportamento conforme agli obblighi previsti.

Capoversi 2 e 3

Per la comminazione della multa alle imprese è stato ripreso per analogia il regolamento della legge sulla protezione dei dati rivista (art. 64 nLPD). Nel caso l'importo non superi i 20 000 franchi, la multa quindi può essere comminata direttamente all'infrastruttura critica piuttosto che alla persona fisica responsabile, in modo da evitare impegnative attività di indagine. Tenuto conto del fatto che l'importo massimo è di 100 000 franchi, per questi «casi di minore importanza» l'ammontare della multa è stato fissato a 20 000 franchi per richiamare al dovere le infrastrutture critiche in quanto tali ed evitare ulteriori indagini sui responsabili. Se si considera che l'obbligo di notifica riguarda principalmente le infrastrutture critiche più significative, che in molti casi possiedono anche quote di mercato corrispondenti, non vi è motivo di ridurre l'importo massimo fissato a 20 000 franchi.

Capoverso 4

Per motivi di trasparenza al capoverso 4, analogamente all'articolo 65 nLPD, si specifica che, in caso di inosservanza di una decisione del NCSC, sono responsabili le autorità cantonali di perseguimento penale. Si è deciso di non menzionare il diritto del NCSC di presentare denuncia perché risulta evidente dal contesto.

Sezione 3: Protezione dei dati e scambio di informazioni

Gli articoli dal 75 al 79, ora inseriti all'interno della sezione 3, sono stati adeguati sia dal punto di vista linguistico che dal punto di vista dei contenuti per essere in linea con la definizione a livello di legge dei compiti del NCSC. Il NCSC ha preso il posto di MELANI, la centrale gestita congiuntamente dall'Organo direzione informatica della Confederazione (ODIC) e dal SIC. Poiché il SIC ha il mandato legale di valutare la situazione di minaccia e di assicurare un servizio di preallerta per i gestori di infrastrutture critiche, la collaborazione del NCSC con il SIC e l'inoltro di informazioni e dati devono essere disciplinati, laddove necessario, nella LSIn.

Articolo 75 Trattamento di dati personali

Capoverso 1

Al posto di una descrizione generica dei servizi federali responsabili, è stato inserito il NCSC, spiegando che può trattare non soltanto dati personali, ma anche dati personali degni di particolare protezione collegati a elementi di indirizzo. Ai sensi dell'articolo 3 lettera f LTC l'elemento di indirizzo è una «sequenza di cifre, lettere o segni, oppure altre informazioni che permettono di identifi-

care le persone, i processi informatici, le macchine, gli apparecchi o gli impianti di telecomunicazione che partecipano a un processo di comunicazione mediante telecomunicazione». Alla *lettera a* è stato inserito il termine «cibersicurezza».

Capoverso 2

Il capoverso 2 riprende sostanzialmente il precedente capoverso 3, riformulandolo dal passivo all'attivo, chiarendo così che i dati vengono trattati dal NCSC. Inoltre sono stati specificati i presupposti che devono essere soddisfatti quando la persona interessata non viene informata del trattamento dei dati.

Capoverso 3

Al capoverso 3 viene precisato che le persone i cui elementi di indirizzo sono utilizzati senza autorizzazione devono esserne informate.

Articolo 76 Cooperazione a livello nazionale

Questo articolo costituisce la base legale per lo scambio di informazioni tra il NCSC e i gestori di infrastrutture critiche (cpv. 1 e 2) nonché tra il NCSC e i fornitori di servizi di telecomunicazione (cpv. 3 e 4).

Inoltre sono state apportate modifiche formali. Ad esempio, in ogni capoverso è stato specificato che la collaborazione è consentita purché sia necessaria per proteggere le infrastrutture critiche da ciber-rischi.

Capoversi 1 e 2

Lo scambio di informazioni tra il NCSC e i gestori di infrastrutture critiche disciplinato al capoverso 1 non è riservato soltanto alle infrastrutture critiche sottoposte all'obbligo di notifica, ma è rivolto a tutte le infrastrutture critiche interessate con sede in Svizzera.

Capoversi 3 e 4

Lo scambio di informazioni tra il NCSC e i fornitori di servizi di telecomunicazione viene disciplinato esplicitamente ai capoversi 3 e 4 perché sebbene la maggior parte lo siano, non tutti i fornitori di servizi di telecomunicazione sono considerati infrastrutture critiche.

Articolo 76a Sostegno alle autorità

Questa è una disposizione nuova che disciplina quali informazioni il NCSC può mettere a disposizione di altre autorità, in quale misura e a quale scopo. In particolare definisce il contenuto e l'entità nonché il tipo e le modalità dello scambio di informazioni operato dal NCSC con il SIC, le autorità di perseguimento penale e i servizi cantonali competenti per la cibersicurezza (cpv. 2-4). Un aspetto importante della collaborazione tra il NCSC e queste autorità è lo scambio di informazioni sugli hacker stessi e sui metodi e le tattiche che utilizzano.

Capoverso 1

Nel primo capoverso di questo articolo, al contrario di quanto disposto nei capoversi successivi, non viene disciplinato lo scambio reciproco di informazioni, ma viene sancito il principio in base al quale il NCSC deve aiutare il SIC nello svolgimento dei suoi compiti con specifiche valutazioni sul numero, sul tipo e sulla portata dei ciberattacchi nonché con analisi tecniche dei ciber-rischi. Questo «quadro della situazione» non contiene dati personali o informazioni concreti o specifici, ma si limitano a fornire valutazioni statistiche e tecniche necessarie per la valutazione della situazione di minaccia e per assicurare il servizio di preallerta. Ai sensi dell'articolo 6 capoverso 2 LAIn il SIC è responsabile della valutazione della situazione di minaccia. Attraverso il servizio di notifica e l'obbligo di notifica il NCSC dispone di una fonte di informazioni importante in merito alla situazione di

minaccia provocata da ciberincidenti. Pertanto è in grado di inoltrare al SIC informazioni su numero, tipo e portata dei ciberattacchi, di fornirgli supporto attraverso analisi tecniche degli attacchi e inoltrargli le informazioni ottenute da queste analisi.

Capoversi 2, 3 e 4

Nei capoversi dal 2 al 4 vengono disciplinati il contenuto e l'entità nonché il tipo e le modalità dello scambio di informazioni operato tra NCSC e SIC, autorità di perseguimento penale e servizi cantonali per la cibersicurezza. Come già accennato, un aspetto importante della collaborazione tra il NCSC e queste autorità è lo scambio di informazioni sugli hacker stessi e sui metodi e le tattiche che utilizzano. Queste informazioni possono essere di natura puramente tecnica (ad es. modello di attacco e valori di hash di malware) e non contenere dati personali. Queste autorità, però, si scambiano anche informazioni con riferimenti personali o che permettono di risalire all'identità di una persona. Per questi casi viene quindi definita una base legale. Concretamente si tratta di elementi di indirizzo (come nome di dominio, indirizzo IP, indirizzi e-mail utilizzati indebitamente) o informazioni su transazioni finanziarie (conti bancari, numeri IBAN, ecc.).

Le autorità autorizzate ai sensi dei capoversi dal 2 al 4 possono accedere alle suddette informazioni anche mediante procedura di richiamo, indicata dato l'elevato numero di ciberattacchi e di informazioni tecniche correlate. L'inoltro delle notifiche al SIC o alle autorità di perseguimento penale con le informazioni sui soggetti interessati avviene soltanto in casi eccezionali e rimane vincolato alle condizioni di cui all'articolo 73*c* capoversi 1 e 2.

Articolo 77 Cooperazione a livello internazionale

Questa disposizione è stata adeguata dal punto di vista formale inserendo esplicitamente un riferimento al NCSC. Inoltre il termine «dati» è stato sostituito dall'iperonimo «informazioni» quando non ci si riferisce in modo specifico ai dati personali ai sensi dell'articolo 75. Per quanto riguarda l'entità, il contenuto e lo scopo dello scambio di informazioni, al fine di fornire maggiori dettagli è stato aggiunto che è consentito con servizi responsabili per la cibersicurezza. All'interno del *capoverso 1* la formula «per la protezione di infrastrutture critiche» è stata sostituita con «per la cibersicurezza» in quanto la prima era troppo limitante per le organizzazioni che operano a livello internazionale nell'ambito della cibersicurezza.

Articolo 78 Sistema d'informazione per il sostegno alle infrastrutture critiche

In applicazione delle modifiche alle basi legali sancite dalla revisione della LPD, questo articolo è stato abrogato. I fini per i quali il NCSC tratta i dati derivano dai suoi compiti, già sufficientemente descritti negli articoli elencati. Tali compiti indicano per quali scopi i sistemi d'informazione del NCSC possono essere utilizzati nel trattamento dei dati personali.

Articolo 79 Conservazione e archiviazione dei dati

Questo articolo è stato leggermente modificato solo al *capoverso 1*, dove viene specificato che i dati personali possono essere conservati al massimo per cinque anni dall'ultimo utilizzo. Questa regola viene stabilita perché determinate informazioni tecniche sui ciberincidenti come, ad esempio, nomi di dominio, indirizzi IP o indirizzi e-mail utilizzati in modo improprio, sono molto importanti per effettuare un confronto con i nuovi ciberincidenti segnalati e per l'analisi dei metodi e dei modelli di attacco. Senza questi dati di confronto il NCSC non può condurre in modo mirato o non può condurre affatto le sue analisi, che costituiscono un requisito fondamentale per l'adempimento dei suoi compiti. Dal momento, però, che questi dati tecnici contengono anche dati personali e quindi, in quanto tali, sono sottoposti alla protezione dei dati, il periodo di conservazione deve essere chiaramente limitato. Sempre per motivi legati alla protezione dei dati, nella seconda parte del periodo viene specificato che i dati personali degni di particolare protezione possono essere conservati al massimo per due anni dall'ultimo utilizzo.

Articolo 80 Disposizioni del Consiglio federale

Questo articolo è stato abrogato. Con le concretizzazioni operate nel testo di legge, le deleghe al Consiglio federale previste in questa sezione sono divenute obsolete. L'emanazione delle disposizioni di esecuzione è di competenza del Consiglio federale anche senza riserva di legge. Inoltre le disposizioni di esecuzione di cui alla lettera c (responsabilità in materia di protezione e sicurezza dei dati) sono già introdotte dagli articoli 33 e 8 capoverso 3 nLPD.

Allegato 1 (Articolo 89 Modifica di altri atti normativi)

L'elenco delle modifiche ad altri atti normativi ai sensi dell'articolo 89 nell'allegato 1 è integrato come riportato di seguito.

Legge del 23 marzo 2007[38] *sull'approvvigionamento elettrico*

La protezione contro i ciber-rischi che si intende ora disciplinare esplicitamente nell'articolo 8*a* della legge sull'approvvigionamento elettrico serve a garantire la sicurezza di tale approvvigionamento. Le misure da attuare previste al capoverso 1 dovrebbero evitare ciberincidenti e, in particolare, guasti dei relativi impianti o comunque permetterne una risoluzione il più possibile rapida. L'obbligo riguarda non soltanto i gestori della rete, che attraverso le tecnologie di comando esercitano un controllo diretto sul funzionamento della rete, ma anche i produttori (ad es. i gestori di centrali eoliche o idroelettriche) e i gestori di impianti di stoccaggio, dal momento che controllando l'immissione e la vendita di energia possono influire in modo significativo sulla sicurezza dell'approvvigionamento. Per stabilire quali misure di protezione sono da considerare adeguate bisogna tenere conto di quanto il soggetto in questione influisce sulla sicurezza dell'approvvigionamento (ad es. livello di rete, prestazioni, numero di utenti finali interessati).

Il nostro Consiglio stabilirà direttive specifiche a livello di ordinanza, in particolare per quanto riguarda il livello di protezione e l'auditing. A tal fine potrà basarsi sulle normative del settore (ad esempio il manuale dell'Associazione delle aziende elettriche svizzere «Handbuch Grundschutz für *Operational Technology* in der Stromversorgung», edizione luglio 2018, attualmente in rielaborazione) che potrà anche dichiarare vincolanti. Per imprese e organizzazioni di dimensioni minori dovranno essere previste eccezioni o agevolazioni.

Tenuto conto dello scopo del nuovo *articolo 8*a, ai sensi del *capoverso 2* sono considerati come altri partecipanti soltanto ulteriori soggetti coinvolti che esercitano un influsso significativo sulla sicurezza dell'approvvigionamento, quindi fornitori di notevoli dimensioni nel settore dell'elettricità, che si occupano, ad esempio, di commercio, misurazione, controllo, flessibilità, trattamento dei dati o elettromobilità.

Modifica della legge federale del 25 settembre 2020[39] *sulla protezione dei dati*

Per fare in modo che l'IFPDT nel corso dell'analisi di una violazione della sicurezza dei dati, segnalatagli dal responsabile sulla base dell'articolo 24 nLPD e dell'articolo 19 dell'avamprogetto dell'ordinanza relativa alla LPD (AP-OLPD), possa coinvolgere gli esperti del NCSC, all'*articolo 24 capoverso 5*^{bis} LPD viene ora stabilito che l'IFPDT ha la facoltà di inoltrare la notifica di una violazione della sicurezza dei dati al NCSC.

La comunicazione inoltrata può contenere qualsiasi informazione ai sensi dell'articolo 19 capoverso 1 AP-OLPD, purché si tratti di dati necessari al NCSC per l'analisi dell'accaduto. Le informazioni trasmesse dall'IFPDT al NCSC possono contenere anche dati personali, compresi dati personali degni di particolare protezione relativi a procedimenti o sanzioni amministrativi e penali riguardanti il responsabile sottoposto all'obbligo di notifica. Le informazioni necessarie per l'analisi di un evento vengono selezionate caso per caso, ma vi è la possibilità che il NCSC riceva indirettamente informazioni su una procedura in corso. È quindi necessario creare una base giuridica per la comunicazione di dati personali degni di particolare protezione.

38 RS **734.7**
39 Legge federale del 25 settembre 2020 sulla protezione dei dati (LPD), FF **2020** 6695

In ogni caso è necessario che il responsabile obbligato a inviare la notifica all'IFPDT abbia precedentemente fornito il suo consenso all'inoltro. Inoltre la trasmissione delle informazioni non deve essere un modo per aggirare quanto disposto dall'articolo 24 capoverso 6 nLPD in base al quale la notifica può essere utilizzata nel quadro di un procedimento penale soltanto con il consenso della persona obbligata alla notifica. Il nuovo capoverso 5bis dell'articolo 24 nLPD non consente l'inoltro sistematico delle notifiche da parte dell'IFPDT al NCSC. L'IFPDT, infatti, è autorizzato a fare ricorso a questa possibilità solo in singoli casi, quando sono necessarie le competenze tecniche del NCSC per effettuare indagini su un determinato caso.

5 Ripercussioni

5.1 Ripercussioni per la Confederazione

Il NCSC gestisce già oggi un servizio di contatto che raccoglie le segnalazioni volontarie di ciberincidenti. Tale servizio basa la sua attività sulla pluriennale esperienza maturata con MELANI, la centrale che dal 2004 ha raccolto in particolare le segnalazioni trasmesse da infrastrutture critiche.

Per la raccolta delle segnalazioni il NCSC gestisce già oggi un modulo elettronico che può essere adattato per poter raccogliere anche quelle inviate per assolvere l'obbligo di notifica. All'inizio l'armonizzazione necessaria con gli altri servizi che già raccolgono segnalazioni di questo tipo (ad es. IFPDT, FINMA, IFSN) e la configurazione del modulo di notifica richiederanno del lavoro aggiuntivo, che potrà però essere coperto con le risorse già a disposizione del NCSC. Per la successiva gestione, però, il NCSC deve poter garantire che le notifiche inviate in adempimento all'obbligo di notifica vengano registrate, quietanzate e documentate correttamente e che vengano inoltrate al giusto servizio ai fini della preallerta, un impegno ulteriore di cui si dovrà tenere conto in fase di potenziamento del NCSC.

Il Centro nazionale per la cibersicurezza in futuro avrà anche il compito di fornire supporto all'infrastruttura critica interessata per la gestione dell'incidente, un servizio già fornito e ben rodato grazie alla pluriennale esperienza maturata dal NCSC (e prima ancora da MELANI) ma che sicuramente dopo l'introduzione dell'obbligo di notifica richiederà un impegno maggiore. Questo perché molto probabilmente il NCSC riceverà più notifiche e, in più, sarà anche tenuto a fornire almeno una prima valutazione e raccomandazioni su come contrastare l'attacco. Di conseguenza anche il team del NCSC addetto all'analisi tecnica (GovCERT) dovrà essere potenziato.

Questo maggior impegno dovrà quindi essere preso in considerazione nel corso degli attuali lavori di potenziamento del NCSC. Al momento, però, non è possibile valutarlo in modo completamente distaccato dagli altri compiti del NCSC; si sta quindi aspettando il risultato della verifica ancora in corso dell'efficacia dell'organizzazione del settore della cibersicurezza in seno alla Confederazione. Alla luce del risultato della presente procedura di consultazione il fabbisogno di risorse verrà concretizzato nel messaggio concernente la modifica della LSIn.

5.2 Ripercussioni per i Cantoni e i Comuni

Con questo progetto non verranno assegnati nuovi compiti ai Cantoni e ai Comuni, ma essi sono comunque toccati dall'obbligo di notifica per due motivi. In primo luogo perché le autorità cantonali e comunali sono esse stesse soggette all'obbligo di notifica ai sensi dell'articolo 74b lettera b e, in secondo luogo, perché molte delle imprese soggette all'obbligo di notifica sottostanno a enti cantonali o comunali.

Cantoni e Comuni, però, potranno anche approfittare dei servizi offerti dal NCSC per potersi proteggere meglio dai ciber-rischi. Già oggi numerosi Cantoni e città partecipano allo scambio di informazioni tra infrastrutture critiche e NCSC.

5.3 Ripercussioni sull'economia e sulla società

Non sono attese ripercussioni dirette sull'economia nazionale, sulla società e sull'ambiente. Tuttavia economia nazionale e società trarranno indirettamente beneficio dall'introduzione dell'obbligo di notifica di ciberattacchi, in quanto il miglioramento della cibersicurezza delle infrastrutture critiche permetterà anche di proteggere meglio la cibersicurezza in Svizzera. L'obbligo di notifica, inoltre, grazie all'attuazione tempestiva di misure preventive e di difesa adeguate, permetterà di evitare che ciberattacchi a infrastrutture critiche provochino malfunzionamenti e guasti di servizi essenziali che metterebbero a rischio il corretto funzionamento dell'economia e dello Stato.

L'introduzione dell'obbligo di notifica di ciberattacchi a infrastrutture critiche avrà ripercussioni minime se non nulle sull'economia nazionale e sulle imprese interessate, pertanto è possibile fare a meno di un'analisi d'impatto della regolamentazione (AIR).

L’obbligo di notifica aiuta a fare luce sulla minaccia rappresentata dai ciberattacchi e contribuisce a sensibilizzare la popolazione sui ciber-rischi. Una maggiore competenza della popolazione in questo ambito è un requisito importante per il successo della digitalizzazione della società.

6 Aspetti giuridici

6.1 Costituzionalità

Nella Costituzione non è presente una base legale esplicita per l'introduzione di un obbligo di notifica di ciberattacchi. La Confederazione può quindi basarsi sulla sua competenza federale inerente per la tutela della sicurezza interna ed esterna della Confederazione per l'introduzione dell'obbligo di notifica di ciberattacchi a infrastrutture critiche.

Le infrastrutture critiche hanno un'elevata rilevanza per quanto riguarda la sicurezza della società, dell'economia e dello Stato. Le ripercussioni potenzialmente molto gravi e con effetti su tutto il territorio nazionale dei ciberattacchi a infrastrutture critiche mettono a rischio il benessere del Paese e rappresentano una minaccia per la sicurezza interna ed esterna. L'introduzione di un obbligo di notifica serve quindi a garantire la stabilità economica, sociale e statale e costituisce la base grazie alla quale è possibile coordinare e avviare tempestivamente azioni volte a contrastare gli attacchi. L'obbligo di notifica di ciberattacchi a infrastrutture critiche serve inoltre ad analizzare, attraverso le notifiche, la situazione di minaccia per poter preallertare e implementare misure di difesa. Dato lo scopo dell'obbligo di notifica, ne deriva che il suo campo di applicazione deve essere limitato ai ciberattacchi a infrastrutture critiche. Il diritto di chiunque di segnalare ciberincidenti e vulnerabilità, che integra altre strategie per la raccolta di informazioni, rappresenta un aiuto per la protezione delle infrastrutture critiche.

Di conseguenza, la competenza federale inerente per la garanzia della sicurezza interna ed esterna – competenze che non sono assegnate esplicitamente alla Confederazione, ma che le spettano in quanto Stato – costituisce una base costituzionale adeguata sulla base della quale introdurre disposizioni di legge che prevedono un obbligo di notifica di ciberattacchi e un diritto di notifica in caso di ciberincidenti e vulnerabilità.

Riguardo a questa competenza federale inerente, in base a quanto sancito da una convezione sulla tecnica legislativa formale[40] viene citato a titolo sussidiario l'articolo 173 capoverso 2 Cost. La legge sulla sicurezza delle informazioni cita nel suo ingresso, oltre agli articoli 54 capoverso 1, 60 capoverso 1, 101, 102 capoverso 1 e 173 capoverso 1 lettere a e b, anche l'articolo 173 capoverso 2 come fondamento costituzionale determinante. Pertanto non è necessario integrare le disposizioni costituzionali nell'ingresso della LSIn.

6.2 Compatibilità con gli impegni internazionali della Svizzera

L'introduzione dell'obbligo di notifica di ciberattacchi non tocca nessun impegno attuale della Svizzera a livello internazionale. Questo regolamento è simile a quelli che molti altri Stati, in particolare gli Stati membri dell'UE, hanno introdotto negli ultimi anni.

6.3 Forma dell'atto

Per l'introduzione dell'obbligo di notifica la base legale ideale sembra essere un'integrazione della LSIn già approvata, non soltanto perché lo scopo, l'oggetto e l'ambito di applicazione sono fondamentalmente compatibili con l'obbligo di notifica per infrastrutture critiche, ma anche perché costituisce la base legale formale per l'istituzione del NCSC come servizio di notifica. Dal punto di vista sistematico l'obbligo di notifica di ciberattacchi e i compiti del NCSC per quanto riguarda la tutela della cibersicurezza possono essere inseriti nel capitolo 5.

Per quanto riguarda le disposizioni di esecuzione dell'obbligo di notifica deve essere ancora deciso se sarà necessario creare un'ordinanza a parte o se verrà integrata l'attuale ordinanza sui ciberrischi.

40 N. marg. 25 delle Direttive di tecnica legislativa, www.bk.admin.ch > Documentazione > Accompagnamento legislativo > Direttive di tecnica legislativa DTL

6.4 Subordinazione al freno alle spese

Con il progetto non vengono introdotte nuove disposizioni in materia di sussidi (che comportano uscite superiori a uno dei valori soglia) né decisi nuovi crediti d'impegno o limiti di spesa (con uscite superiori a uno dei valori soglia).

6.5 Rispetto del principio di sussidiarietà e del principio dell'equivalenza fiscale

Nell'assegnazione e nell'adempimento dei compiti statali va osservato il principio della sussidiarietà (art. 5*a* Cost.). Ai sensi dell'articolo 43*a* capoverso 1 Cost. la Confederazione assume unicamente i compiti che superano la capacità dei Cantoni o che esigono un disciplinamento uniforme da parte sua. Nel contempo la Confederazione deve fare ricorso in modo moderato alle sue competenze, lasciando ai Cantoni un margine sufficiente per l'adempimento dei loro compiti.

Un obbligo di notifica di ciberattacchi a infrastrutture critiche non può essere attuato in modo efficace se non è valido su tutto il territorio nazionale e in tutti i settori. Senza una procedura di notifica uguale per tutti e un servizio di notifica centrale, non sarebbe possibile contrastare i ciberattacchi che si verificano senza tenere conto dei confini geografici e settoriali. In base alla competenza costituzionale della Confederazione, l'obbligo di notifica è stato limitato ai ciberattacchi a infrastrutture critiche, in quanto le loro ripercussioni possono rappresentare una minaccia per la sicurezza del Paese e per il corretto funzionamento dello Stato. L'introduzione dell'obbligo di notifica rappresenta quindi una misura compatibile con il principio di sussidiarietà (art. 5*a* in combinato disposto con l'art. 43*a* Cost.).

Secondo il principio dell'equivalenza fiscale sancito all'articolo 43*a* capoversi 2 e 3 Cost., la collettività che fruisce di una prestazione statale ne assume i costi e la collettività che assume i costi di una prestazione statale può decidere in merito a questa prestazione. In relazione all'introduzione dell'obbligo di notifica questo principio è garantito in quanto i costi per la gestione del servizio centrale di notifica saranno a carico della Confederazione. Per le infrastrutture critiche cambierà poco con l'introduzione dell'obbligo di notifica, perché, come in passato, potranno contare sul supporto del NCSC per la gestione degli incidenti. Rispetto alla segnalazione volontaria di ciberincidenti, l'obbligo di notifica richiede un impegno maggiore ma comunque limitato. Pertanto anche le infrastrutture critiche gestite dai Cantoni e dai Comuni non dovranno sostenere dei reali costi aggiuntivi a seguito dell'introduzione dell'obbligo di notifica.

6.6 Delega di competenze legislative

Secondo il presente progetto posto in consultazione, i principi fondamentali per l'introduzione dell'obbligo di notifica di ciberattacchi devono essere sanciti a livello di legge.

Il nostro Consiglio, inoltre, emetterà disposizioni di esecuzione per concretizzare le disposizioni di legge, se necessario. In particolare, ai sensi dell'articolo 74*c* al nostro Collegio spetta il compito di restringere ulteriormente la cerchia degli assoggettati all'obbligo di notifica. La legge stabilisce i criteri da applicare ma il nostro Consiglio dovrà stabilire quali criteri devono essere applicati per ogni settore e con quali modalità (ad esempio attraverso la definizione di valori di soglia adeguati).

6.7 Protezione dei dati

Il progetto posto in consultazione ha sostanzialmente ripreso senza modifiche le disposizioni in materia di protezione dei dati così come approvate originariamente dal Parlamento nel capitolo 5 LSIn in relazione al supporto per le infrastrutture critiche.

Durante l'elaborazione del progetto posto in consultazione è stato consultato l'IFPDT. In questa fase si è discusso anche delle possibilità di coordinamento con l'obbligo di notifica in caso di violazione della sicurezza dei dati.