Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FF 2023
www.fedlex.admin.ch
La versione elettronica firmata
è quella determinante

22.073

Messaggio concernente la modifica della legge sulla sicurezza delle informazioni

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

del 2 dicembre 2022

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di modifica della legge sulla sicurezza delle informazioni per introdurre l'obbligo di segnalare ciberattacchi a infrastrutture critiche.

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

2 dicembre 2022

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Ignazio Cassis
Il cancelliere della Confederazione, Walter Thurnherr

Compendio

Situazione iniziale

Negli ultimi anni sempre più spesso privati, imprese e autorità sono stati vittime di ciberincidenti che, in alcuni casi, hanno avuto conseguenze gravi.

L'11 dicembre 2020 il Consiglio federale ha incaricato il Dipartimento federale delle finanze di creare basi legali per introdurre l'obbligo di segnalare ciberattacchi a infrastrutture critiche.

Grazie all'obbligo di segnalazione è possibile individuare per tempo i ciberattacchi, analizzarne i modelli di attacco e avvertire tempestivamente altri gestori di infrastrutture critiche. Tale obbligo può quindi contribuire in modo significativo ad aumentare la cibersicurezza in Svizzera. Il 12 gennaio 2022 il Consiglio federale ha aperto la consultazione sull'avamprogetto. I relativi risultati sono stati inseriti nel presente messaggio.

Contenuto del disegno

Il presente disegno definisce non soltanto l'obbligo di segnalare ciberattacchi a infrastrutture critiche, ma disciplina a livello di legge anche i compiti del Centro nazionale per la cibersicurezza (NCSC) istituito nel 2019. In particolare, il disegno stabilisce la funzione dell'NCSC quale servizio centrale per la segnalazione di ciberincidenti, che riceve altresì segnalazioni su base volontaria relative a ciberincidenti e vulnerabilità nei mezzi informatici.

L'obbligo di segnalazione viene introdotto per i ciberattacchi contro infrastrutture critiche provocati intenzionalmente da persone non autorizzate. Vanno segnalati unicamente i ciberattacchi che hanno conseguenze gravi, perché ad esempio compromettono il funzionamento di infrastrutture critiche.

Indice

Messaggio

1 Situazione iniziale

L'introduzione di un obbligo di segnalare ciberattacchi è stata al centro di ripetute discussioni. L'argomento ha acquisito ulteriore importanza perché l'Unione europea (UE), con l'adozione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016[1], recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (di seguito «direttiva NIS»), ha introdotto un obbligo di notificare ciberattacchi. In diverse fasi, il nostro Consiglio ha verificato se l'introduzione di un siffatto obbligo fosse necessaria e attuabile anche per la Svizzera e, sulla base dei risultati di tali verifiche, ha deciso di elaborare un progetto.

1.1 Necessità di agire e obiettivi

Nel nostro rapporto del 13 dicembre 2019 in adempimento del postulato 17.3475 «Obbligo di segnalazione di gravi incidenti legati alla sicurezza delle infrastrutture critiche», abbiamo constatato che in Svizzera non esiste alcun obbligo di segnalare ciberincidenti nelle infrastrutture critiche.[2] Ha pertanto conferito al Centro nazionale per la cibersicurezza (NCSC) il mandato di verificare la possibilità di introdurre un obbligo di questo tipo.

Questo mandato di verifica trovava fondamento in vari documenti precedenti, tra cui la strategia nazionale per la protezione delle infrastrutture critiche 2018–2022 (strategia PIC, misura 8), 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[3]. Inoltre, la questione dell'obbligo di segnalazione è stata affrontata anche nel corso dei dibattiti parlamentari sulla revisione totale della legge federale del 20 dicembre 2019 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 giugno 2020). Dopo un'approfondita verifica delle possibili basi legali e, in particolare, della competenza federale[4], l'11 dicembre 2020 il nostro Collegio ha

1 GU L 194 del 19 luglio 2016, pag. 1.
2 Rapporto del Consiglio federale del 13 dicembre 2019 in adempimento del postulato 17.3475 depositato il 15 giugno 2017 dalla consigliera nazionale Graf-Litscher sulle varianti per l'attuazione di un obbligo di notifica in caso di gravi incidenti legati alla sicurezza delle infrastrutture critiche (in tedesco e francese).
3 Rapporto del gruppo di esperti del 17 agosto 2018 per il futuro del trattamento e della sicurezza dei dati (raccomandazione 28). Il gruppo di esperti è stato istituito dal Dipartimento federale delle finanze il 27 agosto 2015 per tre anni in adempimento della mozione 13.3841 «Commissione di esperti per il futuro del trattamento e della sicurezza dei dati», depositata il 26 settembre 2013 dal consigliere agli Stati Rechsteiner.
4 Rapporto «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen» del 25 novembre 2020, allegato 01 alla proposta del Consiglio federale dell'11 dicembre 2020.

incaricato il Dipartimento federale delle finanze (DFF) di elaborare, entro la fine del 2021, un progetto concernente l'introduzione dell'obbligo di segnalare 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 è stato appurato che l'NCSC, istituito nel 2019 e che nel progetto viene designato come servizio centrale di segnalazione di ciberattacchi, non disponeva delle basi legali necessarie per assumere i propri compiti in qualità di centro di competenza della Confederazione per la cibersicurezza così come richiesto dal Parlamento[5]. Con il progetto sull'introduzione dell'obbligo di segnalazione, anche i compiti e le competenze dell'NCSC devono quindi essere disciplinati a livello di legge.

1.2 Alternative esaminate e opzione scelta

L'introduzione di un obbligo di segnalazione è uno strumento efficace e diretto per garantire che le informazioni su ciberattacchi siano trasmesse a un servizio centrale specializzato. Tuttavia, non è privo di alternative. È stato esaminato in quale misura il potenziamento dello scambio volontario di informazioni possa portare a risultati altrettanto efficaci e se sia possibile, anziché introdurre un nuovo obbligo di segnalazione, estendere gli obblighi esistenti in modo tale da coprire anche i ciberattacchi.

Posto che entrambe le alternative non rappresentano una soluzione soddisfacente, si prevede l'introduzione di un obbligo di segnalazione. Questo deve essere applicato con l'aiuto di incentivi e sanzioni.

1.2.1 Alternativa: 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 l'NCSC. Questo modello, però, sta dimostrando sempre di più i propri limiti. Per fare in modo che lo scambio reciproco funzioni è necessario un rapporto di fiducia, 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, visto 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 rapporti di fiducia sufficiente con tutti gli interessati. Negli ultimi anni, quindi, lo scambio di informazioni è andato limitandosi a una cerchia circoscritta di imprese e organizzazioni con le quali vi era un rapporto di collaborazione già ben consolidato. Tuttavia, a causa dell'elevato numero di infrastrutture critiche esposte a ciberminacce, non è più realistico pensare di estendere questo modello.

5 Mozione 17.3508 «Creazione di un centro di competenza per la cyber-sicurezza a livello di Confederazione», depositata il 16 giugno 2017 dal consigliere agli Stati Eder.

Data la natura volontaria delle segnalazioni, l'attenzione a poche società che effettuano segnalazioni può portare a un quadro incompleto o addirittura distorto della situazione. Non è possibile stabilire quali effetti stia scatenando in Svizzera quale minaccia informatica. Inoltre, lo scambio su base volontaria può condurre anche a incentivi sbagliati. Le imprese che non partecipano allo scambio di informazioni ricevono comunque avvertimenti e indicazioni di carattere tecnico grazie alle segnalazioni degli altri, perché l'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 informazioni importanti, 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 segnalazione, perché consentirebbe di avere una panoramica completa della situazione e garantire che nessuno possa sottrarsi all'obbligo di preallerta reciproca. Sarebbe tuttavia opportuno proseguire la collaborazione e i rapporti di fiducia reciproca sviluppati attraverso lo scambio di informazioni. In questo senso l'elemento determinante sarà la possibilità, per le imprese e le organizzazioni, di ottenere anche un valore aggiunto dall'introduzione dell'obbligo di segnalazione.

1.2.2 Alternativa: potenziamento di obblighi di segnalazione esistenti e scambio di informazioni tra le autorità

In alternativa all'introduzione di un nuovo obbligo, è stata valutata la possibilità di ancorare l'obbligo di segnalare ciberattacchi ai pertinenti obblighi già esistenti, evitando di introdurne uno nuovo a livello intersettoriale. Questa opzione è stata scartata perché le normative sugli incidenti di sicurezza nei vari settori non sono omogenee e spesso non esistono affatto. Lo sforzo di integrare e coordinare gli obblighi esistenti e di regolare ulteriormente lo scambio di informazioni tra le autorità interessate sarebbe stato maggiore rispetto all'introduzione di un nuovo obbligo di segnalazione e avrebbe portato a processi inefficienti.

Occorre inoltre considerare che l'obbligo di segnalare ciberattacchi non sostituisce gli altri obblighi in vigore, ma li completa. Si è anche cercato di fare in modo che le basi legali permettano di adempiere contemporaneamente a più di un obbligo di segnalazione. L'impegno richiesto per assolvere diversi obblighi, infatti, dovrebbe essere il minore possibile, in particolare, ma non soltanto, rispetto all'obbligo di segnalare violazioni della sicurezza dei dati secondo l'articolo 24 della riveduta legge federale del 25 settembre 2020[6] sulla protezione dei dati (nLPD), perché spesso i ciberattacchi provocano anche una perdita di dati. La soluzione scelta permette ai segnalanti di inoltrare la segnalazione del ciberattacco, o di parti di essa, anche ad altri servizi simili nel momento in cui la trasmettono all'NCSC, adempiendo così contemporaneamente

6 RS **235.1**, RU **2022** 491

a più obblighi di segnalazione. Ciò dovrebbe impedire che gli interessati segnalino lo stesso incidente a diversi servizi tramite procedure differenti.

Quando imprese e organizzazioni segnalano all'NCSC un ciberattacco su base volontaria o per adempiere un obbligo, devono sapere come sarà trattata la loro segnalazione e chi riceverà queste informazioni. Anche qui permangono i principi su cui si basava il precedente modello dello scambio di informazioni con MELANI: per poter inoltrare le segnalazioni o parti di esse, l'NCSC necessiterà pertanto del consenso della persona interessata oppure tali informazioni dovranno essere rese anonime (cfr. art. 73*d* cpv. 1 del disegno [D-LSIn]).

Tuttavia, in due casi l'NCSC deve poter inoltrare informazioni che permettono di risalire al segnalante o alla persona interessata anche senza il suo consenso. Primo caso: l'inoltro di informazioni alle autorità di perseguimento penale sarà possibile se la segnalazione contiene informazioni relative a un reato grave. Questo vale quindi solo in casi eccezionali, perché i collaboratori dell'NCSC non sono in linea di principio tenuti a osservare l'obbligo di denuncia di cui all'articolo 22*a* della legge del 24 marzo 2000[7] sul personale federale (LPers). Il direttore dell'NCSC può inoltrare informazioni alle autorità di perseguimento penale se lo ritiene necessario in considerazione della gravità del reato (cfr. art. 73*d* cpv. 3 D-LSIn).

Secondo caso: l'inoltro di informazioni sarà ammesso se riguarda informazioni utili al Servizio delle attività informative della Confederazione (SIC) che servono a individuare tempestivamente e sventare minacce per la sicurezza interna o esterna, valutare la situazione di minaccia o assicurare il servizio di preallerta informativa ai fini della protezione di infrastrutture critiche ai sensi dell'articolo 6 capoversi 1 lettera a, 2 e 5 della legge federale del 25 settembre 2015[8] sulle attività informative (LAIn). Ciò assicura che il SIC, quale autorità competente per il servizio di preallerta informativa per la protezione di infrastrutture critiche e per la valutazione della situazione di minaccia, riceva informazioni importanti e rilevanti per la sicurezza (art. 73*d* cpv. 2 D-LSIn).

1.2.3 Applicazione dell'obbligo di segnalazione mediante incentivi e sanzioni

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

In primo luogo la segnalazione deve poter essere redatta nel modo più facile possibile. L'NCSC soddisfa questo requisito mettendo a disposizione un modulo elettronico che consente di registrare rapidamente la segnalazione e di inviarla in modo semplice.

In secondo luogo è necessario che vi siano degli incentivi a segnalare, che consistono principalmente nella valutazione tecnica e nel sostegno sussidiario offerti dall'NCSC per contrastare l'attacco. Gli incentivi devono essere intesi come un servizio di pronto

7 RS **172.220.1**
8 RS **121**

intervento e non devono avere una portata tale da entrare in concorrenza con altre prestazioni di servizi disponibili sul mercato. Per gli interessati tuttavia può essere molto utile poter contare su un servizio federale che abbia una panoramica completa sulla situazione di minaccia e che possa fornire aiuto e sostegno per una valutazione iniziale e per l'adozione di misure immediate. Le autorità e le organizzazioni assoggettate all'obbligo di segnalazione (di seguito «le autorità e le organizzazioni assoggettate») hanno diritto a questo sostegno nel momento in cui adempiono tale obbligo.

In terzo luogo, un fattore che influisce sulla disponibilità ad assolvere l'obbligo sono i deterrenti, ovvero le multe. Se, nonostante una richiesta e un confronto con l'infrastruttura critica, si dovesse arrivare comunque a una violazione dell'obbligo di segnalazione, è necessario prevedere la possibilità di sanzionare tale comportamento.

In alternativa alla multa, sarebbe stato possibile citare pubblicamente gli enti inadempienti. Questa alternativa è stata tuttavia scartata perché non favorirebbe una cooperazione basata sulla fiducia tra le autorità e le organizzazioni assoggettate e l'NCSC. Un'altra opzione potrebbe essere quella di rifiutare di sostenere gli inadempienti nella gestione degli incidenti. Neppure questa alternativa è però praticabile sotto il profilo della politica di sicurezza, in quanto potrebbe avere gravi ripercussioni sull'economia e sulla società.

Pertanto, rimane solo la possibilità che l'NCSC, come ultima ratio, possa emanare una decisione indicando la comminatoria della multa. Proponiamo un importo massimo della multa pari a 100 000 franchi, di cui 20 000 franchi al massimo potranno essere addossati direttamente all'impresa che gestisce l'infrastruttura critica. Dato il lungo e consolidato rapporto di collaborazione con le infrastrutture critiche, il nostro Consiglio ritiene che questa disposizione abbia principalmente un valore simbolico e che serva soprattutto a conferire all'obbligo di segnalazione la necessaria considerazione.

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[9] sul programma di legislatura 2019–2023 e nel decreto federale del 21 settembre 2020[10] 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 delle TIC. L'articolo 19 del decreto federale sul programma di legislatura stabilisce quanto segue all'obiettivo 18: «la Confederazione affronta i ciber-rischi e sostiene e adotta provvedimenti volti a proteggere la cittadinanza e le infrastrutture critiche». Inoltre, sia nel messaggio che nel decreto federale summenzionati si rimanda alla Strategia nazionale del 18 aprile 2018 per la protezione della Svizzera contro i cyber-rischi 2018–2022 e al relativo piano di attuazione.

9 FF **2020** 1565, in particolare 1653.
10 FF **2020** 7365, in particolare 7372.

Nel preventivo 2022[11] con piano integrato dei compiti e delle finanze 2023–2025, il miglioramento della cibersicurezza a livello di Confederazione e nazionale viene definito quale priorità strategica e l'obbligo di segnalazione è menzionato tra gli affari. Inoltre, viene sottolineato che l'NCSC contribuisce attivamente alla protezione della Svizzera contro i ciber-rischi.

2 Procedura di consultazione

2.1 Testo sottoposto a consultazione

Il 12 gennaio 2022 il Consiglio federale ha preso atto dell'avamprogetto (AP-LSIn) e del rapporto esplicativo e ha incaricato il DFF di condurre una procedura di consultazione. L'avamprogetto modifica il capitolo 5 della LSIn, che contiene già disposizioni sulla cibersicurezza delle infrastrutture critiche. Oltre alle modifiche della LSIn, prevede anche modifiche della LPD[12], della legge del 23 marzo 2007[13] sull'approvvigionamento elettrico (LAEl) e della legge federale del 21 giugno 2019[14] sugli appalti pubblici (LAPub).

Nelle disposizioni generali (sezione 1) sono definiti i compiti della Confederazione nella protezione dalle ciberminacce a livello di legge. Con la creazione dell'NCSC, nell'ambito delle decisioni sull'organizzazione della Confederazione in materia di ciber-rischi del 30 gennaio 2019[15] è sorta la necessità di creare basi legali specifiche per i compiti dell'NCSC.

L'articolo 73*a* AP-LSIn definisce i compiti principali dell'NCSC. A questi si aggiunge l'articolo 74 AP-LSIn, che specifica il tipo di sostegno che l'NCSC fornisce ai gestori di infrastrutture critiche. Per quanto riguarda l'introduzione dell'obbligo di segnalazione, è importante rilevare che l'articolo 73*b* AP-LSIn descrive la funzione dell'NCSC quale servizio di segnalazione degli incidenti e delle vulnerabilità informatiche e che gli articoli 73*c* e 73*d* AP-LSIn specificano quando e a chi l'NCSC può inoltrare quali informazioni derivanti dalle segnalazioni.

L'avamprogetto stabilisce che l'NCSC non può pubblicare o inoltrare informazioni su ciberincidenti che contengano dati personali o dati di persone giuridiche, salvo che sia stato dato il consenso. Rimane possibile la trasmissione, ad altre autorità o al pubblico, delle valutazioni statistiche e dei risultati delle segnalazioni pervenute. Tuttavia, l'articolo 73*d* AP-LSIn definisce anche le eccezioni a questo principio. In primo luogo, l'NCSC trasmette al SIC le informazioni contenute nelle segnalazioni, necessarie per il suo mandato legale di valutazione della situazione di minaccia e di preallerta a favore dei gestori di infrastrutture critiche. In secondo luogo, le informazioni

11 Preventivo 2022 con PICF 2023–2025 delle unità amministrative (DFF, DEFR, DATEC), volume 2B, pag. 11 e segg., consultabile al sito: www.efv.admin.ch > Pagina iniziale > Rapporti finanziari > Rapporti finanziari > Preventivo con piano integrato dei compiti e delle finanze.
12 RS **235.1**, RU **2022** 491
13 RS **734.7**
14 RS **172.056.1**
15 Cfr. comunicato stampa del 31 gennaio 2019 «Il Consiglio federale dà il via per un Centro di competenza in materia di cibersicurezza».

che forniscono indicazioni su un possibile reato in relazione alla segnalazione di un incidente informatico o alla sua analisi possono essere inoltrate alle autorità di perseguimento penale a discrezione del direttore dell'NCSC, sempre che ciò appaia opportuno in considerazione della gravità del possibile reato. Questo vale solo in casi eccezionali. Pertanto, i collaboratori dell'NCSC sono esentati dall'obbligo di denuncia di cui all'articolo 22*a* LPers se ricevono indicazioni di un possibile reato penale in relazione alla segnalazione di un ciberincidente o alla sua analisi.

L'obbligo di segnalare ciberattacchi a infrastrutture critiche è introdotto nella sezione 2. L'articolo 74*a* AP-LSIn stabilisce che le infrastrutture critiche devono segnalare all'NCSC i ciberattacchi ai loro mezzi informatici. L'articolo 74*b* AP-LSIn definisce i destinatari dell'obbligo di segnalazione, elencando specificatamente i settori nei quali viene introdotto tale obbligo. Infine, l'articolo 74*c* AP-LSIn obbliga il Consiglio federale a limitare i destinatari dell'obbligo di segnalazione per determinati settori, al fine di esentare le organizzazioni non rilevanti. L'articolo 74*d* specifica quali ciberattacchi devono essere segnalati e gli articoli 74*e* e 74*f* AP-LSIn stabiliscono quali termini e informazioni devono essere rispettati dal segnalante e le relative modalità. Infine, gli articoli 74*g* e 74*h* AP-LSIn definiscono la procedura e le conseguenze qualora le imprese non adempiano il proprio obbligo di segnalare ciberattacchi.

Infine, l'avamprogetto prevede anche modifiche di altri tre atti normativi. La nLPD è adeguata per consentire all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) di avvalersi delle conoscenze specialistiche dell'NCSC nel valutare le segnalazioni secondo la nLPD. La LAEl è adeguata per disporre di una base legale che obblighi i gestori di rete, i produttori e i gestori di impianti di stoccaggio ad adottare misure per proteggere adeguatamente i loro impianti dalle ciberminacce. Nella LAPub è inserita una disposizione in virtù della quale i produttori di hardware o software che non eliminano una vulnerabilità constatata entro il termine fissato potranno essere ritenuti responsabili di questo comportamento scorretto nel quadro del diritto sugli appalti pubblici.

2.2 Riassunto dei risultati della procedura di consultazione

La consultazione si è svolta dal 12 gennaio al 14 aprile 2022. Complessivamente sono pervenute 99 prese di posizione (25 Cantoni, 4 conferenze cantonali, 7 partiti politici, 5 organizzazioni mantello, 39 organizzazioni interessate, 19 imprese). L'introduzione di un obbligo di segnalare ciberattacchi a infrastrutture critiche è stata accolta perlopiù favorevolmente nella consultazione. 89 partecipanti alla consultazione su 99, tra cui tutti i Cantoni, accolgono con favore l'impostazione del progetto, pur formulando diverse riserve. 7 partecipanti rifiutano espressamente il progetto, tra cui un partito, un'organizzazione mantello dell'economia svizzera, 2 organizzazioni interessate, 2 imprese e una persona fisica.

Le riserve dei partecipanti favorevoli riguardano essenzialmente i seguenti punti:

– *Onere per gli interessati:* l'impegno richiesto per ottemperare al nuovo obbligo di segnalazione deve essere mantenuto il più esiguo possibile per gli

interessati. La segnalazione deve essere facile da compilare e deve essere possibile adempiere obblighi di segnalazione analoghi tramite un processo unico («one-stop-shop»).

– *Sanzioni in caso di inadempienza:* 24 partecipanti rifiutano le sanzioni per principio. Ritengono che l'obbligo di segnalazione non debba essere imposto con multe, bensì con incentivi. Le sanzioni sarebbero in contrasto con l'obiettivo di uno scambio di informazioni ottimale tra la Confederazione e i privati.
– *Definizione troppo ampia di ciberattacchi:* l'avamprogetto include anche i tentativi di attacco nella definizione di ciberattacchi (art. 5 AP-LSIn) e non delimita chiaramente quali ciberattacchi siano da segnalare (art. 74*d* AP-LSIn). Al riguardo, 23 partecipanti auspicano una definizione più chiara e ristretta. In generale è stato espresso il desiderio che i termini (ciberattacco, ciberincidente, ciberminaccia, ciber-rischio) fossero definiti più chiaramente e utilizzati in modo più rigoroso.
– *Ampio campo di applicazione dell'obbligo di segnalazione:* l'elenco dei settori interessati di cui all'articolo 74*b* AP-LSIn non è delimitato in modo sufficientemente chiaro, il che può generare incertezza giuridica sul campo di applicazione dell'obbligo di segnalazione. 39 partecipanti chiedono di modificare questo articolo; la maggior parte delle richieste di modifica riguarda una più chiara delimitazione dei settori nella legge o a livello di ordinanza.
– *Inoltro di informazioni:* la possibilità di inoltrare le informazioni contenute nelle segnalazioni alle autorità penali o al SIC è vista in modo critico da 6 partecipanti, che chiedono che tale inoltro possa avvenire solo in forma anonima. Il Cantone di Berna e la Conferenza dei comandanti di polizia cantonali chiedono invece che l'NCSC trasmetta tutte le segnalazioni alle autorità di perseguimento penale.
– *Legge sulla trasparenza:* 6 partecipanti chiedono che le attività dell'NCSC e le segnalazioni siano esplicitamente esentate dalla legge del 17 dicembre 2004[16] sulla trasparenza (LTras).

Oltre alle riserve, nella consultazione è stato anche richiesto di completare il progetto come segue:

– *Standard minimi e competenza dell'NCSC di emanare istruzioni:* la prevenzione di ciberincidenti non dovrebbe essere promossa soltanto mediante l'obbligo di segnalazione, ma anche introducendo standard minimi di cibersicurezza delle infrastrutture critiche. 9 partecipanti chiedono inoltre che l'NCSC possa emanare istruzioni sulla cibersicurezza destinate ai gestori di infrastrutture critiche.
– *Impunità per i cosiddetti «hacker etici»:* gli hacker etici, cioè quelli che cercano in modo mirato le vulnerabilità e poi avvertono gli interessati, forniscono un contributo prezioso in materia di cibersicurezza. Alcuni partecipanti chiedono che venga incoraggiata la segnalazione delle vulnerabilità e che gli hacker etici non vengano puniti per le loro attività.

16 RS **152.3**

– *Produttori inadempienti:* CH++ sollecita un approccio più coerente nei confronti dei produttori che non eliminano le vulnerabilità del software o dell'hardware nonostante la richiesta dell'NCSC. Nel concreto, occorrerebbe tenere conto di questa circostanza nei contratti esistenti o nelle procedure di appalto in corso.

2.3 Valutazione dei risultati della procedura di consultazione

Grande consenso in merito all'obbligo di segnalazione

L'introduzione dell'obbligo di segnalazione, la creazione dell'NCSC come servizio nazionale di segnalazione e il relativo chiarimento dei compiti della Confederazione nell'analisi di tali segnalazioni e nel fornire un sostegno sussidiario ai gestori di infrastrutture critiche sono accolti con favore. Il progetto è considerato un passo importante per migliorare la cibersicurezza della Svizzera, perché regola esplicitamente la responsabilità della Confederazione in caso di ciberincidenti. Tuttavia, molti partecipanti alla procedura di consultazione chiedono una maggiore precisione terminologica. In particolare, il termine «ciber-rischio» spesso utilizzato ma non definito, è stato reputato poco chiaro. Nel disegno le definizioni dei termini sono state quindi adeguate e il termine «ciber-rischio» è stato sostituito con «ciberminaccia».

Ruolo dell'NCSC

Molti partecipanti alla consultazione hanno chiesto anche di potenziare il ruolo dell'NCSC, proponendo ad esempio di conferire a quest'ultimo la facoltà di emanare istruzioni destinate ai gestori di infrastrutture critiche. Le istruzioni potrebbero ad esempio contenere la richiesta di standard minimi di sicurezza o l'ordine di eliminare vulnerabilità. A queste richieste non abbiamo dato seguito. Il progetto mira a promuovere la preallerta e lo scambio di informazioni con le infrastrutture critiche. Se all'NCSC fosse assegnata una funzione di vigilanza e regolamentazione, le imprese saranno difficilmente disposte a condividere informazioni con l'NCSC anche su base volontaria.

Oneri e benefici per le autorità e le organizzazioni assoggettate

Benché la maggioranza dei partecipanti alla consultazione si sia espressa a favore dell'obbligo di segnalazione, sono state avanzate anche diverse riserve. Per i Cantoni e per l'economia è importante che l'obbligo sia concepito in modo tale da generare il minor onere possibile e che la procedura di segnalazione sia concepita in modo tale da consentire contemporaneamente l'adempimento di altri obblighi di notifica. Il progetto crea le condizioni legali per tali soluzioni.

Da più parti è inoltre stato auspicato che l'obbligo di segnalazione generi un valore aggiunto per i segnalanti, rafforzando così l'economia nel suo complesso. Il disegno è quindi stato integrato con una disposizione che prevede il diritto dei gestori adempienti di ottenere il sostegno dell'NCSC.

Campo di applicazione dell'obbligo di segnalazione

Per quanto concerne il campo di applicazione personale dell'obbligo di segnalazione secondo l'articolo 74*b* AP-LSIn, è stato osservato che la cerchia delle autorità e delle organizzazioni assoggettate è molto ampia e che deve essere specificata a livello di ordinanza. Nel disegno abbiamo previsto che, al fine di chiarire tempestivamente eventuali ambiguità in merito all'assoggettamento, gli interessati possano chiedere informazioni al riguardo. Se necessario, l'NCSC può anche disporre l'assoggettamento tramite decisione (cfr. art. 74*a* cpv. 2 D-LSIn). Inoltre, i criteri per le deroghe sono stati resi più severi (art. 74*c* D-LSIn).

Nella consultazione è stato inoltre chiesto di limitare l'obbligo di segnalazione alle parti dell'impresa che svolgono i compiti previsti nell'articolo 74*b* AP-LSIn. Ciò risulterebbe rilevante soprattutto per i gruppi operanti in settori eterogenei. Inoltre, l'obbligo dovrebbe essere applicato anche se le imprese gestiscono i loro mezzi informatici all'estero, sempre che un ciberattacco abbia conseguenze in Svizzera. Queste preoccupazioni sono state prese in considerazione nei due nuovi capoversi (cfr. art. 74*b* cpv. 2 e 3 D-LSIn).

I partecipanti alla consultazione hanno chiesto maggiori precisazioni in merito al campo di applicazione materiale dell'obbligo di segnalazione. Pertanto abbiamo rielaborato la disposizione che disciplina quali ciberattacchi devono essere segnalati (art. 74*d* D-LSIn), omettendo i criteri non comprensibili o di difficile attuazione. Anche la disposizione contenuta nell'articolo 74*a* AP-LSIn, secondo cui i ciberattacchi devono essere segnalati «il più rapidamente possibile», è stata precisata e sostituita con un termine chiaramente misurabile di 24 ore (cfr. art. 74*e* D-LSIn).

Riservatezza delle segnalazioni

Un'altra importante richiesta dei partecipanti alla consultazione era che le segnalazioni fossero trattate in modo confidenziale. In particolare, volevano che le segnalazioni all'NCSC non fossero assoggettate alla LTras, altrimenti ci sarebbe il rischio che le informazioni sensibili dei gestori di infrastrutture critiche che segnalano un ciberincidente all'NCSC debbano essere rese pubbliche. Questa richiesta viene soddisfatta con un'eccezione al diritto di accesso conformemente alla LTras per quanto riguarda informazioni di terzi in relazione a segnalazioni e analisi (cfr. art. 4 cpv. 1bis D-LSIn).

Multa comminata in caso di inadempienza dell'obbligo di segnalazione

Senza alcun dubbio, la proposta di introdurre una multa in caso di inadempienza dell'obbligo di segnalazione ha suscitato la maggiore opposizione. Il disegno prevede che prima di imporre una sanzione, l'NCSC informi gli interessati in merito all'obbligo di segnalazione. Se non vi provvedono, l'NCSC emana una decisione con comminatoria di multa in caso di inadempienza. Nel disegno è stata inoltre inserita una disposizione secondo cui, non appena dispone di tutte le informazioni necessarie, l'NCSC è tenuto a informare l'autorità o l'organizzazione assoggettata che essa ha adempiuto l'obbligo di segnalazione (cfr. art. 74*e* cpv. 5 D-LSIn). Questa procedura garantisce che siano escluse sanzioni dovute ad ambiguità nell'interpretazione dell'obbligo di segnalazione. Infatti soltanto se, nonostante la decisione, l'autorità o l'organizzazione assoggettata non adempie i propri obblighi, ovvero non segnala

neppure a posteriori un ciberattacco concreto, è prevista una sanzione sotto forma di multa (cfr. art. 74*h* D-LSIn).

In merito, nella consultazione molti hanno messo in dubbio che una multa rappresenti lo strumento adatto per far rispettare l'obbligo di segnalazione e 13 partecipanti hanno chiesto di eliminare l'articolo corrispondente (art. 74*h* AP-LSIn). A questa richiesta non abbiamo dato seguito. Un valore aggiunto significativo dell'introduzione dell'obbligo di segnalazione rispetto al sistema di segnalazione volontaria è che tutte le organizzazioni interessate sottostanno all'obbligo di trasmettere informazioni e che non sarà più possibile beneficiare della preallerta senza contribuire in prima persona. Se un'autorità o un'organizzazione assoggettata rifiuta di partecipare a questo scambio di informazioni, è necessario prevedere la possibilità di sanzioni.

3 Diritto comparato, in particolare rapporto con il diritto europeo

Da luglio del 2016, quando è stata approvata la direttiva NIS, tutti gli Stati membri dell'UE sono tenuti ad attuare un obbligo di notificare ciberincidenti. Il termine fissato per l'attuazione è scaduto a maggio 2018. L'obbligo di notifica riguarda gli «operatori di servizi essenziali». Secondo l'articolo 4 della direttiva NIS, rientrano in questa definizione i soggetti pubblici o privati che svolgono un ruolo chiave per la garanzia della sicurezza nei seguenti settori: sanitario, trasporti, energia, bancario, infrastrutture dei mercati finanziari, infrastrutture digitali nonché fornitura e distribuzione di acqua. Il 16 maggio 2022 il Parlamento e la Commissione dell'UE hanno concordato un progetto di revisione della direttiva NIS (NIS2). Alla direttiva vengono ora assoggettati altri otto settori (acque reflue, smaltimento dei rifiuti, pubblica amministrazione, servizi postali, alimentazione, industria, prodotti chimici, spazio). Pertanto, i destinatari corrispondono grosso modo alla cerchia assoggettata all'obbligo di segnalazione definita nel presente progetto.

Per quanto riguarda la portata dell'obbligo di notifica, la direttiva NIS lascia agli Stati membri dell'UE uno spazio di manovra relativamente ampio. L'obbligo di notifica si applica agli incidenti più gravi e l'articolo 14 stabilisce che per determinare la rilevanza dell'impatto di un incidente si tiene conto in particolare dei seguenti parametri: il numero di utenti interessati, la durata dell'incidente e la diffusione geografica. A differenza del presente progetto, 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 volte a minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi (art. 14 direttiva NIS).

Per contro, il presente progetto (D-LSIn) si limita a creare le basi legali per tali requisiti nel settore dell'energia elettrica. Nei restanti settori è necessario anzitutto chiarire se la Confederazione abbia la competenza di fissare norme giuridicamente vincolanti in materia di cibersicurezza e quali requisiti debbano essere fissati in quali settori.

4 Punti essenziali del progetto

4.1 La normativa proposta

L'introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche viene proposto anzitutto al fine di creare un sistema di preallerta e di 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 segnalazione, permettendo la rapida individuazione dei metodi di attacco e la diffusione di informazioni al riguardo, può aumentare notevolmente la cibersicurezza delle infrastrutture critiche. Il maggior numero di segnalazioni che l'NCSC riceverà a seguito dell'introduzione dell'obbligo consentirà una valutazione più accurata della situazione di minaccia.

L'obbligo riguarda soltanto i ciberattacchi che possono arrecare notevoli danni. I ciberincidenti provocati da un comportamento errato, ad esempio un'operazione sbagliata compiuta involontariamente da un collaboratore, non sono invece assoggettati all'obbligo di segnalazione. Infine abbiamo rinunciato anche alla possibilità di estendere tale obbligo alle vulnerabilità riscontrate nei mezzi informatici. Le vulnerabilità vengono solitamente scoperte da terzi (ricercatori nel settore della sicurezza), che possono essere motivati a segnalare le vulnerabilità attraverso incentivi (ad es. i cosiddetti programmi «bug bounty», cioè che prevedono una ricompensa per i segnalanti). In un contesto simile, invece, un obbligo di segnalazione avrebbe probabilmente un certo effetto deterrente.

Tuttavia, a prescindere dall'introduzione dell'obbligo di segnalare ciberattacchi, chiunque potrà continuare a segnalare volontariamente ciberincidenti e vulnerabilità. Questa opportunità non è riservata soltanto alle infrastrutture critiche e tutti possono ricorrervi.

Con l'introduzione dell'obbligo di segnalare ciberattacchi vengono inoltre regolamentati a livello di legge i compiti dell'NCSC, che attualmente sono definiti soltanto nell'ordinanza del 27 maggio 2020[17] sui ciber-rischi (OCiber).

4.2 Compatibilità tra compiti e finanze

L'NCSC gestisce già oggi un servizio di contatto che riceve le segnalazioni di ciberincidenti effettuate su base volontaria. La sua attività si basa sulla pluriennale esperienza maturata con MELANI, la centrale che dal 2004 ha raccolto le segnalazioni.

L'NCSC utilizza già un modulo di segnalazione elettronico per ricevere le segnalazioni volontarie. Il sistema di segnalazione elettronica dell'NCSC può essere utilizzato anche per ricevere le segnalazioni in adempimento del relativo obbligo. La necessaria armonizzazione con gli altri servizi che ricevono già segnalazioni di questo tipo – come l'IFPDT, l'Autorità federale di vigilanza sui mercati finanziari (FINMA), l'Ispettorato federale della sicurezza nucleare (IFSN) – e l'approntamento del modulo di segnalazione richiederanno lavoro aggiuntivo nella fase iniziale, che tuttavia potrà

17 RS **120.73**

essere compensato con le risorse a disposizione dell'NCSC. Per attuare il progetto, però, l'NCSC deve poter garantire che le segnalazioni inviate in adempimento dell'obbligo siano registrate, quietanzate e documentate correttamente e che le informazioni derivanti dalle segnalazioni siano inoltrate al servizio preposto ai fini della preallerta. Questo rappresenta un onere supplementare che va considerato nella fase di potenziamento dell'NCSC.

In futuro l'NCSC fornirà sostegno all'infrastruttura critica interessata nel contrastare ciberincidenti. Si tratta peraltro di una prestazione di servizio già fornita e consolidata grazie alla pluriennale esperienza maturata dall'NCSC (e prima ancora da MELANI), ma che sicuramente dopo l'introduzione dell'obbligo di segnalazione richiederà un impegno maggiore. Questo perché, in primo luogo, l'NCSC riceverà un numero di segnalazioni più elevato e, in secondo luogo, sarà anche tenuto, secondo l'articolo 74*a* capoverso 3 D-LSIn, a fornire almeno una prima valutazione e raccomandazioni su come contrastare l'attacco. Di conseguenza anche il team dell'NCSC preposto all'analisi tecnica (GovCERT) dovrà essere potenziato.

4.3 Attuazione

4.3.1 Necessità di una base legale

In base al principio di legalità (art. 5 cpv. 1 della Costituzione federale [Cost.][18]) e alle disposizioni in materia di legislazione di cui all'articolo 164 capoverso 1 Cost., l'obbligo di segnalare ciberattacchi deve essere disciplinato a livello di legge almeno nei suoi elementi fondamentali. Il progetto contiene quindi gli elementi fondamentali dell'obbligo di segnalare ciberattacchi, ossia il fattore scatenante e l'entità dell'obbligo (ciberattacchi che possono potenzialmente arrecare danni), la cerchia dei destinatari (gestori di infrastrutture critiche operanti in determinati settori), il termine e il contenuto delle segnalazioni e il loro utilizzo da parte dell'NCSC. Per i gestori di infrastrutture critiche, l'obbligo di segnalazione rappresenta un'ingerenza nei diritti di soggetti privati o, nel caso di enti cantonali o comunali, nella loro autonomia federalistica. L'ingerenza tuttavia non è grave e non ha praticamente alcuna ripercussione finanziaria sulle imprese interessate.

4.3.2 LSIn, una base legale appropriata

Nell'ambito dei lavori preparatori si è esaminato se le nuove regole dovessero essere inserite in una legge separata o in una esistente, il cui scopo, oggetto e campo di applicazione fosse compatibile con un obbligo di segnalare ciberattacchi a infrastrutture critiche[19]. Le leggi prese in considerazione come possibili basi legali per l'introduzione di un obbligo di segnalazione sono state quelle che sanciscono già disposizioni in materia di tutela delle infrastrutture critiche e che sono incentrate sulla protezione

18 RS **101**
19 Cfr. rapporto «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen» del 25 novembre 2020.

dell'ordine pubblico, ovvero la LPPC, la legge del 17 giugno 2016[20] sull'approvvigionamento del Paese, la legge federale del 21 marzo 1997[21] sulle misure per la salvaguardia della sicurezza interna, la LAIn e la LSIn.

Dopo un esame approfondito, però, soltanto la LSIn si è dimostrata appropriata. Il suo scopo (garantire la sicurezza delle informazioni trattate dalla Confederazione e dei mezzi informatici impiegati), è direttamente collegato alla cibersicurezza, benché nella legge non sia utilizzato questo termine. Inoltre la LSIn contiene già disposizioni che prevedono un sostegno alle infrastrutture critiche da parte della Confederazione. Questo compito dell'NCSC era dunque già disciplinato a livello di legge in tali disposizioni. Perciò la LSIn si è rivelata non soltanto appropriata, ma anche la base legale ideale all'interno della quale introdurre l'obbligo di segnalare ciberattacchi. Un altro elemento a suo favore è rappresentato dal fatto che nei dibattiti parlamentari sul disegno di legge si era discusso dell'introduzione dell'obbligo di segnalazione per i gestori di infrastrutture critiche in caso di «incidenti gravi», ma a giugno 2020 tale proposta era stata respinta dalla maggioranza del Consiglio nazionale, dopo che il nostro Consiglio aveva annunciato l'elaborazione di un progetto da porre in consultazione su questo argomento.

4.3.3 Disposizioni di esecuzione

All'NCSC compete l'esecuzione dell'obbligo di segnalazione. Il 12 maggio 2022 il nostro Collegio ha già deciso di potenziare l'NCSC per farlo diventare un ufficio federale e dargli la forma organizzativa necessaria per poter svolgere i compiti indicati nel progetto.

I requisiti legali per i compiti dell'NCSC e l'obbligo di segnalare i ciberattacchi saranno specificati dal nostro Consiglio in un'ordinanza. In virtù dell'articolo 182 capoverso 2 Cost., il Consiglio federale può emanare disposizioni esecutive o attuative su tutti gli articoli del capitolo 5 D-LSIn, nel senso di norme completive della legge. Non ha bisogno di una norma di delega per questo, visto che non gli vengono conferiti poteri legislativi, ad eccezione della competenza di messa in vigore mediante decreto di promulgazione. Di conseguenza può decidere liberamente quali di queste disposizioni di legge devono essere specificate a livello di ordinanza. Solo nel caso delle eccezioni all'obbligo di segnalazione di cui all'articolo 74*c*, il nostro Collegio è tenuto a definire i valori soglia in base ai criteri ivi elencati.

4.3.4 Attuabilità dell'obbligo di segnalazione

Dalla consultazione è emerso un ampio consenso di fondo sull'introduzione di un obbligo di segnalazione, a condizione tuttavia che esso richieda un impegno esiguo da parte delle autorità o organizzazioni assoggettate e che ne scaturisca un valore aggiunto per la loro cibersicurezza. Per questo motivo è previsto un modulo online per

20 RS **531**
21 RS **120**

adempiere l'obbligo di segnalazione che consente di registrare rapidamente le informazioni necessarie e di trasmetterle elettronicamente all'NCSC. Quest'ultimo dispone già di un'esperienza nella messa a disposizione di portali di segnalazione, poiché dal 2020 riceve segnalazioni da parte della popolazione e delle imprese su base volontaria. L'NCSC garantisce che le procedure di segnalazione siano organizzate nel modo più semplice possibile e cerca lo scambio diretto con le autorità e le organizzazioni assoggettate.

Un ciberattacco a un'infrastruttura critica può comportare, oltre all'obbligo di segnalazione all'NCSC, l'avvio di altri processi assoggettati a tale obbligo e quindi determinare simultaneamente diversi obblighi di notifica. Possono ad esempio verificarsi i casi indicati di seguito.

– Le infrastrutture critiche operanti nel settore dei mercati finanziari sotto la vigilanza della FINMA sono tenute, già dal 1° settembre 2020, a notificare i ciberincidenti a quest'ultima.[22]

– Un ciberattacco a un'infrastruttura critica può comportare una violazione della sicurezza dei dati, che, a seconda della gravità, può rientrare nell'obbligo di notifica all'IFPDT (cfr. art. 24 nLPD).

– Se un ciberattacco provoca il malfunzionamento di un'infrastruttura critica, ad esempio un incidente radioattivo in una centrale nucleare, anche questo evento di norma deve essere notificato (IFSN, Centrale nazionale d'allarme ecc.).

Il nuovo obbligo di segnalare ciberattacchi previsto dal presente disegno non sostituirà gli obblighi già in vigore, che rimarranno validi e inalterati. È quindi importante che l'impegno richiesto alle autorità e alle organizzazioni assoggettate sia sostenibile anche qualora debbano adempiere simultaneamente altri obblighi di questo tipo. Per questo motivo l'NCSC metterà a disposizione un sistema per la registrazione elettronica della segnalazione (modulo, maschera di segnalazione o strumenti analoghi) che le autorità e le organizzazioni assoggettate potranno usare per inoltrare informazioni ad altri servizi che avranno scelto di parteciparvi. In tal modo, l'NCSC contribuisce a garantire lo sfruttamento di sinergie con gli obblighi di notifica esistenti, a condizione che questi riguardino il ciberattacco o le sue ripercussioni.

Le autorità e le organizzazioni assoggettate possono decidere autonomamente se inviare la segnalazione registrata elettronicamente all'NCSC, a parti di esso o inserire eventuali informazioni aggiuntive per altri servizi pertinenti. È importante che le informazioni specifiche per adempiere i rispettivi obblighi di segnalare siano accessibili soltanto al servizio di segnalazione interessato. Registrando le proprie informazioni e inoltrandole, le autorità e le organizzazioni assoggettate possono controllare quale servizio di segnalazione riceve queste informazioni.

22 Cfr. «Comunicazione FINMA del 7 maggio 2020 sulla vigilanza 05/2020 – Obbligo di notificare i cyber-attacchi secondo l'art. 29 cpv. 2 LFINMA» (RS **956.1**).

5 Commento ai singoli articoli

5.1 Spiegazioni generali

Le basi legali sull'obbligo di segnalare ciberattacchi, a parte il titolo dell'atto ed alcuni adeguamenti al capitolo 1, verrebbero inserite nel capitolo 5 della LSIn. Questo capitolo è stato completamente rielaborato in modo da integrare anche i compiti dell'NCSC che esulano dall'obbligo di segnalazione e che non si riferiscono unicamente alle infrastrutture critiche. Per questo motivo è stato adeguato anche il titolo del capitolo («Capitolo 5: Misure della Confederazione per la protezione della Svizzera contro le ciberminacce»).

I principali contenuti delle disposizioni di legge sono stati in parte già descritti in modo esaustivo e motivati nei numeri precedenti. Il commento agli articoli contempla quindi soltanto le integrazioni. Per le disposizioni che sono state solo formalmente adattate, le spiegazioni contenute nel messaggio del 22 febbraio 2017[23] concernente la legge sulla sicurezza delle informazioni continuano a essere determinanti.

5.2 Commenti ai singoli articoli

Titolo

Il titolo «Legge federale sulla sicurezza delle informazioni in seno alla Confederazione» è stato cambiato in «Legge federale sulla sicurezza delle informazioni». Sebbene tali disposizioni riguardino principalmente la Confederazione, la cibersicurezza in Svizzera quale compito dell'NCSC, disciplinato nel capitolo 5, non è limitata alla Confederazione. L'introduzione dell'obbligo di segnalare ciberattacchi avviene a livello nazionale e comprende anche autorità cantonali e organizzazioni intercantonali.

Capitolo 1: Disposizioni generali

Nel primo capitolo sono state apportate modifiche agli articoli 1, 2, 4 e 5. I restanti articoli rimangono invariati.

Art. 1 Scopo

L'articolo della LSIn concernente lo scopo è stato integrato al capoverso 1 ed è stato ulteriormente suddiviso 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 le ciberminacce. L'articolo è stato quindi ampliato per tenere conto degli aspetti inseriti con l'introduzione dell'obbligo di segnalare ciberattacchi e con la regolamentazione a livello di legge dei compiti dell'NCSC.

23 FF **2017** 2953, in particolare 2563 segg.

Art. 2 Autorità e organizzazioni assoggettate

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

Art. 4 Rapporto con altre leggi federali

Nella consultazione sull'avamprogetto è stato suggerito da più parti che per le segnalazioni all'NCSC si debba garantire la confidenzialità e che per questo motivo l'NCSC debba essere escluso dall'ambito di applicazione della LTras.

Questo suggerimento è stato parzialmente soddisfatto con l'inserimento nell'articolo 4 LSIn, che regola il rapporto della LSIn con la LTras, di un capoverso 1bis che esclude l'accesso alle informazioni di terzi di cui l'NCSC viene a conoscenza nella sua funzione di servizio di segnalazione tramite la ricezione e l'analisi delle segnalazioni. Si è tuttavia deciso di non escludere del tutto l'NCSC dall'ambito di applicazione della LTras.

È essenziale che l'NCSC possa garantire ai segnalanti il trattamento riservato delle loro segnalazioni. Il rapporto di fiducia è un prerequisito importante affinché le infrastrutture critiche assolvano il nuovo obbligo di segnalare ciberattacchi. La garanzia della confidenzialità acquisirà maggiore importanza con l'introduzione di tale obbligo, poiché il numero di segnalazioni all'NCSC aumenterà.

Rispetto all'OCiber (maggio 2020) e alla versione originale della LSIn (dicembre 2020), il presente disegno comporta un ampliamento del settore di compiti dell'NCSC soprattutto in relazione all'obbligo di segnalazione.

Affinché l'NCSC possa svolgere la sua funzione di servizio di segnalazione e in considerazione del numero crescente di segnalazioni, è essenziale che l'accesso a informazioni di terzi (conformemente alla LTras) di cui l'NCSC viene a conoscenza in relazione a segnalazioni e analisi sia escluso. Per contro, le informazioni provenienti da autorità oppure da organizzazioni assoggettate altresì alla LTras continuano a essere sottoposte al diritto di accesso ai sensi della LTras.

Un'eccezione si applica anche all'obbligo di segnalare ciberincidenti nel settore dei mercati finanziari, per i quali la FINMA è il servizio di segnalazione in qualità di autorità di vigilanza. A differenza dell'NCSC, la FINMA è stata completamente esentata dalla LTras (cfr. art. 2 cpv. 2 LTras). Per contro, nel caso dell'NCSC il diritto di accesso alle informazioni di terzi è escluso solo se l'NCSC riceve tali informazioni nella sua funzione di servizio di segnalazione. Per il resto, la LTras continua a prevalere sull'LSIn (art. 4 cpv. 1 LSIn).

Art. 5 Definizioni

Le definizioni alle lettere a, b e c non sono state modificate. In relazione all'obbligo di segnalare i ciberattacchi ai sensi dell'art. 74*a* D-LSIn e seguenti, occorre sottolineare che la definizione di infrastruttura critica di cui alla lettera c è ampia e pertanto non può essere utilizzata direttamente come base per i destinatari dell'obbligo di segnalazione.

Il catalogo dei termini è completato da quattro definizioni aggiuntive (d. ciberincidente, e. ciberattacco, f. ciberminaccia, g. vulnerabilità). Questi termini hanno una rilevanza diretta per l'introduzione dell'obbligo di segnalazione, motivo per cui è necessaria una definizione giuridica. Le nuove definizioni introdotte corrispondono a quelle degli standard riconosciuti a livello internazionale[24].

Lett. d Ciberincidente

La definizione di ciberincidente chiarisce che si tratta del termine generico per tutti gli eventi che compromettono gli obiettivi di protezione della sicurezza delle informazioni ai sensi dell'articolo 6 capoverso 2 LSIn, ossia la confidenzialità, la disponibilità o l'integrità delle informazioni o la tracciabilità del loro trattamento. L'integrità delle informazioni è garantita se la loro incolumità e correttezza sono preservate. Tracciabilità significa che è possibile vedere chi ha elaborato le informazioni, quando e come (cfr. le spiegazioni nel messaggio del 22 febbraio 2017[25] concernente la legge sulla sicurezza delle informazioni).

I ciberattacchi comprendono sia gli eventi provocati intenzionalmente da persone non autorizzate (ciberattacchi), sia quelli provocati involontariamente da persone autorizzate (ad es. attraverso una manipolazione errata) o quelli che si verificano a causa di malfunzionamenti dei mezzi informatici. Questi ultimi includono anche gli errori nei sistemi decisionali algoritmici (intelligenza artificiale).

La caratteristica essenziale di un ciberincidente è la compromissione della confidenzialità, della disponibilità o dell'integrità delle informazioni[26] oppure della tracciabilità del loro trattamento. Gli eventi che hanno il potenziale di compromettere gli obiettivi di protezione ma non li compromettono effettivamente non costituiscono ciberincidenti ai sensi della presente legge, bensì ciberminacce ai sensi della lettera f. Questa restrizione e delimitazione nella definizione di ciberincidente è necessaria, poiché le organizzazioni e le imprese constatano ogni giorno numerosi eventi che teoricamente mettono in pericolo gli obiettivi di protezione, ma che in pratica possono essere scongiurati con successo dalle misure tecniche di protezione (ad es. tentativi di phishing, spam ecc.). Solo quando gli obiettivi di protezione vengono effettivamente compromessi, l'evento diventa un ciberincidente.

Lett. e Ciberattacco

I ciberattacchi sono una delle possibili manifestazioni del ciberincidente. Un ciberincidente è considerato un ciberattacco se è stato provocato intenzionalmente, a prescindere dal fatto che abbia coinvolto collaboratori interni o una fonte esterna (o entrambi). La questione decisiva non è da dove è stato sferrato l'attacco (interno/esterno), ma se l'aggressore ha intenzionalmente compromesso gli obiettivi di protezione confidenzialità, disponibilità, integrità e tracciabilità (cfr. definizione di ciberincidente alla lettera d). Rientrano nella definizione di ciberattacco soltanto gli attacchi riusciti, cioè quelli che non hanno potuto essere respinti in tutto o in parte.

24 In particolare ISO 27000; ISO/IEC 29147:2018; NIST.
25 FF **2017** 2563, in particolare 2629.
26 Nella LSIn, il termine «informazioni» è utilizzato come termine generico che comprende anche i dati personali.

La distinzione tra ciberattacco e ciberincidente è importante, perché i ciberattacchi possono essere eseguiti più volte utilizzando lo stesso metodo. La panoramica di questi metodi di attacco è quindi essenziale per la preallerta delle infrastrutture critiche.

Per questo motivo, l'obbligo di segnalazione è limitato ai ciberattacchi, mentre gli altri ciberincidenti (ad es. quelli provocati involontariamente da collaboratori attraverso manipolazioni errate) e le ciberminacce (ad es. i tentativi di attacco non riusciti o le vulnerabilità) possono continuare a essere segnalati volontariamente e da chiunque. I ciberattacchi devono essere segnalati se colpiscono sottosettori critici (art. 74*b* D-LSIn) e hanno un certo grado di gravità (art. 74*d* D-LSIn).

Lett. f Ciberminaccia

Per ciberminaccia si intende qualsiasi circostanza o evento potenzialmente in grado di provocare un ciberincidente. Questo include quindi anche tutti gli eventi scongiurati con successo, come i tentativi di phishing. La definizione del termine si basa sulle definizioni di «cyberthreat» utilizzate a livello internazionale[27].

Il termine ciberminaccia è preferibile a ciber-rischio, utilizzato spesso in passato. A ben vedere, un ciber-rischio non è una ciberminaccia, bensì una mera valutazione della probabilità che l'evento si verifichi e dell'entità del danno.

Lett. g Vulnerabilità

Anche il termine «vulnerabilità», ossia una ciberminaccia dovuta a punti deboli o errori nei mezzi informatici, è stato recentemente inserito nelle definizioni dei termini. Una vulnerabilità è una manifestazione della ciberminaccia.

La definizione di vulnerabilità si basa su quella di «vulnerability» dell'agenzia governativa statunitense «National Institute of Standards and Technology» (NIST).[28] Le cause di una vulnerabilità possono risiedere nella progettazione, negli algoritmi utilizzati, nell'implementazione, nella configurazione, nel funzionamento o nell'organizzazione. Talvolta le definizioni di vulnerabilità distinguono anche il grado di vulnerabilità.[29] In questa sede si è tuttavia rinunciato a fare una distinzione tra diversi livelli di vulnerabilità.

Una vulnerabilità può essere essa stessa la causa del ciberincidente (ad es. se i malfunzionamenti portano a una crittografia insufficiente dei dati e quindi mettono direttamente a rischio la loro confidenzialità). Normalmente però una vulnerabilità nei

27 NIST: Cyber Threat – Glossary | CRSC (nist.gov); ISO: ISO/IEC TS 27100:2020(en), Information technology – Cybersecurity – Overview and concepts; ENISA: Glossary – ENISA (europa.eu).

28 La NIST, subordinata al Dipartimento del Commercio degli Stati Uniti, pubblica sul proprio sito Internet la seguente definizione: «vulnerability: weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source». Nel glossario dell'agenzia governativa «Cybersecurity and Infrastructure Security Agency» (CISA) presso la «National Initiative for Cybersecurity Careers and Studies» (NICCS), risulta chiaro che il termine «weakness» costituisce il precursore del termine «vulnerability».

29 Cfr. la definizione nel glossario della CISA: «vulnerability (expressing degree of vulnerability): qualitative or quantitative expression of the level of susceptibility to harm when a threat or hazard is realized».

mezzi informatici implica soltanto una maggiore suscettibilità ai ciberincidenti, ad esempio perché viene utilizzata come porta d'ingresso per ciberattacchi.[30]

Capitolo 2: Misure generali

Sezione 1: Principi

Alla fine della sezione 1 del capitolo 2 è aggiunto un nuovo articolo 10*a*, che non ha nulla a che vedere con l'introduzione dell'obbligo di segnalazione o con la definizione dei compiti dell'NCSC. È stato incluso nel D-LSIn perché attualmente non esiste alcuna base legale materiale per il trattamento dei dati personali nel contesto della sicurezza delle informazioni, lacuna che proponiamo di completare contestualmente alla presente revisione parziale.

Art. 10a Trattamento di dati personali

Nell'ambito della gestione della sicurezza delle informazioni, ad esempio durante la formazione o le verifiche, vengono regolarmente trattati dati personali. Di norma, per il loro trattamento è sufficiente una base legale a livello di ordinanza. Il fatto di contrastare gli incidenti di sicurezza richiede invece il trattamento di dati sui potenziali autori, che possono essere collegati a procedimenti e sanzioni di carattere amministrativo o penale e sono quindi considerati dati personali degni di particolare protezione ai sensi dell'articolo 3 lettera c della LPD[31] vigente o dell'articolo 5 lettera c nLPD. Quando la presente revisione parziale entrerà in vigore, si applicherà già la nuova legge sulla protezione dei dati. Perciò nel disegno si fa già riferimento a essa.

La LPD richiede una base legale a livello di legge per il trattamento di dati personali degni di particolare protezione, base che oggi manca e che proponiamo di creare con l'articolo 10*a* D-LSIn. I dati personali degni di particolare protezione includono, in particolare, i dati su identità, azioni, condotta e motivazioni dei potenziali autori di reati. Vengono trattati anche i dati delle persone che possono essere anche solo coinvolte nell'incidente, perché ad esempio subiscono un danno.

Secondo la LPD, nel trattamento di dati personali deve essere rispettato il principio di proporzionalità, motivo per cui i dati personali degni di particolare protezione possono essere conservati solo per due anni dopo che la violazione della sicurezza delle informazioni è stata contrastata o la vulnerabilità è stata eliminata. Il periodo massimo per il trattamento di dati personali degni di particolare protezione è di dieci anni, poiché non è prevista alcuna procedura fissa disciplinata dalla legge, come ad esempio nel Codice di procedura penale[32].

L'articolo 10*a* non disciplina il trattamento dei dati personali da parte dell'NCSC. Questo è disciplinato dall'articolo 75 e seguenti D-LSIn.

30 Cfr. la definizione nella pubblicazione NISTIR 7511 Rev. 4 della NIST: «vulnerability: error, flaw, or mistake in computer software that permits or causes an unintended behavior to occur».
31 RS **235.1**
32 RS **312.0**

Art. 23 Zone di sicurezza

Cpv. 3

Adeguamento redazionale nel testo francese.

Capitolo 3: Controllo di sicurezza relativo alle persone

Art. 44 Tutela giurisdizionale

Cpv. 2

Adeguamento redazionale.

Capitolo 5:
Misure della Confederazione per la protezione della Svizzera contro le ciberminacce

Nel capitolo 4 della LSIn non sono state apportate modifiche.

Nel capitolo 5, oltre all'obbligo di segnalare ciberattacchi a infrastrutture critiche, sono state inserite anche le disposizioni di base relative ai compiti dell'NCSC. Per renderlo più chiaro, il capitolo 5 è quindi stato suddiviso in tre sezioni: «Sezione 1: Disposizioni generali», «Sezione 2: Obbligo di segnalare ciberattacchi» e «Sezione 3: Protezione dei dati e scambio di informazioni».

Sezione 1: Disposizioni generali

Le disposizioni della sezione 1 contengono principi generali, ad esempio sulla procedura di segnalazione e sulla gestione delle segnalazioni da parte dell'NCSC. Tali principi si applicano anche all'obbligo di segnalazione (sezione 2), alla protezione dei dati e allo scambio di informazioni (sezione 3).

Art. 73a Principio

Cpv. 1

Il capoverso 1 descrive le attività di analisi dell'NCSC come prerequisito dell'adempimento dei suoi compiti. Le analisi tecniche dell'NCSC comprendono anche ricerche estese di siti web infetti o di vulnerabilità.

Cpv. 2

Nel capoverso 2, i compiti dell'NCSC sono elencati alle lettere a–e. Si tratta di un elenco non esaustivo. I singoli compiti e la collaborazione con le autorità nazionali ed estere sono specificati in altri articoli e commentati in quella sede.

Art. 73b Segnalazioni

Dal 1° gennaio 2020 l'NCSC gestisce un servizio nazionale di contatto per le ciberminacce (cfr. art. 12 cpv. 1 lett. a OCiber), che riceve ed elabora le segnalazioni di ciberincidenti e ciberminacce. Il servizio dell'NCSC è stato realizzato sulla base di MELANI, la centrale che ha raccolto segnalazioni dal 2004. Questo servizio viene

utilizzato attivamente dalle imprese e dalla popolazione. Nel 2021 ha ricevuto 21 714 segnalazioni.

Cpv. 1

Nella sua funzione di servizio di segnalazione, l'NCSC accetta sia segnalazioni volontarie di ciberincidenti e ciberminacce, sia segnalazioni di ciberattacchi che rientrano nell'obbligo di segnalazione. Questo secondo aspetto non è esplicitamente menzionato nella legge, in quanto i ciberattacchi sono una manifestazione dei ciberincidenti.

I ciberincidenti e le ciberminacce, in particolare le vulnerabilità, possono essere segnalati all'NCSC non solo dagli stessi interessati, ma anche da terzi, se lo desiderano anche in forma anonima. I segnalanti devono assicurarsi di essere autorizzati a effettuare la segnalazione all'NCSC, soprattutto se agiscono per conto di terzi. Il capoverso 1 non costituisce una norma di autorizzazione della fattispecie di «whistleblowing». Devono essere rispettati gli obblighi di confidenzialità previsti dal contratto o dalla legge.

La scoperta di vulnerabilità attraverso l'accesso indebito a sistemi per l'elaborazione di dati di terzi («hacking»)[33] continua pertanto a essere passibile di sanzioni penali. Non è consigliabile introdurre un regime di protezione («porto sicuro legale») per le segnalazioni di vulnerabilità, perché ciò significherebbe che anche gli hacker criminali, e non solo i ricercatori di sicurezza, resterebbero impuniti o potrebbero esimersi dalla responsabilità penale con la segnalazione. Il reato di hacking rimane quindi punibile. Secondo l'articolo 73*d* capoverso 3 D-LSIn, i collaboratori dell'NCSC sono esentati dall'obbligo di denuncia in virtù dell'articolo 22*a* LPers. Inoltre, gli hacker o i ricercatori di sicurezza possono segnalare all'NCSC in forma anonima le vulnerabilità scoperte.

Cpv. 2

L'NCSC analizza le segnalazioni e ne valuta l'importanza per la protezione della Svizzera dalle ciberminacce. Se le segnalazioni non sono anonime e, se i segnalanti lo desiderano, l'NCSC può svolgere valutazioni dell'incidente e formulare raccomandazioni per ulteriori azioni sulla base di queste analisi.

L'NCSC tratta le segnalazioni in modo confidenziale. La confidenzialità è un prerequisito importante perché le segnalazioni vengano fatte e perché il servizio di segnalazione possa godere della fiducia degli utenti. Per questo motivo, i collaboratori dell'NCSC sono stati esonerati dall'obbligo di denuncia di reati (cfr. art. 73*d* cpv. 3 D-LSIn) e le informazioni che l'NCSC riceve da terzi nella sua funzione di servizio di segnalazione sono state esentate dal diritto di accesso secondo la LTras (cfr. art. 4 cpv. 1bis D-LSIn).

Cpv. 3

Le vulnerabilità dei mezzi informatici aumentano la suscettibilità ai ciberincidenti e costituiscono una ciberminaccia (cfr. art. 5 lett. f e g D-LSIn). Le vulnerabilità non

33 Cfr. art. 143bis del Codice penale (CP; RS **311.0**).

sottostanno all'obbligo di segnalazione ma possono essere segnalate all'NCSC su base volontaria.

Se una vulnerabilità viene segnalata all'NCSC, quest'ultimo informa il produttore del software o dell'hardware interessato secondo la procedura di «coordinated vulnerability disclosure»[34], in modo che il produttore possa eliminare la vulnerabilità e fornire agli utenti una soluzione, ad esempio sotto forma di «fix» o «patch». Il termine «produttore» va inteso in senso funzionale e comprende, ad esempio, anche gli sviluppatori di software.

L'NCSC fissa un termine per l'eliminazione della vulnerabilità da parte dei produttori, con la comminatoria che la mancata osservanza del termine durante la procedura di appalto può comportarne l'esclusione o la revoca dell'aggiudicazione[35] e che l'NCSC può pubblicare la vulnerabilità dopo la scadenza del termine.

Se il produttore offre una soluzione per una vulnerabilità che non è direttamente implementata da lui, spetta agli utenti decidere se implementarla o no. L'obbligo di colmare le vulnerabilità equivale a una forte ingerenza nella libertà economica e può essere controllato solo con un onere elevato. Sotto il profilo tecnico non conviene implementare aggiornamenti di sicurezza per qualsiasi sistema in ogni caso. Si è quindi deciso di non introdurre siffatti obblighi.

Art. 73c Pubblicazione di informazioni provenienti da segnalazioni

Cpv. 1

L'NCSC può pubblicare informazioni sui ciberincidenti, sempre che esse non contengano dati personali o dati di persone giuridiche. Queste informazioni possono rivelare l'identità della persona fisica o giuridica interessata solo se questa vi acconsente e se riguardano caratteristiche di identificazione ed elementi d'indirizzo utilizzati in modo abusivo, come nel caso di abuso dei loghi negli attacchi di phishing. In questi casi, oltre all'organizzazione o all'autorità proprietaria del logo, di solito sono coinvolti anche privati (ad es. clienti). L'NCSC chiederà il consenso dell'organizzazione o dell'autorità interessata che ha subito l'abuso del logo per poter informare il pubblico in merito.

Cpv. 2

La rapida pubblicazione di una vulnerabilità con l'indicazione del nome dell'hardware o del software interessato può essere necessaria per prevenire altri ciberattacchi. Nel settembre 2021, l'organizzazione statunitense MITRE ha riconosciuto l'NCSC quale servizio esperto di vulnerabilità, definite in gergo tecnico anche «common vulnerabilities and exposure», e ha autorizzato l'NCSC ad assegnare alle vulnerabilità un numero di identificazione univoco conformemente al sistema di riferimento internazionale, al fine di identificare, definire e catalogare le vulnerabilità rese pubbliche nel settore della sicurezza informatica.

34 Detto anche «responsible vulnerability disclosure».
35 Cfr. art. 44 cpv. 1 lett. f^{bis} LAPub (cifra II n.1 D-LSIn).

Quando si pubblicano le vulnerabilità, si segue il processo di «coordinated vulnerability disclosure» (divulgazione coordinata delle vulnerabilità). Questo processo corrisponde all'usuale buona prassi, osservata anche dai programmi «bug bounty». I produttori hanno il tempo di correggere la vulnerabilità prima della pubblicazione per la quale l'NCSC fissa un termine specifico.

Spesso non è necessario pubblicare una vulnerabilità se è stata risolta dal produttore, soprattutto quando le patch vengono applicate automaticamente. In singoli casi, tuttavia, può avere senso rendere pubblica una vulnerabilità benché sia stata risolta dal produttore. Nella fattispecie, la pubblicazione è possibile solo con il consenso del produttore. Se quest'ultimo non risolve la vulnerabilità, l'NCSC può pubblicarla senza il suo consenso. L'NCSC si astiene dalla pubblicazione se questa non serve alla protezione dalle ciberminacce, ad esempio se porta a informare gli aggressori su possibili vettori di attacco prima che questi li abbiano scoperti («zero day exploit»).

Il capoverso 2 costituisce la base legale per consentire all'NCSC di nominare l'hardware e il software interessati, e quindi implicitamente il suo produttore, se quest'ultimo non ha posto rimedio alla vulnerabilità in tempo utile.

Art. 73d Inoltro di informazioni

Questa disposizione definisce le condizioni in cui l'NCSC è autorizzato a inoltrare ad autorità e organizzazioni informazioni rilevanti per la sicurezza emerse in relazione a una segnalazione o alla sua analisi (capoversi 1–3).

Se queste informazioni contengono segreti legali o contrattuali, il collaboratore della NCSC responsabile dell'inoltro deve essere sciolto dal segreto d'ufficio secondo la procedura di cui all'art. 320 CP, al fine di non rendersi perseguibile (capoverso 4).

Cpv. 1

I requisiti per l'inoltro di informazioni alle autorità e alle organizzazioni attive nel settore della cibersicurezza devono essere soddisfatti in maniera cumulativa. L'inoltro richiede quindi che le informazioni in questione servano agli esperti di cibersicurezza nella protezione dalle ciberminacce e, se le informazioni rivelano l'identità della persona fisica o giuridica interessata, che quest'ultima abbia dato il proprio consenso.

A differenza della pubblicazione di tali informazioni ai sensi dell'articolo 73*c* capoverso 1 D-LSIn, l'inoltro di informazioni agli esperti di cibersicurezza non presume alcun abuso di identità.

Cpv. 2

Conformemente all'articolo 6 capoversi 1 lettera a, 2 e 5 LAIn, il SIC ha il mandato di individuare e sventare tempestivamente le minacce per la sicurezza interna ed esterna, di valutare la situazione di minaccia e di avvertire le infrastrutture critiche riguardo a eventuali minacce. Per questi compiti del SIC, le informazioni provenienti dalle segnalazioni sui ciberincidenti e la loro analisi da parte dell'NCSC possono essere rilevanti per la sicurezza. L'NCSC inoltra quindi al SIC le informazioni necessarie per questi compiti. Questo inoltro riguarda unicamente le informazioni relative alla segnalazione di un ciberincidente e alla sua analisi, ma non le informazioni sulle vulnerabilità segnalate.

Cpv. 3

L'obbligo di denuncia cui sono assoggettati gli impiegati federali (cfr. art. 22*a* LPers) si applica ai collaboratori dell'NCSC che ricevono indizi di un possibile reato grave in relazione a una segnalazione o alla sua analisi soltanto nei confronti del direttore dell'NCSC. Questa disposizione derogatoria è necessaria perché l'obbligo di denuncia è in contrasto con il principio del trattamento confidenziale delle segnalazioni da parte dell'NCSC. Qualora i collaboratori dell'NCSC scoprano indizi di reato al di fuori della procedura di segnalazione e analisi, l'obbligo di denuncia continua naturalmente a essere applicato.

In caso di sospetto di un reato grave, il direttore dell'NCSC può coinvolgere le autorità giudiziarie sulla base delle informazioni contenute nelle segnalazioni o nella loro analisi. L'NCSC non svolge alcuna attività investigativa.

Questo diritto di denuncia in casi eccezionali è stato previsto ad esempio per situazioni nelle quali, a seguito dell'analisi di un incidente, viene scoperto del materiale pedopornografico. Prima di sporgere denuncia, il direttore dell'NCSC valuta l'interesse dello Stato a un'azione penale e l'interesse del segnalante a mantenere la confidenzialità delle informazioni.

Il problema dell'autoaccusa del segnalante è disciplinato nell'ambito dell'obbligo di segnalazione. Anziché rendere obbligatorio il divieto di autoaccusa come nel diritto sulla protezione dei dati (cfr. art. 24 cpv. 6 nLPD), il presente disegno prevede che il segnalante non sia tenuto a fornire indicazioni che lo rendano penalmente perseguibile (cfr. commenti all'art. 74*e* cpv. 4 D-LSIn).

Cpv. 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 2 e 3, laddove le informazioni contengano segreti protetti dalla legislazione penale i collaboratori dell'NCSC preposti all'inoltro devono essere esonerati dall'osservanza del segreto d'ufficio conformemente alle disposizioni dell'articolo 320 CP.

Art. 74 Sostegno ai gestori di infrastrutture critiche

I compiti dell'NCSC, menzionati nell'articolo 73*a* D-LSIn sotto forma di panoramica non esaustiva, comprendono non solo la ricezione e l'elaborazione delle segnalazioni (cfr. art. 73*b*–73*d* D-LSIn), ma anche il sostegno ai gestori di infrastrutture critiche ai sensi dell'articolo 73*a* capoverso 2 lettera e, la cui portata è precisata nell'articolo 74 D-LSIn.

Si rammenta che la definizione di infrastrutture critiche di cui all'articolo 5 lettera c LSIn è molto ampia. Perciò vi è una certa mancanza di chiarezza su quando un'impresa o un'organizzazione debba o non debba essere considerata un'infrastruttura critica.

Inoltre, alle infrastrutture critiche di cui all'articolo 2 capoversi 1–3 LSIn (ad es. le autorità federali) si applicano altre disposizioni della LSIn che non si applicano ad altre infrastrutture critiche come la Migros.

Cpv. 1 e 2

L'NCSC sostiene i gestori di infrastrutture critiche nel proteggersi contro le ciberminacce. A tal fine, mette loro a disposizione gratuitamente gli strumenti necessari. I gestori di infrastrutture critiche sono liberi di decidere se avvalersi del sostegno dell'NCSC. Gli strumenti sono quindi messi a disposizione per l'utilizzo su base volontaria.

I principali strumenti sono elencati a titolo esemplificativo (lettere a–c). Questo elenco non è esaustivo.

Lett. a

Lo scambio reciproco di informazioni è uno strumento essenziale per la protezione delle infrastrutture critiche dalle ciberminacce. 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. L'NCSC, portando avanti la stretta collaborazione tramite MELANI, offre ai gestori di infrastrutture critiche una piattaforma attraverso la quale scambiarsi le informazioni. L'NCSC utilizza questo canale informativo protetto anche per informare tempestivamente le infrastrutture critiche su modelli di attacco che non sono ancora noti al pubblico e che non possono essere pubblicati dall'NCSC per motivi di sicurezza.

Lett. b

L'NCSC mette a disposizione delle infrastrutture critiche informazioni tecniche su ciberminacce attuali (ad es. vulnerabilità) nonché raccomandazioni per l'adozione di misure preventive e reattive contro i ciberincidenti. Gli strumenti elencati alla lettera b si limitano a indicazioni generalmente utili per qualsiasi infrastruttura critica. Non viene fornita una consulenza specifica per una determinata impresa.

Lett. c

L'NCSC fornisce anche strumenti tecnici e istruzioni per l'individuazione precoce di ciberincidenti. Tali strumenti possono includere regole per l'identificazione di flussi di rete e file potenzialmente dannosi, elenchi di indicatori tecnici di attacchi sferrati o tentati («indicator of compromise», IOC) oppure applicazioni specializzate per il rilevamento di modelli di attacco e la protezione da questi ultimi.

Questi strumenti sono talvolta progettati per essere utili a tutte le infrastrutture critiche. Tuttavia, possono anche essere specificamente adattati a determinati gruppi di infrastrutture critiche o a determinati settori di attività. Gli strumenti succitati non sostituiscono i piani di protezione di una singola infrastruttura, ma devono essere integrati in essa.

Cpv. 3

L'NCSC può sostenere i gestori di infrastrutture critiche nel contrastare ciberincidenti e risolvere vulnerabilità fornendo consulenza tecnica. Il sostegno dell'NCSC alle infrastrutture critiche viene fornito su richiesta e in stretta collaborazione con le parti interessate.

L'NCSC può anche fornire supporto tecnico agli operatori se un ciberincidente mette a rischio il funzionamento dell'infrastruttura critica interessata. Per quanto riguarda la sua portata, il sostegno tecnico fornito dall'NCSC è limitato alle misure di emergenza. Ulteriori misure, in particolare per ripristinare la cibersicurezza in generale, competono alle infrastrutture critiche colpite ed esulano dai compiti dell'NCSC. Il sostegno è sussidiario ai servizi informatici disponibili sul mercato, sempre che si tratti di gestori privati. Il fattore decisivo è l'ente responsabile, non la forma giuridica dell'infrastruttura critica. Il sostegno sussidiario ai gestori privati intende evitare che l'NCSC distorca la concorrenza sul mercato dei servizi informatici.

Se è soggetta all'obbligo di segnalazione secondo gli articoli 74*b* e 74*c* D-LSIn, l'infrastruttura critica interessata ha diritto al sostegno tecnico dell'NCSC (cfr. art. 74*a* cpv. 4 D-LSIn). Anche in questo caso si applica la riserva secondo cui, nel caso di organizzazioni di diritto privato, l'NCSC non può competere con il mercato dei servizi informatici. Sostiene i privati assoggettati all'obbligo di segnalazione nel contrastare l'incidente se non è disponibile per tempo un servizio di mercato equivalente.

Cpv. 4

In caso di ciberincidenti, in particolare sotto forma di ciberattacchi, l'NCSC dovrebbe avere la possibilità di accedere ai sistemi dell'infrastruttura critica interessata per contrastare l'incidente o limitare i danni. Ciò, ovviamente, a condizione che il gestore dell'infrastruttura critica vi acconsenta. Spetta al gestore verificare se eventuali obblighi di segretezza sono in contrasto con questo consenso. In pratica, solo in casi eccezionali l'NCSC accede direttamente ai mezzi informatici. Nella maggior parte dei casi, l'NCSC e gli specialisti informatici delle infrastrutture critiche collaborano in modo tale che l'NCSC fornisca raccomandazioni sugli indicatori da ricercare nei sistemi.

Sezione 2: Obbligo di segnalare ciberattacchi

Art. 74a Principi

Questo articolo disciplina il campo di applicazione dell'obbligo di segnalazione, il processo di segnalazione, l'assoggettamento all'obbligo e il sostegno dell'NCSC nel contrastare gli incidenti. Come per la segnalazione di ciberincidenti e ciberminacce su base volontaria, l'NCSC svolge la funzione di servizio di segnalazione anche per i ciberattacchi contemplati dall'obbligo di segnalazione.

Cpv. 1

L'oggetto e i destinatari dell'obbligo di segnalazione nonché il servizio di segnalazione sono specificati nel capoverso 1. Le autorità e le organizzazioni assoggettate devono segnalare all'NCSC i ciberattacchi ai propri mezzi informatici. La cerchia dei destinatari assoggettati è elencata all'articolo 74*b* D-LSIn e le eccezioni saranno specificate nelle disposizioni di attuazione secondo l'articolo 74*c* D-LSIn.

Secondo l'articolo 74*d* D-LSIn i ciberattacchi devono essere segnalati soltanto se colpiscono i mezzi informatici delle stesse parti assoggettate all'obbligo. Ad esempio, i fornitori di servizi Internet non sono responsabili della segnalazione di incidenti che coinvolgono i loro clienti.

L'obbligo di segnalazione è adempiuto anche se le autorità o le organizzazioni assoggettate incaricano un terzo, ad esempio il gestore dei loro mezzi informatici, di effettuare la segnalazione. Se lo stesso fornitore di servizi informatici lavora per più autorità od organizzazioni assoggettate, può essere incaricato da più parti assoggettate di segnalare all'NCSC eventuali ciberattacchi ai rispettivi mezzi informatici. Dato il termine breve di 24 ore (cfr. art. 74*e* cpv. 1 D-LSIn), le autorità e le organizzazioni assoggettate dovranno incaricare eventuali terzi anticipatamente, poiché rimane poco tempo per la segnalazione quando viene scoperto un ciberattacco e la gestione dell'incidente rischia di impegnare molte risorse.

Se le autorità o le organizzazioni assoggettate incaricano una terza parte di effettuare la segnalazione, non trasferiscono la titolarità dell'obbligo di segnalazione, che quindi permane presso di loro. Se la terza parte incaricata omette di segnalare un ciberattacco all'NCSC, l'autorità o l'organizzazione assoggettata resta pertanto responsabile della violazione dell'obbligo.

Cpv. 2

Poiché l'elenco di cui all'articolo 74*b* capoverso 1 D-LSIn comprende un numero molto eterogeneo di settori, è prevedibile che, anche con una precisazione a livello di ordinanza, per alcune organizzazioni non sia chiaro se rientrano o no nell'assoggettamento. Per garantire che questa incertezza non vada a scapito degli interessati e che l'introduzione dell'obbligo di segnalazione non perda la sua efficacia, nei casi limite l'NCSC informa gli interessati, per quanto possibile tramite un questionario elettronico, in merito al loro assoggettamento . Se gli interessati mettono in dubbio o contestano questa classificazione da parte dell'NCSC, quest'ultimo emana una decisione impugnabile con indicazione dei rimedi giuridici.

Cpv. 3

Per gli interessati, l'assoggettamento all'obbligo di segnalazione non dovrebbe comportare soltanto un onere minimo, bensì produrre anche benefici concreti. Di conseguenza, le autorità e le organizzazioni assoggettate che scoprono un ciberattacco ai propri mezzi informatici e lo segnalano all'NCSC nelle forme e nei tempi dovuti hanno diritto al sostegno dell'NCSC nella gestione degli incidenti conformemente all'articolo 74 capoverso 3 D-LSIn. Se le capacità sono limitate, l'NCSC sosterrà di conseguenza in via prioritaria le autorità e le organizzazioni assoggettate.

Il diritto al sostegno da parte dell'NCSC garantisce che i benefici dell'obbligo di segnalazione siano superiori a un eventuale onere supplementare e che le autorità e le organizzazioni assoggettate non ricevano soltanto una contropartita, ma idealmente anche un valore aggiunto.

Cpv. 4

L'obbligo di segnalazione intende consentire all'NCSC di individuare per tempo modelli di attacco contro le infrastrutture critiche, avvisare quindi le potenziali vittime e raccomandare loro misure di prevenzione e di difesa adeguate. La raccomandazione relativa a queste misure è uno dei compiti statutari dell'NCSC.

L'NCSC non ha alcuna funzione di vigilanza sulle autorità e sulle organizzazioni assoggettate; l'obbligo di segnalare i ciberattacchi non è quindi uno strumento di

controllo[36]. Per l'NCSC, è uno strumento prezioso per venire a conoscenza degli attacchi in una fase precoce e poter così migliorare la cibersicurezza di infrastrutture critiche attraverso misure mirate di prevenzione e di difesa.

Dalla finalità dell'obbligo di segnalazione si evince che esso deve essere limitato ai ciberattacchi. Le segnalazioni su ciberincidenti che derivano da manipolazioni errate o guasti funzionali non sono rilevanti ai fini degli avvisi per la protezione della cibersicurezza. Anche le segnalazioni sulle ciberminacce, segnatamente sulle vulnerabilità, non sono assoggettate all'obbligo (cfr. n. 4.1).

Sebbene un ciberattacco violi generalmente anche la sicurezza dei dati, l'obbligo di segnalare ciberattacchi persegue uno scopo diverso rispetto all'obbligo di notifica previsto dalla nLPD (cfr. art. 24 nLPD). Mentre gli obblighi analoghi nel settore della sicurezza dell'aviazione o dell'energia nucleare mirano a una registrazione completa del maggior numero possibile di errori, compresi quelli di lieve entità, nel senso di una cultura della sicurezza, l'obbligo di segnalare i ciberattacchi non ha per oggetto gli errori commessi all'interno dell'azienda, per cui la cosiddetta «giusta cultura» (o «just culture»)[37] non si applica in caso di sanzioni.

Art. 74b Autorità e organizzazioni assoggettate all'obbligo di segnalazione

In linea di principio, il campo di applicazione dell'obbligo di segnalazione copre i settori che rappresentano obiettivi particolarmente interessanti per i ciberattacchi dal punto di vista della cibersicurezza. L'elenco esaustivo dell'articolo 74*b* D-LSIn si basa sui sottosettori critici della strategia nazionale per la protezione delle infrastrutture critiche 2018–2022 (PIC)[38] e sulle conoscenze acquisite dall'Ufficio federale della protezione della popolazione (UFPP), responsabile dell'attuazione della strategia PIC.

Poiché la definizione di infrastruttura critica è molto ampia[39], si parte dal presupposto che quasi tutte le autorità e le organizzazioni assoggettate siano anche infrastrutture critiche ai sensi dell'articolo 5 lettera c LSIn.

Il campo di applicazione dell'obbligo di segnalazione è precisato, per quanto possibile, con rimandi alle basi legali esistenti. I settori per i quali tale rimando non è possibile (perché non esiste alcuna base legale appropriata per tale delimitazione) vengono descritti nel modo più preciso possibile. Questa procedura mira a garantire che sia chiaro già a livello di legge chi è assoggettato all'obbligo.

36 La situazione è diversa nel caso del settore finanziario, in cui l'obbligo di notifica sussiste nei confronti della FINMA che è anche l'autorità di vigilanza sugli assoggettati.

37 Secondo il sito web www.justculture.ch/was-ist-just-culture, la «just culture» è una cultura in cui i collaboratori operativi o altre persone non vengono penalizzati per azioni, omissioni o decisioni coerenti con la loro esperienza e formazione, fermo restando che non sono tollerate negligenze gravi, violazioni intenzionali e azioni distruttive.

38 FF **2018** 455

39 L'art. 5 lett. c LSIn definisce le infrastrutture critiche nel seguente modo: «le infrastrutture per l'approvvigionamento di acqua potabile e di energia, le infrastrutture nei settori dell'informazione, della comunicazione e dei trasporti nonché altri processi, sistemi e installazioni essenziali per il funzionamento dell'economica e per il benessere della popolazione».

Data l'ampiezza della cerchia di destinatari, non si prevede che l'elenco debba essere ampliato nei prossimi anni. Nelle disposizioni di esecuzione, il Consiglio federale può concretizzare e precisare ulteriormente la cerchia dei destinatari dei singoli settori. Qualora in singoli casi non sia chiaro chi sia assoggettato all'obbligo di segnalazione, l'NCSC è autorizzato a decidere in merito al caso specifico emanando una decisione, previa consultazione dell'UFPP e delle autorità di vigilanza e regolamentazione settoriali (cfr. art. 74*a* cpv. 2 D-LSIn).

Inoltre, il Consiglio federale stabilirà le eccezioni all'obbligo di segnalazione all'interno di determinati settori mediante valori soglia. L'Esecutivo è quindi tenuto a garantire la proporzionalità dell'obbligo esentandone le organizzazioni che non sono essenziali per il funzionamento dell'economia o il benessere della popolazione (cfr. art. 74*c* D-LSIn).

Cpv. 1

Lett. a Scuole universitarie

Le scuole universitarie sono fondamentali per la piazza formativa ed economica svizzera, in particolare poiché la loro attività di ricerca è uno dei motori dell'innovazione. Per tale motivo le scuole universitarie sono un bersaglio interessante per gli hacker. Sono dunque assoggettate all'obbligo di segnalazione le università cantonali, i politecnici federali, le scuole universitarie professionali e le alte scuole pedagogiche.

Lett. b Autorità

I ciberattacchi alle autorità, a tutti i livelli federali, devono essere segnalati perché è importante sapere con quale frequenza e chi sferra attacchi a queste istituzioni. In tal modo possono essere predisposte misure di difesa mirate in funzione della minaccia. Fanno parte delle autorità anche il Parlamento federale e i Parlamenti cantonali.

L'Aggruppamento Difesa del Dipartimento federale della difesa, della protezione della popolazione e dello sport è esonerato dall'obbligo di segnalazione se le forze armate prestano un servizio di appoggio secondo l'articolo 67 o un servizio attivo secondo l'articolo 76 della legge militare del 3 febbraio 1995[40]. In questi casi, l'obbligo di segnalazione potrebbe mettere a repentaglio i segreti militari o rendere più difficile la cooperazione con le organizzazioni partner.

Lett. c Organizzazioni attive nei settori della sicurezza e del salvataggio, dell'approvvigionamento di acqua potabile, del trattamento delle acque di scarico e dello smaltimento dei rifiuti

Intendiamo assoggettare all'obbligo di segnalazione anche organizzazioni cui sono affidati compiti di diritto pubblico in determinati settori. Questi sono concretizzate nella lettera c. 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 assoggettate le organizzazioni attive nell'approvvigionamento di acqua potabile, nel trattamento delle acque di scarico e nello smaltimento dei rifiuti.

40 RS **510.10**

L'obbligo si applica soltanto alle attività che implicano l'esercizio dell'autorità sovrana di queste autorità e organizzazioni.

Lett. 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 assoggettate all'obbligo di segnalazione. Secondo l'articolo 6 capoverso 1 della legge federale del 30 settembre 2016[41] sull'energia, l'approvvigionamento energetico comprende «la produzione, la trasformazione, lo stoccaggio, la messa a disposizione, il trasporto, la trasmissione, nonché la distribuzione di vettori energetici ed energia fino alla loro consegna al consumatore finale, compresi l'importazione, l'esportazione e il transito». Inoltre, sono incluse anche le imprese attive nei settori del commercio, della misurazione o della gestione dell'energia.

I titolari di licenze secondo la legge federale del 21 marzo 2003[42] sull'energia nucleare (LENu) sono esentati dal presente obbligo di segnalazione per quanto riguarda i ciberattacchi che si verificano in un impianto nucleare. Nel quadro della vigilanza nucleare, hanno già ampi obblighi di notificare all'IFSN gli incidenti che si verificano nell'ambito della sicurezza e della protezione, compresi i ciberattacchi agli impianti nucleari (cfr. art. 22 cpv. 2 lett. f LENu in combinato disposto con l'art. 38 cpv. 3 e con l'art. 39 cpv. 2 dell'ordinanza del 10 dicembre 2004[43] sull'energia nucleare).

In qualità di autorità federale di sorveglianza degli impianti nucleari svizzeri, l'IFSN ha un servizio di segnalazione settoriale che dispone anche di un'organizzazione sempre pronta nell'ambito della cibersicurezza e dotata di personale specializzato. I processi definiti per le segnalazioni sono stabiliti e collaudati, in modo da funzionare in modo affidabile in caso di incidenti in un impianto nucleare.

In questo settore strettamente definito, i titolari delle licenze ai sensi della LENu sono esonerati da un ulteriore obbligo di segnalazione, al fine di escludere il rischio che, in caso di incidente, i processi consolidati e sensibili nel settore della sicurezza nucleare possano essere disturbati. Il disegno prevede invece l'introduzione di un nuovo capoverso 2 nell'articolo 102 LENu che obbliga l'IFSN a inoltrare all'NCSC le segnalazioni di un ciberattacco a un impianto nucleare che soddisfano i requisiti dell'articolo 74*d* D-LSIn.

Lett. 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. Il vigente obbligo di notifica alla FINMA per

41 RS **730.0**
42 RS **732.1**
43 RS **732.11**

quanto riguarda i ciberattacchi rimane in vigore parallelamente al nuovo obbligo di segnalazione all'NCSC. Nella messa a punto del processo di segnalazione, la FINMA e l'NCSC si accorderanno in modo da ridurre il più possibile l'onere per le imprese assoggettate.

Lett. f *Istituzioni* sanitarie

Secondo l'articolo 4 capoverso 1 lettera l dell'ordinanza del 1° luglio 2020[44] relativa ai dispositivi medici, per ospedale si intende un'istituzione sanitaria nella quale sono attuati mediante prestazioni mediche e infermieristiche e con degenza ospedaliera trattamenti di malattie oppure trattamenti di riabilitazione medica o interventi medici per scopi estetici. Tuttavia, secondo l'articolo 39 capoverso 1 lettera e della legge federale del 18 marzo 1994[45] sull'assicurazione malattie, soltanto gli ospedali che sono inclusi nell'elenco degli ospedali del Cantone in questione sono assoggettati all'obbligo di segnalazione.

Gli ospedali per malattie somatiche acute, riabilitazione e psichiatria figuranti negli elenchi cantonali degli ospedali garantiscono la copertura del fabbisogno di cure mediche di base nel rispettivo territorio cantonale. Secondo l'articolo 39 capoverso 3 LAMal, possono figurare nell'elenco anche le case per partorienti e le case di cura. L'obbligo di segnalare ciberattacchi deve essere applicato a tutte le istituzioni sanitarie elencate, perché è importante evitare che l'assistenza medica di base sia compromessa a causa di ciò. Se ciberattacchi a istituzioni sanitarie o all'Ufficio federale della sanità pubblica comportano una minaccia per la sicurezza dei dati delle cartelle cliniche elettroniche dei pazienti, l'organizzazione colpita dal ciberattacco è tenuta a segnalarlo.

Lett. g *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, essi dipendono in larga misura da infrastrutture informatiche funzionanti. Per questo motivo i ciberattacchi a tali laboratori devono essere segnalati.

Lett. h *Fabbricazione, immissione in commercio e importazione di medicamenti*

La fabbricazione, la distribuzione e l'importazione di medicamenti rivestono un'importanza centrale per garantire le prestazioni mediche alla popolazione. Per questo le imprese attive in questi settori che dispongono di un'autorizzazione ai sensi della legge del 15 dicembre 2000[46] sugli agenti terapeutici sono assoggettate all'obbligo di segnalazione.

44 RS **812.213**
45 RS **832.10**
46 RS **812.21**

Lett. i Assicurazioni sociali

Sono assoggettate all'obbligo di segnalazione anche le organizzazioni che forniscono prestazioni volte a coprire le conseguenze di malattie, infortuni, incapacità al lavoro e al guadagno, vecchiaia, invalidità e grande invalidità. Il termine «assicurazioni sociali» non è menzionato nel testo della legge, poiché non è una nozione definita nella legislazione.

L'obbligo di segnalazione è circoscritto in base alle prestazioni per i rischi coperti dalle disposizioni generali della legge federale del 6 ottobre 2000[47] sulla parte generale del diritto delle assicurazioni sociali (LPGA), al fine di coprire il maggior numero possibile di rami delle assicurazioni sociali. Tuttavia, l'obbligo di segnalazione non è limitato alle assicurazioni sociali sottoposte alla LPGA. Si è deciso di non elencare le singole leggi – ad esempio la legge federale del 19 giugno 1959[48] sull'assicurazione per l'invalidità, la legge federale del 20 dicembre 1946[49] sull'assicurazione per la vecchiaia e per i superstiti – per coprire non solo le prestazioni obbligatorie, ma anche quelle sovraobbligatorie, come la previdenza professionale sovraobbligatoria o l'assicurazione complementare all'assicurazione obbligatoria delle cure medico-sanitarie.

Nel caso della previdenza professionale (2° pilastro), sono coperti tutti gli istituti di previdenza registrati e non registrati (compresi gli istituti collettori), gli istituti di libero passaggio e il fondo di garanzia.

La previdenza facoltativa (pilastri 3*a* e 3*b*) è generalmente offerta da banche e compagnie di assicurazione, che a loro volta sono assoggettate all'obbligo di segnalazione.

Anche nel caso delle assicurazioni sociali, il Consiglio federale può imporre, a livello di ordinanza, restrizioni alla cerchia di persone assoggettate all'obbligo di segnalazione e, ad esempio, limitare il gruppo di destinatari degli istituti di previdenza e di libero passaggio assoggettati mediante criteri adeguati (cfr. art. 74*c* D-LSIn e le spiegazioni al n. 4.3.3).

Lett. j Società svizzera di radiotelevisione

Il mandato della Società svizzera di radiotelevisione (SSR) è fornire programmi radiofonici e televisivi completi e di pari valore a tutta la popolazione nelle tre lingue ufficiali. Inoltre, secondo l'articolo 24 capoversi 1 lettera a e 4 lettera a della legge federale del 24 marzo 2006[50] sulla radiotelevisione, la SSR contribuisce alla libera formazione delle opinioni del pubblico mediante un'informazione completa, diversificata e corretta, in particolare sulla realtà politica, economica e sociale. Il suo mandato va quindi chiaramente oltre gli obblighi di pubblicazione di altre emittenti concessionarie e rende la SSR un obiettivo allettante per un ciberattacco. È quindi giustificato assoggettare all'obbligo di segnalazione unicamente la SSR.

47 RS **830.1**
48 RS **831.20**
49 RS **831.10**
50 RS **784.40**

Lett. k *Agenzie di stampa d'importanza nazionale*

Secondo l'articolo 44*a* dell'ordinanza del 9 marzo 2007[51] sulla radiotelevisione, un'agenzia di stampa è d'importanza nazionale se diffonde regolarmente in almeno tre lingue nazionali informazioni sulle quattro regioni linguistiche della Svizzera (cfr. art. 18 lett. a della legge del 5 ottobre 2007[52] sulle lingue in combinato disposto con l'art. 13 cpv. 2 dell'ordinanza del 4 giugno 2010[53] sulle lingue). Nel concreto, in Svizzera è ancora operativa solo l'agenzia di stampa nazionale Keystone-ATS (si veda l'ordinanza COVID-19 media elettronici del 20 maggio 2020[54]).

Lett. l *Fornitori di servizi postali*

Anche le imprese che offrono ai clienti servizi postali a proprio nome sono assoggettate all'obbligo di segnalazione se sono registrate presso la Commissione delle poste secondo l'articolo 4 capoverso 1 della legge del 17 dicembre 2010[55] sulle poste (LPO). Il nostro Collegio può esonerare dall'obbligo di segnalazione le imprese più piccole a livello di ordinanza, ad esempio analogamente all'esonero delle imprese che realizzano una cifra d'affari economicamente modesta previsto nell'articolo 4 capoverso 3 LPO.

Lett. m *Trasporto pubblico (trasporto di viaggiatori e trasporto ferroviario di merci)*

Il rimando alle due leggi federali pertinenti (legge federale del 20 dicembre 1957[56] sulle ferrovie e legge del 20 marzo 2009[57] sul trasporto di viaggiatori [LTV]) copre i principali settori del trasporto pubblico di passeggeri, del trasporto ferroviario di merci e dell'infrastruttura ferroviaria. Le piccole imprese che gestiscono autobus o funivie e che dispongono di un'autorizzazione cantonale ai sensi dell'articolo 7 LTV non rientrano quindi nel campo di applicazione della disposizione. Anche il trasporto transfrontaliero di passeggeri non è contemplato. L'elenco separato delle imprese ferroviarie è necessario perché il trasporto ferroviario di merci non necessita di alcuna autorizzazione.

Lett. n *Imprese dell'aviazione civile*

Le imprese dell'aviazione civile che dispongono di un'autorizzazione dell'Ufficio federale dell'aviazione civile, ad esempio un'autorizzazione di esercizio secondo l'articolo 27 della legge federale del 21 dicembre 1948[58] sulla navigazione aerea (LNA), nonché gli aeroporti nazionali conformemente al Piano settoriale dei trasporti, Parte Infrastruttura aeronautica (PSIA), sono assoggettati all'obbligo di segnalare ciberattacchi.

51 RS **784.401**
52 RS **441.1**
53 RS **441.11**
54 RS **784.402**
55 RS **783.0**
56 RS **742.101**
57 RS **745.1**
58 RS **748.0**

Nella LNA sono menzionati gli aeroporti nazionali di Zurigo e Ginevra (cfr. art. 37*u* cpv. 2 LNA), ma non l'aeroporto di Basilea. È sembrato quindi necessario fare riferimento al PSIA per poter coprire tutti gli aeroporti nazionali. Il Consiglio federale adotta una scheda PSIA per ogni aeroporto nazionale (Zurigo, Basilea, Ginevra). Il Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni approva i piani per gli aeroporti (cfr. art. 37 segg. LNA).

Lett. o Porti basilesi e navigazione sul Reno

I porti renani svizzeri garantiscono l'accesso della Svizzera ai mari di tutto il mondo e rivestono un ruolo strategico per l'approvvigionamento nazionale di merci di ogni tipo. L'obbligo di segnalare ciberattacchi si applica quindi alle imprese che trasportano merci sul Reno secondo la legge federale del 23 settembre 1953[59] sulla navigazione marittima sotto bandiera svizzera e ai processi rilevanti per l'esercizio e il funzionamento dei porti basilesi.

Lett. p Beni indispensabili di uso quotidiano

Nell'approvvigionamento della popolazione con beni indispensabili di uso quotidiano, in particolare generi alimentari, sono coinvolti numerosi attori. Oltre ai produttori e agli importatori, infatti, vi sono anche i trasformatori, i centri di distribuzione e i commercianti al dettaglio. Non tutti questi attori hanno la stessa importanza per la sicurezza dell'approvvigionamento del nostro Paese. Per questo motivo, già a livello di legge è stata introdotta una limitazione alle imprese la cui interruzione parziale o totale comporterebbe significative strozzature nell'approvvigionamento.

L'obbligo di segnalare ciberattacchi sarà quindi applicato soltanto a quegli attori che svolgono un ruolo importante in questa ottica. Il nostro Consiglio restringerà quindi l'obbligo nel settore dell'approvvigionamento di beni indispensabili di uso quotidiano a livello di ordinanza applicando i criteri di cui all'articolo 74*c* D-LSIn.

Lett. q Fornitori di servizi di telecomunicazione

Secondo l'articolo 3 lettera c della legge del 30 aprile 1997[60] sulle telecomunicazioni (LTC), una trasmissione mediante telecomunicazione è un'emissione o ricezione elettrica, magnetica, ottica oppure elettromagnetica di altro tipo, di informazioni su linea o via radioonde. La fornitura di capacità di trasmissione è altresì considerata una forma di trasmissione mediante telecomunicazione.

Chiunque fornisce una trasmissione di informazioni a terzi è considerato in linea di principio un fornitore di servizi di telecomunicazione. I fornitori di servizi di telecomunicazione registrati ai sensi dell'articolo 4 LTC sono assoggettati all'obbligo di segnalazione.

Lett. r Gestori di registri e centri di registrazione di domini Internet

I nomi di dominio Internet consentono di assegnare un indirizzo unico a ciascun sito web. Tali nomi, come bakom.ch, sono utilizzati principalmente per accedere a siti web o per inviare e-mail.

59 RS **747.30**
60 RS **784.10**

I domini Internet sono amministrati a livello globale dall'«Internet Corporation for Assigned Names and Numbers» (ICANN). La Confederazione amministra i nomi di dominio di primo livello relativi alla Svizzera conformemente all'articolo 28*b* e seguenti LTC.

L'Ufficio federale delle comunicazioni esercita la funzione di gestore del registro, ma ha delegato questo compito a SWITCH. A determinate condizioni, può agire quale centro di registrazione («registrar») se non c'è un'offerta di mercato soddisfacente. Per i domini «.ch» e «.swiss», il gestore del registro («registry») è responsabile dell'amministrazione tecnica e operativa centrale dei domini, mentre la funzione di centro di registrazione, che può essere esercitata da diverse imprese, commercializza i nomi di dominio in libera concorrenza conformemente alle disposizioni dell'ordinanza del 5 novembre 2014[61] sui domini Internet (ODIn).

I centri di registrazione che hanno stipulato un contratto di registrazione con il gestore di registri possono richiedere e amministrare nomi di dominio per conto dei loro clienti. Questi centri fungono quindi da interfaccia esclusiva tra il gestore di registri e la persona richiedente (cfr. art. 24 cpv. 1 e allegato lett. m ODIn).

Lett. s Diritti politici

I servizi e le infrastrutture nel settore dei diritti politici comprendono i sistemi utilizzati per la raccolta e il conteggio delle firme per le petizioni referendarie, nonché per la preparazione e l'attuazione delle votazioni come pure per le procedure successive alle stesse.

Ciò include, ad esempio, sistemi per il voto elettronico («e-voting»), sistemi per la tenuta dei registri elettorali e per la determinazione e la trasmissione dei risultati delle votazioni. Inoltre, sono possibili sistemi futuri per la raccolta elettronica delle firme («e-collecting»). Altri servizi e infrastrutture includono, ad esempio, le imprese incaricate della stampa del materiale elettorale.

Lett. t Servizi digitali

L'obbligo di segnalazione si applica ai fornitori e agli operatori di cloud computing (ad es. «software as a service», SaaS), ai motori di ricerca, ai servizi di sicurezza e fiduciari digitali e ai centri dati, sempre che abbiano una sede legale in Svizzera.

Per analogia con il diritto dell'UE,[62] il termine «servizio fiduciario» comprende i servizi di firma elettronica, i sigilli e le marche temporali, la consegna di posta elettronica raccomandata, i certificati di autenticazione e i servizi di conservazione delle firme elettroniche, i sigilli e i certificati. Anche l'identità elettronica, ad esempio, è un servizio fiduciario.

Il termine servizio di sicurezza si riferisce in particolare a soluzioni per la crittografia delle informazioni o a mezzi informatici per la protezione da ciberattacchi (filtri antispam, programmi antivirus, firewall).

61 RS **784.104.2**

62 Il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93 all'art. 3 punto 16 definisce il concetto di «servizio fiduciario»; GU L 257 del 28.8.2014, pag. 73.

Lett. u Produttori di hardware e software

I ciberattacchi a infrastrutture critiche attraverso le catene di approvvigionamento sono diventati una minaccia rilevante. In particolare, i fornitori di hardware e software sono al centro dell'attenzione. Gli aggressori manipolano i mezzi informatici prima della consegna ai clienti finali, in modo da poter accedere successivamente ai sistemi. Per la cibersicurezza, i ciberattacchi ai produttori di hardware e software delle infrastrutture critiche assumono una grande importanza.

Sono di particolare rilevanza i ciberattacchi ai produttori se questi hanno accesso ai sistemi per la manutenzione da remoto. L'accesso alla manutenzione remota consente ai produttori che dispongono delle relative autorizzazioni di accedere ai componenti IT e OT della rete locale dall'esterno, ossia solitamente tramite Internet, a scopo di manutenzione o risoluzione dei problemi. Gli aggressori possono tentare di penetrare direttamente nei sistemi delle infrastrutture critiche attraverso questi punti di accesso legittimi.

Oltre al criterio legato alla manutenzione remota, i produttori di hardware e software sono assoggettati all'obbligo di segnalazione se offrono prodotti utilizzati in settori particolarmente delicati. Si tratta di hardware e software per la gestione e il monitoraggio di dispositivi fisici, processi ed eventi (la cosiddetta tecnologia operativa od «operational technology»), in particolare i sistemi di controllo industriale («industrial control system») e le soluzioni di automazione che assumono funzioni di controllo e regolazione di ogni tipo. Altri esempi sono le apparecchiature di laboratorio, ad esempio microscopi automatizzati o strumenti analitici, i sistemi logistici, come gli scanner di codici a barre con microcalcolatori o la tecnica di gestione degli edifici (n. 1).

L'attenzione è rivolta anche a hardware e software utilizzati per garantire la sicurezza pubblica (n. 2). Questo vale in particolare per la comunicazione delle organizzazioni di primo intervento o per i sistemi di indagine della polizia.

Cpv. 2

Per le grandi imprese, i conglomerati e i gruppi con settori di attività che rientrano in parte nell'elenco del capoverso 1, l'obbligo di segnalare i ciberattacchi non si applica a tutte le loro attività, ma soltanto a quelle che riguardano un settore citato nel capoverso 1. Se, ad esempio, un'impresa attiva nell'approvvigionamento alimentare gestisce anche parchi di divertimento o se un istituto finanziario gestisce anche un museo, queste imprese risultano assoggettate unicamente se un attacco informatico colpisce i mezzi informatici rilevanti per i compiti inerenti all'approvvigionamento alimentare o ai servizi finanziari.

Cpv. 3

Nel caso di imprese e organizzazioni attive a livello internazionale, occorre stabilire se l'obbligo di segnalazione include anche i ciberattacchi ai mezzi informatici situati all'estero. Questo è il caso se queste imprese e organizzazioni hanno una sede legale in Svizzera, svolgono un'attività in un settore menzionato al capoverso 1 e i mezzi informatici colpiti dal ciberattacco sono utilizzati per svolgere questa attività in Svizzera.

Art. 74c Eccezioni all'obbligo di segnalazione

La cerchia dei destinatari dell'obbligo di segnalazione stabilita dall'articolo 74*b* D-LSIn è definita in modo ampio e potrebbe includere anche le organizzazioni e le autorità che, considerate di per sé, ossia a causa delle loro dimensioni o del loro livello di approvvigionamento, non sono di importanza essenziale per il funzionamento dell'economia o per il benessere della popolazione, anche se sono attive in un sottosettore critico menzionato all'articolo 74*b* capoverso 1 D-LSIn.

L'articolo 74*c* D-LSIn stabilisce quindi che il Consiglio federale deve restringere ulteriormente la cerchia dei destinatari a livello di ordinanza. Proponiamo di escludere dall'obbligo di segnalazione le organizzazioni o autorità il cui malfunzionamento ha conseguenze soltanto minime sul funzionamento dell'economia o sul benessere della popolazione. Tali conseguenze sono quantificabili in particolare considerando il numero di persone colpite.

Art. 74d Ciberattacchi da segnalare

L'ambito di applicazione materiale dell'obbligo di segnalazione, ovvero quali tipi di ciberattacchi vanno segnalati, è sancito a livello di legge. Alle lettere a–d del capoverso 1 sono elencati i criteri determinanti per stabilire quali ciberattacchi siano di particolare rilevanza ai fini della preallerta e della valutazione della situazione di minaccia e dunque che devono essere segnalati. I criteri sono selezionati in modo tale da essere il più possibile direttamente accertabili dalle imprese. All'occorrenza i criteri saranno ulteriormente precisati a livello di ordinanza.

Lett. a

La minaccia al funzionamento è l'unico criterio che non si basa sulla rilevanza per la cibersicurezza, bensì sulle conseguenze. Questa minaccia è stata quindi inserita come soglia per i ciberattacchi da segnalare, perché il potenziale di danno è determinante anche per il diritto a ricevere un sostegno dell'NCSC nel contrastare i ciberincidenti (cfr. art. 74*a* cpv. 4 D-LSIn in combinato disposto con l'art. 74 cpv. 3 D-LSIn).

Lett. b

La manipolazione delle informazioni è uno dei criteri che rende un ciberattacco oggetto di una segnalazione obbligatoria. La manipolazione comprende, ad esempio, la crittografia delle informazioni appartenenti all'organizzazione interessata.

Lett. c

Se un ciberattacco non è stato identificato per un periodo prolungato, non si può escludere lo spionaggio, ad esempio lo spionaggio industriale, o la preparazione di altri attacchi. Le informazioni concernenti attacchi sferrati intenzionalmente in modo da rendere il più difficile possibile il rilevamento sono particolarmente importanti per mettere in guardia altri gestori di infrastrutture critiche.

Lett. d

La lettera d stabilisce che un ciberattacco deve essere sempre segnalato se vi sono circostanze rilevanti ai fini del diritto penale. Molti criminali informatici tentano di

ricattare i gestori delle infrastrutture critiche, i loro clienti o i singoli collaboratori minacciando o sferrando attacchi, ad esempio mediante crittazione con ransomware, minacciando di compromettere la loro disponibilità con attacchi «distributed denial of service» (DDoS) o minacciando di pubblicare informazioni compromettenti su determinate persone.

I ciberattacchi con circostanze penalmente rilevanti devono essere segnalati se l'estorsione, la minaccia o la coazione hanno un collegamento con l'impresa assoggettata all'obbligo di segnalazione e possono avere conseguenze negative sulle sue attività. La segnalazione di tali attacchi è importante per valutare l'entità della minaccia posta dai criminali informatici alle infrastrutture critiche.

Art. 74e Termine e contenuto della segnalazione

Cpv. 1

Ai fini della preallerta e della prevenzione è fondamentale che gli attacchi vengano segnalati immediatamente dopo essere stati individuati. Un termine di 24 ore per l'inoltro della segnalazione tiene conto di questo obiettivo. Entro 24 ore devono essere segnalate solo le informazioni note fino a quel momento; la segnalazione può essere completata successivamente[63].

Cpv. 2

Il contenuto della segnalazione, ossia le informazioni essenziali necessarie per adempiere l'obbligo di segnalazione, sono disciplinate al capoverso 2. Il contenuto concreto delle informazioni da segnalare sarà specificato nelle disposizioni di esecuzione. Nel modulo di segnalazione, l'NCSC descriverà in dettaglio il significato delle singole informazioni. Per «tipo di ciberattacco e sua esecuzione» si intende ad esempio l'indicatore di compromissione (IOC). Ciò include indirizzi IP o record DNS di infrastrutture di attacco note (ad es. botnet o server di comando e controllo), URL di pagine sospette, valori hash di malware, firme di virus, anomalie nel traffico di rete o comportamenti sospetti del software. La formulazione relativa alle «misure disposte» si basa su quella dell'articolo 24 capoverso 2 nLPD.

Per adempiere l'obbligo di segnalazione non sono necessarie informazioni che possano pregiudicare e violare i segreti professionali o aziendali delle autorità e delle organizzazioni assoggettate o che possano incriminarle (cfr. cpv. 4).

Cpv. 3

Al fine di contenere al massimo l'onere per i segnalanti, al momento della scoperta del ciberattacco vengono richieste solo le informazioni strettamente indispensabili. Nel caso dei ciberattacchi, spesso non è chiaro per molto tempo quanto sia grave l'attacco e cosa sia successo esattamente. Se queste informazioni sono incomplete al momento della segnalazione, gli interessati avranno quindi la possibilità di presentare le informazioni richieste nel capoverso 2 anche in un secondo momento, non appena

63 Cfr. «Comunicazione FINMA del 7 maggio 2020 sulla vigilanza 05/2020 – Obbligo di notificare i cyber-attacchi secondo l'art. 29 cpv. 2 LFINMA», consultabile al sito: www.finma.ch > Documentazione > Comunicazioni FINMA sulla vigilanza.

hanno sufficienti conoscenze al riguardo. Questa procedura in due fasi corrisponde anche all'obbligo di segnalare i ciberattacchi alla FINMA. Si è consapevolmente rinunciato a fissare un secondo termine per consentire agli interessati di concentrarsi sulla gestione dell'incidente. Al posto di un secondo termine, si prevede che l'NCSC informi le autorità e le organizzazioni assoggettate quando dispone di tutte le informazioni necessarie e l'obbligo di segnalazione si considera dunque adempiuto (cfr. cpv. 5).

Cpv. 4

Di norma, le informazioni da trasmettere all'NCSC nell'ambito dell'obbligo di segnalazione non contengono informazioni che possano incriminare penalmente l'autorità o l'organizzazione assoggettata o il segnalante. Per garantire il rispetto del principio del divieto di autoaccusa, si fa riferimento a questa circostanza già a livello di legge; un riferimento corrispondente è previsto anche nel modulo di segnalazione.

Cpv. 5

Affinché le autorità e le organizzazioni assoggettate possano sapere se le informazioni fornite sono sufficientemente complete e precise, l'NCSC li informerà dell'avvenuto adempimento dell'obbligo di segnalazione non appena disporrà di tutte le informazioni necessarie a tal fine.

Art. 74f Trasmissione della segnalazione

Cpv. 1

Per garantire che l'obbligo di segnalazione possa essere adempiuto con il minor onere possibile, l'NCSC dovrà fornire un sistema elettronico sicuro per l'invio delle segnalazioni, ad esempio attraverso un apposito modulo. La struttura sarà simile al modulo esistente per la segnalazione volontaria di ciberincidenti e ciberminacce. In considerazione dell'evoluzione tecnologica, il modulo di segnalazione è genericamente descritto nel testo di legge come un «sistema con cui trasmettere la segnalazione».

L'NCSC consentirà di registrarsi in anticipo, in modo che le imprese o le organizzazioni non debbano più inserire informazioni aggiuntive su di sé quando effettuano una segnalazione, conformemente al principio secondo il quale i dati del segnalante devono essere registrati una sola volta. La segnalazione automatica tramite «application programming interface» (API) non ha senso, perché in questo modo verrebbero trasmesse troppe informazioni all'NCSC. Spetta all'autorità o all'organizzazione assoggettata trasmettere all'NCSC solo le informazioni desiderate in relazione al ciberattacco.

Oltre a questo modulo di segnalazione, è comunque consentito informare l'NCSC in merito al ciberattacco con altri mezzi (posta elettronica, telefono).

Cpv. 2 e 3

L'NCSC progetterà il sistema di segnalazione, su richiesta e in collaborazione con altri servizi di segnalazione, in modo tale che i segnalanti abbiano la possibilità di inoltrare ad altre autorità la segnalazione dell'attacco informatico o delle sue conseguenze (ad es. sulla sicurezza dei dati o sul funzionamento dell'infrastruttura critica)

riguardo all'intera infrastruttura critica o soltanto a parte di essa (cpv. 2), o anche di raccogliere informazioni supplementari necessarie per soddisfare ad altri obblighi di notifica (cpv. 3), sempre con l'obiettivo di ridurre al minimo l'onere per i segnalanti. Se diversi obblighi di notifica coincidono, i segnalanti possono così informare tutte le autorità competenti in modo rapido, tempestivo e senza grandi sforzi.

Particolare rilievo assume il fatto che, ai sensi del capoverso 2, la segnalazione o parti di essa possono essere inoltrate unicamente dalle autorità od organizzazioni assoggettate. Spetta a loro stabilire quale autorità, oltre all'NCSC, debba ricevere la segnalazione del ciberattacco o delle sue conseguenze.

Secondo il capoverso 3, le autorità e le organizzazioni assoggettate possono, per adempiere un altro obbligo di notifica, registrare nel sistema dell'NCSC eventuali informazioni supplementari non rilevanti ai fini della segnalazione all'NCSC per trasmetterle poi a uno o più servizi di segnalazione. Tali informazioni supplementari vengono solo trasmesse dall'NCSC, ma non salvate. L'NCSC non ha alcuna possibilità di accedervi.

L'NCSC offre ad altri servizi di segnalazione interessati la possibilità di completare il modulo digitale conformemente ai rispettivi obblighi di segnalazione al fine di ridurre l'onere per le autorità e le organizzazioni assoggettate e di poter sfruttare le sinergie. Questa offerta non sostituisce gli altri obblighi esistenti, né significa che l'NCSC assume il ruolo di servizio competente per tali obblighi. La funzione di inoltro tiene conto della necessità di uno sportello unico («one stop shop»), in quanto gli obblighi che si sovrappongono possono essere adempiuti mediante un unico processo di comunicazione. Tuttavia, l'NCSC non svolge un ruolo attivo nell'inoltro delle informazioni ad altri servizi di segnalazione; l'inoltro viene effettuato esclusivamente dalle autorità o dalle organizzazioni assoggettate.

Art. 74g Violazione dell'obbligo di segnalazione

Cpv. 1

In caso di violazione dell'obbligo di segnalazione, l'NCSC richiama anzitutto l'attenzione delle autorità e delle organizzazioni assoggettate sulla violazione, fissando un congruo termine per porvi rimedio. Eventuali malintesi possono così essere chiariti.

Per prevenire simili malintesi, l'NCSC può altresì chiedere ulteriori informazioni dall'autorità o dall'organizzazione assoggettata al momento della segnalazione se quest'ultima è incompleta o imprecisa. Informa l'autorità o l'organizzazione assoggettata dell'avvenuto adempimento dell'obbligo di segnalazione non appena ha ricevuto tutte le informazioni necessarie a tal fine (cfr. art. 74*e* cpv. 5 D-LSIn).

Nel caso di un'eventuale violazione dell'obbligo di segnalazione, l'NCSC procederà quindi in modo pragmatico e informerà anzitutto l'autorità o l'organizzazione assoggettata interessata sulla violazione dell'obbligo. L'NCSC è tenuto a prendere questo primo contatto, che è un prerequisito per l'emanazione di una decisione ai sensi del capoverso 2.

Cpv. 2

In una seconda fase, se l'autorità o l'organizzazione assoggettata non provvede entro il termine fissato benché la violazione dell'obbligo sia evidente, l'NCSC emana una decisione indicando la comminatoria di una multa. Nella decisione l'NCSC precisa gli obblighi violati in modo tale da non lasciare dubbi all'autorità o all'organizzazione assoggettata su cosa deve fare. Ciò facilita anche il lavoro delle autorità di perseguimento penale cantonali che, in caso di inosservanza della decisione, devono condurre indagini sui fatti denunciati dall'NCSC ed emettere una sentenza o un decreto d'accusa (cfr. art. 74*h* D-LSIn).

Art. 74h Inosservanza di decisioni dell'NCSC

Proponiamo un sistema di multe che riprende ampiamente il meccanismo previsto dalla nLPD in caso di violazione degli obblighi o di inosservanza di decisioni dell'IFPDT (art. 60 e segg. nLPD). Richiamiamo al riguardo quanto spiegato nel messaggio del 15 settembre 2017[64] 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. Anche nel presente disegno prevediamo che la persona che avrebbe dovuto garantire l'osservanza della decisione dell'NCSC all'interno dell'infrastruttura critica sia perseguibile penalmente (cfr. art. 29 CP). La responsabilità per l'adempimento dell'obbligo di segnalazione, che in realtà compete all'impresa, è così attribuita alla persona fisica.

Il rimando all'articolo 6 della legge federale del 22 marzo 1974[65] sul diritto penale amministrativo indirizza la responsabilità penale al livello dirigenziale delle imprese, cioè ai dirigenti che hanno poteri di prendere decisioni e impartire istruzioni. Ciò consente un'adeguata attribuzione della responsabilità penale alle imprese assoggettate all'obbligo di segnalazione. Spetta all'organizzazione interna dell'azienda regolare le pertinenti responsabilità.

Cpv. 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 della società, dell'economia e dello Stato e per sottolineare la loro responsabilità per la garanzia della cibersicurezza nei confronti 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 altre misure adottate si sono rivelate inefficaci. Tenuto conto dei diversi livelli di cibersicurezza nei singoli settori e dei requisiti aggiuntivi imposti con il nuovo obbligo di segnalare ciberattacchi, si è consapevolmente rinunciato a riprendere il limite massimo della multa pari a 250 000 franchi previsto dalla nLPD, anche tenuto conto del fatto che gli interessi e l'attribuzione di responsabilità in caso di violazione della protezione dei dati sono diversi. La minaccia di una multa di 100 000 franchi dovrebbe essere sufficiente per indurre i responsabili delle infrastrutture critiche assoggettate all'obbligo di segnalazione a tenere un comportamento conforme.

64 FF **2017** 5939, in particolare 5975 e 6088 seg.
65 RS **313.0**

La determinazione della multa deve tenere conto delle circostanze personali della persona interessata conformemente ai principi del diritto penale.

Cpv. 2 e 3

Per la comminazione della multa alle imprese è stato ripreso per analogia il regolamento della nLPD (art. 64 nLPD). L'importo della multa per le aziende, pari a 20 000 franchi con un massimo di 100 000 franchi, corrisponde allo stesso rapporto previsto dalla legge sulla protezione dei dati (50 000 vs. 250 000 CHF).

Fino a un importo di 20 000 franchi, la multa può quindi essere comminata direttamente all'azienda soggetta all'obbligo di segnalazione anziché alla persona fisica responsabile, per evitare costose indagini. In considerazione dell'importo massimo di 100 000 franchi, l'importo per questi casi di lieve entità è stato fissato a 20 000 franchi

Se si considera che l'obbligo di segnalazione riguarda principalmente le infrastrutture critiche più significative, che in molti casi possiedono anche relative quote di mercato, non vi è motivo di ridurre l'importo massimo fissato di 20 000 franchi.

Sarebbe peraltro escluso stabilire una multa più alta per l'impresa e, ad esempio, determinarla rispetto a una certa percentuale della cifra d'affari, giacché in Svizzera la responsabilità penale delle imprese è sempre sussidiaria rispetto alla responsabilità penale personale (cfr. anche gli art. 29 e 102 CP). L'attribuzione di una multa all'impresa è quindi ammissibile solo nei casi di lieve entità.

Cpv. 4

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

Sezione 3: Protezione dei dati e scambio di informazioni

Rispetto al diritto vigente, gli articoli 75–79 D-LSIn, inseriti all'interno della nuova sezione 3 D-LSIn, sono stati adeguati sia sotto il profilo linguistico che dei contenuti per essere in linea con la definizione a livello di legge dei compiti dell'NCSC. L'NCSC ha preso il posto di MELANI, la centrale gestita congiuntamente dal precedente Organo direzione informatica della Confederazione 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 dell'NCSC con il SIC e l'inoltro di informazioni e dati devono essere disciplinati, laddove necessario, nella LSIn.

Art. 75 Trattamento di dati personali

La disposizione dell'articolo 75 D-LSIn è stata ampliata in termini di contenuto durante la revisione del capitolo 5, in modo che l'NCSC abbia una base per trattare i dati personali anche se questi non sono collegati a elementi di indirizzo. Inoltre, sono stati apportati diversi adeguamenti strutturali e formali, ad esempio inserendo la denominazione «NCSC».

Cpv. 1

Al posto di una descrizione generica dei servizi federali responsabili, la disposizione menziona esplicitamente l'NCSC e gli attuali capoversi 1 e 2 sono stati uniti. Anche in futuro sarà possibile trattare non soltanto dati personali, ma anche dati personali degni di particolare protezione collegati a elementi di indirizzo. Secondo la definizione di cui all'articolo 3 lettera f LTC, l'elemento di indirizzo è una «sequenza di cifre, lettere o segni, oppure altre informazioni che permettono di identificare le persone, i processi informatici, le macchine, gli apparecchi o gli impianti di telecomunicazione che partecipano a un processo di comunicazione mediante telecomunicazione».

Nella versione tedesca, le lettere *a* e *b* hanno subito un adeguamento redazionale, con stralcio dei verbi. Nelle tre lingue alla lettera a è stato inserito il termine «cibersicurezza». Per le spiegazioni sui dati personali degni di particolare protezione ai sensi delle lettere *a* e *b*, si rimanda al messaggio del 22 febbraio 2017[66] concernente la legge sulla sicurezza delle informazioni.

Cpv. 2

Il capoverso 2 riprende sostanzialmente gli attuali capoversi 3 e 4 ma è stato riformulato dal passivo all'attivo. In tal modo risulta chiaro che i dati vengono trattati dall'NCSC. Inoltre sono stati precisati i presupposti da soddisfare quando l'NCSC non informa la persona interessata sul trattamento di dati o sull'abuso di identità.

Art. 76 Cooperazione a livello nazionale

Questo articolo costituisce la base legale per lo scambio di informazioni tra l'NCSC e i gestori di infrastrutture critiche (cpv. 1 e 2) nonché tra l'NCSC e i fornitori di servizi di telecomunicazione (cpv. 3 e 4), sempre che questi non siano considerati gestori di infrastrutture critiche.

In termini di contenuto, l'articolo 76 corrisponde in gran parte alla versione adottata dal Parlamento il 18 dicembre 2020. Oltre agli adeguamenti linguistici (ad es. inserimento dei termini «ciberminacce» e «NCSC»), sono state apportate anche modifiche strutturali: i capoversi 1 e 2 descrivono lo scambio di informazioni tra l'NCSC e le infrastrutture critiche; i nuovi capoversi 3 e 4 descrivono lo scambio di informazioni tra l'NCSC e i fornitori di servizi di telecomunicazione.

Cpv. 1 e 2

Lo scambio di informazioni tra l'NCSC e i gestori di infrastrutture critiche disciplinato nei capoversi 1 e 2 non è limitato alle infrastrutture critiche assoggettate all'obbligo di segnalazione ai sensi dell'articolo 74*b* D-LSIn, ma è aperto a tutte le infrastrutture critiche interessate con sede in Svizzera (quindi anche quelle esentate dall'obbligo di segnalazione in virtù dell'articolo 74*c* D-LSIn).

Per lo scambio di informazioni con le infrastrutture critiche, che avviene attraverso un canale di comunicazione protetto, l'NCSC utilizza lo standard «Traffic Light Proto-

66 FF **2017** 2563, pag. 2673 segg.

col» (TLP), ossia la classificazione comune a livello internazionale delle informazioni degne di protezione in quattro categorie, che ne disciplinano l'utilizzo e l'eventuale inoltro.

Il contenuto dello scambio di informazioni tra l'NCSC e le infrastrutture critiche è stato ampliato rispetto alla versione attuale, poiché la restrizione agli elementi di indirizzo e ai dati personali associati non era appropriata. Per la preallerta e la difesa da ciberattacchi immediati, l'NCSC dipende dalla possibilità di rendere noti alle infrastrutture critiche dati personali che non siano legati a elementi di indirizzo. Le infrastrutture critiche devono essere autorizzate a comunicare all'NCSC anche i dati personali che, pur non essendo direttamente collegati a un ciberincidente (condizione prevista nell'attuale capoverso 3), sono collegati, ad esempio, a ciberminacce. Questa aggiunta è in linea con il messaggio sulla LSIn, secondo cui le infrastrutture critiche possono comunicare informazioni a MELANI «connesse con pericoli e incidenti» e in tal modo «dare indicazioni in merito alle prestazioni di servizi, alle trasmissioni e ad altre operazioni effettuate per sventare pericoli e di conseguenza per impedire danni»[67]. La presente revisione del capitolo 5 è stata colta come un'opportunità per precisare il testo della legge. Ciò garantisce che l'NCSC possa scambiare con le infrastrutture critiche tutte le informazioni, compresi i dati personali, necessarie alla preallerta e alla difesa dalle ciberminacce.

Cpv. 3 e 4

Lo scambio di informazioni tra l'NCSC e i fornitori di servizi di telecomunicazione è stato esplicitamente disciplinato nei capoversi 3 e 4 perché la maggior parte di questi ultimi, anche se probabilmente non tutti, rientra nella categoria delle infrastrutture critiche.

La seconda frase del capoverso 3 contenuta nella versione attuale, secondo la quale MELANI poteva trasmettere i dati per scopi di perseguimento penale solo con il consenso esplicito dei fornitori di dati, è stata eliminata. Questa norma è diventata superflua perché ora il direttore dell'NCSC ha il diritto di sporgere denuncia (cfr. art. 73*d* cpv. 3 D-LSIn).

Art. 76a Sostegno alle autorità

Si tratta di una disposizione nuova, che disciplina quali informazioni l'NCSC può mettere a disposizione di altre autorità, in quale misura e a quale scopo. Chiarisce in particolare la divisione dei ruoli tra l'NCSC e il SIC (cpv. 1) nonché il contenuto e le modalità della trasmissione di informazioni al SIC, le autorità di perseguimento penale e i servizi cantonali competenti per la cibersicurezza (cpv. 2–4).

Un aspetto importante della collaborazione tra l'NCSC e queste autorità è lo scambio di informazioni raccolte dall'NCSC sugli hacker stessi e sui metodi e le tattiche che utilizzano. Solo queste informazioni vengono messe a disposizione delle autorità.

67 FF **2017** 2563, in particolare 2675 seg.

Cpv. 1

Nel primo capoverso di questo articolo si stabilisce che l'NCSC sostiene il SIC nello svolgimento dei suoi compiti con specifiche valutazioni sul numero, sul tipo e sulla portata dei ciberattacchi nonché con analisi tecniche delle ciberminacce. Questo «quadro della situazione» non contiene informazioni o dati personali concreti o specifici, ma si limita a fornire valutazioni statistiche e tecniche necessarie per la valutazione della situazione di minaccia e per assicurare il servizio di preallerta. In virtù dell'articolo 6 capoverso 2 LAIn, il SIC è responsabile della valutazione della situazione di minaccia. Attraverso il servizio di segnalazione e il relativo obbligo, l'NCSC dispone di una fonte di informazioni importante in merito alla situazione di minaccia provocata dai ciberincidenti. Pertanto è in grado di inoltrare al SIC informazioni sul numero, sul tipo e sulla portata dei ciberattacchi, di fornirgli supporto attraverso analisi tecniche degli attacchi e inoltrargli le informazioni ottenute da queste analisi.

Cpv. 2, 3 e 4

Nei capoversi 2–4 vengono disciplinati il contenuto, l'entità nonché il tipo e le modalità dello scambio di informazioni operato tra l'NCSC e il SIC, le autorità di perseguimento penale e i servizi cantonali competenti per la cibersicurezza.

In termini di contenuto, il sostegno dell'NCSC consiste nel garantire alle autorità l'accesso alle informazioni sugli aggressori stessi e sui loro metodi e tattiche. 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. Concretamente si tratta di elementi di indirizzo (come il nome di dominio, l'indirizzo IP o indirizzi e-mail utilizzati indebitamente) o informazioni su transazioni finanziarie (conti bancari, numeri IBAN ecc.). Per lo scambio di informazioni in relazione a questi dati personali viene quindi definita una base legale.

Le autorità autorizzate secondo i capoversi 2–4 possono accedere alle suddette informazioni autonomamente. Questa procedura è opportuna, considerato l'elevato numero di ciberattacchi e di informazioni tecniche correlate.

Le altre informazioni ricevute dall'NCSC in relazione alle segnalazioni di ciberincidenti sono trasmesse unicamente in casi eccezionali e restano vincolate alle condizioni di cui all'articolo 73*c* D-LSIn.

Art. 77 Cooperazione a livello internazionale

Questa disposizione è stata modificata solo formalmente rispetto alla versione attuale. L'NCSC viene ora citato per nome. Inoltre, il termine «dati» è stato sostituito dal termine generico «informazioni» ed è stata chiarita la cerchia dei servizi esteri che possono beneficiare dello scambio di informazioni: si tratta dei servizi «competenti per la cibersicurezza». La formulazione attuale («competenti per la protezione di infrastrutture critiche») è troppo poco specifica e avrebbe potuto ostacolare lo scambio di informazioni con organizzazioni di importanza internazionale attive nel settore della cibersicurezza.

Cpv. 1 e 2

Il contenuto delle informazioni che l'NCSC trasmette a queste organizzazioni si limita all'identità e al modus operandi degli aggressori. L'entità è quindi la stessa del sostegno alle autorità descritta all'articolo 76*a* D-LSIn. La trasmissione di informazioni da parte dell'NCSC avviene ovviamente nel rispetto del diritto sulla protezione dei dati.

Le organizzazioni attive nel settore della cibersicurezza estere e internazionali devono utilizzare le informazioni dell'NCSC sulle caratteristiche e i metodi di attacco conformemente allo scopo previsto. L'NCSC garantisce il rispetto di tale principio utilizzando lo standard TLP, una classificazione delle informazioni degne di protezione, stabilita a livello internazionale, che specifica le condizioni di utilizzo e inoltro per ciascun livello di protezione.

Quando la presente revisione parziale entrerà in vigore, si applicherà già la nLPD. Perciò si fa già riferimento a essa.

Cpv. 3

La riserva sull'assistenza amministrativa e giudiziaria di cui all'attuale capoverso 3 è stata eliminata.

Con l'introduzione dell'obbligo di segnalazione, il contesto del capitolo 5 è cambiato. Il trattamento confidenziale delle segnalazioni da parte dell'NCSC ha assunto un peso ancora maggiore. Le segnalazioni all'NCSC e le loro analisi, in quanto basate su informazioni di terzi, sono state pertanto escluse dal campo di applicazione della LTras (cfr. art. 4 cpv. 1bis D-LSIn). Per lo stesso motivo, l'obbligo di denuncia dei reati per i collaboratori del servizio di segnalazione è stato circoscritto al direttore dell'NCSC. Allo stesso modo, il diritto di inoltrare informazioni in relazione ai ciberincidenti segnalati esiste solo in casi eccezionali, sempre che questi siano di notevole rilevanza per la sicurezza o il diritto penale (art. 73*d* D-LSIn).

In questa ottica, la riserva sull'assistenza amministrativa e giudiziaria può dare adito a malintesi. L'NCSC può fornire assistenza amministrativa solo se una disposizione materiale lo prevede. Anche in questi casi, può rilasciare informazioni solo in assenza di disposizioni contrarie concernenti la confidenzialità. Di fatto, l'NCSC potrà quindi fornire assistenza amministrativa solo in rari casi.

Art. 78 Sistema d'informazione per il sostegno alle infrastrutture critiche

In seguito alla revisione della LPD, questo articolo è superfluo e ne proponiamo dunque l'abrogazione.

Gli scopi per i quali l'NCSC tratta i dati derivano dai suoi compiti, già sufficientemente descritti negli articoli elencati. Tali compiti indicano per quali scopi i sistemi d'informazione dell'NCSC possono essere utilizzati nel trattamento di dati personali.

Art. 79 Conservazione e archiviazione dei dati

Il capoverso 1 è stato formulato in modo più rigoroso rispetto alla versione originariamente adottata dal Parlamento[68].

È stato precisato che i dati personali saranno conservati per un massimo di cinque anni dall'ultimo utilizzo per rilevare ciberminacce o per contrastare ciberincidenti. Il contesto in cui si inserisce questa regolamentazione è che alcune informazioni tecniche sui ciberincidenti, come il nome del dominio, l'indirizzo IP o gli indirizzi di posta elettronica utilizzati in modo improprio, sono di importanza fondamentale per il confronto di nuovi ciberincidenti e per l'analisi dei metodi e dei modelli di attacco. Senza questi dati comparativi, l'NCSC non può svolgere le sue analisi o non può farlo in modo mirato, che è un prerequisito fondamentale per l'adempimento dei suoi compiti.

L'NCSC deve quindi essere in grado di recuperare i set di dati a scopo comparativo anche se non vengono utilizzati per un periodo di tempo più lungo. Al proposito, il messaggio del 22 febbraio 2017[69] concernente la legge sulla sicurezza delle informazioni menziona che i vettori d'attacco possono mantenere la loro validità per diversi anni. Tuttavia, poiché questi dati tecnici contengono anche elementi personali e sono quindi assoggettati alla protezione dei dati come dati personali e l'anonimizzazione ostacolerebbe notevolmente o addirittura impedirebbe l'adempimento dei compiti, il periodo di conservazione dall'ultimo utilizzo è stato chiaramente limitato.

Per motivi di protezione dei dati, nella seconda parte della frase è stato aggiunto che i dati personali degni di particolare protezione possono essere conservati per un massimo di due anni dall'ultimo utilizzo. Questo chiarimento non è incluso nella versione attuale.

Art. 80 Disposizioni del Consiglio federale

Questo articolo è abrogato.

L'emanazione delle disposizioni di esecuzione compete al Consiglio federale anche senza riserva di legge (cfr. n. 4.3.3).

Legge federale del 21 giugno 2019[70] sugli appalti pubblici

Nella consultazione sull'avamprogetto è stato suggerito che i produttori di hardware o software che non risolvono una vulnerabilità scoperta in tempo utile dovrebbero essere ritenuti responsabili di questa cattiva condotta nell'ambito della legislazione sugli appalti pubblici[71].

Oltre all'interesse pubblico di non mettere a repentaglio la cibersicurezza attraverso vulnerabilità aperte, vi è anche l'interesse pubblico di escludere i produttori inadempienti dai contratti del settore pubblico. Le offerte con prodotti che contengono

68 «I servizi di cui all'articolo 74 capoverso 5 conservano i dati personali soltanto fino a che sono utili per prevenire minacce o individuare incidenti, ma al massimo per cinque anni» (art. 79 cpv. 1, versione del 18 dicembre 2020).
69 FF **2017** 2563, pag. 2677.
70 RS **172.056.1**
71 Cfr. presa di posizione di CH++.

vulnerabilità non risolte possono già essere escluse in base all'attuale situazione legale. I prodotti che non soddisfano (o non soddisfano più) i requisiti (ad es. che contengono vulnerabilità non risolte) hanno un difetto e quindi non soddisfano (o non soddisfano più) le specifiche tecniche se il difetto è rilevante per lo scopo previsto o atteso. Giacché le specifiche tecniche e gli standard industriali attuali devono essere sempre rispettati, le offerte in questione possono essere escluse in base all'articolo 44 capoverso 1 lettera a o b LAPub.[72]

Tuttavia, è ancora necessaria una possibilità esplicita di esclusione come conseguenza diretta di un comportamento non collaborativo da parte dei produttori nel processo di divulgazione coordinata delle vulnerabilità («coordinated vulnerability disclosure»). Solo se un produttore si impegna seriamente per risolvere le vulnerabilità è opportuno informarlo in merito alle stesse.

L'aggiunta della lettera f^{bis} all'elenco dei criteri di cui all'articolo 44 capoverso 1 LAPub crea la possibilità di escludere gli offerenti da futuri contratti o di rescindere i contratti esistenti come conseguenza diretta di un comportamento non cooperativo nella risoluzione delle vulnerabilità.

Affinché siano informati tempestivamente sulle vulnerabilità aperte nell'hardware o nel software, i servizi d'acquisto centrali, i responsabili della cibersicurezza e della gestione dei contratti possono partecipare allo scambio di informazioni dell'NCSC con le infrastrutture critiche.

Infine, occorre sottolineare che la nuova disposizione introdotta nella LAPub si applicherà solo a livello federale. È quindi in contraddizione con l'obiettivo principale della recente revisione totale della LAPub: l'armonizzazione della LAPub con il Concordato intercantonale sugli appalti pubblici (CIAP 2019).

Legge federale del 25 settembre 2020[73] sulla protezione dei dati

Per fare in modo che l'IFPDT nel corso dell'analisi di una violazione della sicurezza dei dati, segnalatagli dal titolare del trattamento in virtù dell'articolo 24 nLPD e dell'articolo 19 dell'ordinanza del 14 giugno 1993[74] relativa alla legge federale sulla protezione dei dati (OLPD), possa coinvolgere gli esperti dell'NCSC, all'articolo 24 capoverso 5bis D-nLPD viene stabilito che l'IFPDT ha la facoltà di inoltrare all'NCSC la notifica di una violazione della sicurezza dei dati.

La segnalazione inoltrata può contenere qualsiasi informazione ai sensi dell'articolo 19 capoverso 1 OLPD, purché si tratti di dati necessari all'NCSC per l'analisi dell'incidente. Le informazioni trasmesse dall'IFPDT all'NCSC possono contenere anche dati personali, compresi dati personali degni di particolare protezione relativi a perseguimenti o sanzioni amministrativi e penali riguardanti il titolare del trattamento assoggettato all'obbligo di notifica. Le informazioni necessarie per l'analisi di un incidente vengono selezionate caso per caso, ma non è escluso che esse contengano anche informazioni su un procedimento in corso e che l'NCSC ne venga così indiret-

72 Cfr. H. R. Trüeb, «Handkommentar zum Schweizerischen Beschaffungsrecht», Schulthess Verlag, Zurigo 2020, contributo di P. Locher sull'art. 44 LAPub, N12 e N13.
73 RS **235.1,** RU **2022** 491
74 RS **235.11**

tamente a conoscenza. È quindi necessario creare una base legale per la comunicazione di dati personali degni di particolare protezione.

In ogni caso è necessario che il titolare tenuto a inviare la notifica all'IFPDT abbia precedentemente fornito il suo consenso all'inoltro. L'inoltro delle informazioni non può comportare una violazione di quanto disposto dall'articolo 24 capoverso 6 nLPD, secondo cui la notifica può essere utilizzata nel quadro di un procedimento penale soltanto con il consenso della persona assoggettata. Ciò significa che un titolare potrà invocare il divieto di utilizzo ai sensi della nLPD anche se la sua notifica viene inoltrata all'NCSC. Il nuovo capoverso 5bis dell'articolo 24 D-nLPD non consente l'inoltro sistematico delle notifiche da parte dell'IFPDT all'NCSC, poiché prevede che l'IFPDT è autorizzato ad avvalersi di questa possibilità soltanto nei casi in cui sono necessarie le competenze tecniche dell'NCSC per effettuare chiarimenti su un determinato incidente.

Il diritto dell'IFPDT di inoltrare informazioni all'NCSC è limitato a uno scambio unilaterale di informazioni. Da parte sua, l'NCSC non fornisce all'IFPDT informazioni provenienti da segnalazioni, anche se queste concernono violazioni della sicurezza dei dati. Tuttavia, l'NCSC mette a disposizione un sistema elettronico che consente ai segnalanti di inoltrare la segnalazione o parti di essa. Il segnalante ha quindi la possibilità di utilizzare il modulo di segnalazione anche per notificare all'IFPDT una violazione della sicurezza dei dati.

La nLPD dovrebbe entrare in vigore nel settembre del 2023, ossia poco dopo l'entrata in vigore della LSIn (senza il presente disegno di legge). La presente revisione del capitolo 5 della LSIn non entrerà in vigore prima della fine del 2023; nel frattempo, la normativa prevista dall'articolo 24 capoverso 5bis D-LSIn si applicherà già a livello di ordinanza (cfr. art. 41 cpv. 1 dell'ordinanza del 31 agosto 2022[75] sulla protezione dei dati [OPDa]). Con l'entrata in vigore del presente disegno di legge, il Consiglio federale abrogherà questa disposizione dell'OPDa.

Legge federale del 21 marzo 2003[76] sull'energia nucleare (LENu)

Con l'introduzione dell'articolo 102 capoverso 2 D-LENu, il legislatore crea una base legale esplicita affinché l'IFSN, quale servizio di segnalazione settoriale, possa inoltrare all'NCSC, quale servizio di segnalazione intersettoriale, una notifica concernente un ciberattacco a un impianto nucleare che soddisfi i requisiti dell'articolo 74*d* D-LSIn. In tal modo, l'NCSC riceverà le segnalazione di simili ciberattacchi senza influenzare i processi stabiliti per gli impianti nucleari.

Legge del 23 marzo 2007[77] sull'approvvigionamento elettrico (LAEl)

Uno studio commissionato dall'Ufficio federale dell'energia ha individuato un'elevata necessità di regolamentazione della cibersicurezza nel settore energetico, cruciale

75 RS **235.11**, RU **2022** 568
76 RS **732.1**
77 RS **734.7**

per l'approvvigionamento economico e la sicurezza del Paese[78]. I risultati mostrano che le linee guida del settore, disponibili da anni e basate su principi sussidiari, non hanno portato a una protezione adeguata contro le ciberminacce. La protezione contro le ciberminacce, che proponiamo di sancire esplicitamente nel nuovo articolo 8*a* D-LAEl, serve a garantire la sicurezza dell'approvvigionamento.

Le misure da adottare secondo il capoverso 1 sono volte a prevenire i ciberincidenti e quindi, in particolare, i malfunzionamenti degli impianti corrispondenti, o a porvi rimedio il più rapidamente possibile. Oltre ai gestori di rete che influenzano direttamente il funzionamento della rete attraverso la tecnologia di controllo, l'obbligo si applica anche ai produttori (ad es. i gestori di impianti eolici o idroelettrici) e ai gestori di impianti di stoccaggio, soprattutto perché possono esercitare un'influenza significativa sulla sicurezza dell'approvvigionamento attraverso l'immissione e l'erogazione di energia. Il grado di protezione appropriato dipende dall'influenza del corrispondente attore sulla sicurezza dell'approvvigionamento (ad es. livello della rete, potenza allacciata, potenza dell'impianto, numero di consumatori finali interessati).

Sulla base della sua competenza generale sussidiaria (cfr. art. 22 cpv. 1 LAEl), la Commissione federale dell'energia elettrica (ElCom) vigilerà sul rispetto dell'articolo 8*a* D-LAEl. Il nostro Consiglio emanerà le relative disposizioni di esecuzione, in particolare per quanto riguarda il livello di protezione e le verifiche (ad es. obblighi di documentazione all'attenzione della ElCom). In tale contesto il nostro Collegio, ai sensi del principio di sussidiarietà (art. 3 cpv. 2 LAEl), si baserà sulle linee guida pertinenti del settore (ad es. il manuale *Handbuch Grundschutz für «Operational Technology» in der Stromversorgung* dell'Associazione delle aziende elettriche svizzere, edizione luglio 2018, attualmente in rielaborazione), che potrà anche dichiarare vincolanti.

La disposizione di cui al capoverso 2 consente al nostro Consiglio di assoggettare all'obbligo di cui al capoverso 1 determinati fornitori attivi nel settore dell'approvvigionamento elettrico. Ciò è ipotizzabile, ad esempio, nei settori del commercio, della misurazione, del controllo, della flessibilità, dell'elaborazione dei dati o dell'elettromobilità. In considerazione dell'obiettivo della disposizione, sono ammissibili solo gli attori che esercitano un'influenza significativa sulla sicurezza dell'approvvigionamento. Ciò avviene in particolare se i fornitori di servizi, nell'ambito delle loro prestazioni, possono accedere ai sistemi di controllo di un gran numero di imprese di approvvigionamento elettrico e quindi un gran numero di consumatori finali sarebbe interessato, oppure se, ad esempio nel settore dell'elettromobilità o della produzione decentrata, controllano un'ampia produzione nel sistema di approvvigionamento elettrico attraverso l'aggregazione.

Il nostro Collegio può anche prevedere eccezioni in virtù del capoverso 2, ad esempio per i gestori di sistemi di distribuzione con pochi consumatori finali o per i produttori con impianti a bassa potenza. Sono inoltre ipotizzabili anche eccezioni per le imprese che devono già adottare direttive nel settore del ciberspazio a seguito di altre direttive

78 Cfr. il rapporto del 28.6.2021 «Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung», consultabile al sito: www.bfe.admin.ch > Approvvigionamento > Digitalizzazione nel mondo dell'energia > Cyber Security.

legali speciali (ad es. nel settore della corrente di trazione). In questo caso è necessario un adeguato coordinamento a livello di ordinanza.

Legge del 22 giugno 2007[79] *sulla vigilanza dei mercati finanziari (LFINMA)*

Anche nel settore dei mercati finanziari vige l'obbligo di notificare ciberattacchi; l'autorità di vigilanza FINMA riceve tali notifiche. Poiché esistono quindi obblighi di segnalazione paralleli per gli attori dei mercati finanziari in caso di ciberattacchi, l'NCSC imposterà il sistema di segnalazione elettronica in modo tale che i segnalanti possano utilizzare anche l'apposito modulo dell'NCSC per la FINMA.

A prescindere dagli obblighi di notifica paralleli, la FINMA deve poter trasmettere informazioni non pubbliche all'NCSC in caso di ciberattacco, se ciò è necessario per l'adempimento dei compiti dell'NCSC. A tale scopo, proponiamo di aggiungere nell'articolo 39 capoverso 1 LFINMA l'NCSC all'elenco delle altre autorità nazionali, creando così la base legale per la trasmissione di informazioni all'NCSC.

6 Ripercussioni

6.1 Ripercussioni per la Confederazione

L'NCSC gestisce già oggi un servizio di contatto che riceve le segnalazioni di ciberincidenti effettuate su base volontaria. La sua attività si basa sulla pluriennale esperienza maturata con MELANI, la centrale che dal 2004 ha raccolto in particolare le segnalazioni delle infrastrutture critiche.

6.1.1 Ripercussioni finanziarie

Per la ricezione delle segnalazioni l'NCSC gestisce già oggi un modulo digitale che può essere adattato anche per la ricezione delle segnalazioni inviate in adempimento dell'obbligo di segnalazione. La necessaria armonizzazione con gli altri servizi che ricevono già segnalazioni di questo tipo – come l'IFPDT, la FINMA e l'IFSN – e l'approntamento del modulo di segnalazione richiederanno lavoro aggiuntivo nella fase iniziale, che tuttavia potrà essere compensato con le risorse a disposizione dell'NCSC. Per la successiva gestione, però, l'NCSC deve poter garantire che le segnalazioni inviate in adempimento dell'obbligo siano registrate, quietanzate e documentate correttamente e che siano inoltrate al servizio preposto ai fini della preallerta. Questo rappresenta un onere supplementare che va considerato nella fase di potenziamento dell'NCSC.

79 RS **956.1**

6.1.2 Ripercussioni sull'effettivo del personale

Dopo un ciberattacco l'NCSC avrà 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 dall'NCSC (e prima ancora da MELANI) ma che sicuramente dopo l'introduzione dell'obbligo di segnalazione richiederà un impegno maggiore. Questo perché molto probabilmente l'NCSC riceverà più segnalazioni e sarà anche tenuto a fornire almeno una prima valutazione e raccomandazioni su come contrastare l'incidente. Di conseguenza anche il team dell'NCSC addetto all'analisi tecnica (GovCERT) dovrà essere potenziato. Al momento, l'onere supplementare per il personale che ne deriva non può ancora essere stimato con sufficiente precisione. Inoltre, esso non può essere valutato separatamente dal futuro orientamento della SNPC 2018–2022 e dalla forma organizzativa dell'NCSC, attualmente in fase di chiarimento da parte del nostro Consiglio. Tale onere si concretizzerà al momento dell'emanazione delle disposizioni di esecuzione e sarà quindi oggetto di una richiesta separata.

6.2 Ripercussioni per i Cantoni e i Comuni, per le città, gli agglomerati e le regioni di montagna

Con questo progetto non verranno assegnati nuovi compiti ai Cantoni e ai Comuni, ma l'obbligo di segnalazione li riguarderà comunque per due motivi: in primo luogo perché le autorità cantonali e comunali sono esse stesse assoggettate all'obbligo di segnalazione ai sensi dell'articolo 74*b* capoverso 1 lettera b D-LSIn; in secondo luogo perché molte delle imprese assoggettate all'obbligo sottostanno a enti cantonali o comunali.

I Cantoni e i Comuni, tuttavia, potranno anche approfittare delle prestazioni di servizi offerte dall'NCSC per potersi proteggere meglio dalle ciberminacce. Già oggi numerosi Cantoni e città partecipano allo scambio di informazioni tra infrastrutture critiche e NCSC.

6.3 Ripercussioni sull'economia, sulla società e sull'ambiente

Non sono attese ripercussioni dirette sull'economia nazionale, sulla società e sull'ambiente. Tuttavia l'economia nazionale e la società trarranno indirettamente beneficio dall'introduzione dell'obbligo di segnalare ciberattacchi, in quanto il miglioramento della cibersicurezza delle infrastrutture critiche permetterà anche, in generale, di proteggere meglio la cibersicurezza in Svizzera. Inoltre, grazie all'attuazione tempestiva di adeguate misure di prevenzione e di difesa, l'obbligo di segnalazione 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.

Visto che l'introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche avrà ripercussioni minime se non nulle sull'economia nazionale e sulle imprese interessate, si può fare a meno di un'analisi d'impatto della regolamentazione.

L'obbligo aiuta a fare luce sulla minaccia rappresentata dai ciberattacchi e contribuisce a sensibilizzare la popolazione sulle ciberminacce. Una maggiore competenza della popolazione in questo ambito è un requisito importante per il successo della digitalizzazione della società.

7 Aspetti giuridici

7.1 Costituzionalità

Nella Costituzione federale (Cost.) non è presente una base legale esplicita per l'introduzione di un obbligo di segnalare ciberattacchi. La Confederazione può però basarsi sulla sua competenza inerente per la tutela della sicurezza interna ed esterna della Confederazione per l'introduzione dell'obbligo di segnalare 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 segnalare ciberattacchi 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 serve inoltre ad analizzare, attraverso le segnalazioni, la situazione di minaccia per poter preallertare gli attori coinvolti e implementare misure di difesa. Dato questo scopo, ne deriva che il campo di applicazione dell'obbligo deve essere limitato ai ciberattacchi a infrastrutture critiche. Il diritto di segnalare ciberincidenti e vulnerabilità, che integra altre strategie per la raccolta di informazioni, rappresenta a titolo complementare un aiuto per la protezione delle infrastrutture critiche.

Di conseguenza, la competenza federale inerente per la tutela 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 segnalare ciberattacchi e un diritto di segnalare ciberincidenti e vulnerabilità.

Riguardo a questa competenza federale inerente, in base a quanto sancito da una convezione sulla tecnica legislativa formale[80], viene citato a titolo sussidiario l'articolo 173 capoverso 2 Cost. La LSIn 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.

80 N. marg. 25 delle Direttive di tecnica legislativa, consultabili al sito: www.bk.admin.ch > Documentazione > Accompagnamento legislativo > Direttive di tecnica legislativa DTL.

7.2 Compatibilità con gli impegni internazionali della Svizzera

L'introduzione dell'obbligo di segnalare ciberattacchi non riguarda alcun impegno attuale della Svizzera a livello internazionale. Questo obbligo di segnalazione è analogo a quello che molti altri Stati, in particolare gli Stati membri dell'UE, hanno introdotto negli ultimi anni.

7.3 Forma dell'atto

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

Per quanto riguarda le disposizioni di esecuzione dell'obbligo di segnalazione, deve essere ancora deciso se sarà necessario creare un'ordinanza a parte o se verranno integrate ordinanze esistenti.

7.4 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).

7.5 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 segnalare 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 segnalazione uguale per tutti e un servizio centrale di segnalazione, 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 segnalazione 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 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 segnalazione, questo principio è garantito in quanto i costi per la gestione del servizio centrale di segnalazione saranno a carico della Confederazione. Per le infrastrutture critiche cambierà poco, perché, come in passato, potranno contare sul supporto dell'NCSC per la gestione degli incidenti. Rispetto alla segnalazione volontaria di ciberincidenti, l'obbligo di segnalazione 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.

7.6 Delega di competenze legislative

Il presente disegno prevede di sancire a livello di legge i principi fondamentali per l'introduzione dell'obbligo di segnalare ciberattacchi.

Il nostro Consiglio emanerà disposizioni di esecuzione per concretizzare le disposizioni di legge, se necessario. In particolare, ai sensi dell'articolo 74*c* D-LSIn spetta al nostro Collegio il compito di restringere ulteriormente la cerchia degli assoggettati all'obbligo di segnalazione. 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 es. attraverso la definizione di valori di soglia adeguati).

7.7 Protezione dei dati e principio della trasparenza

Il disegno 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 sostegno per le infrastrutture critiche.

Il disegno prevede tuttavia una nuova disposizione (art. 4 cpv. 1bis D-LSIn), secondo cui le informazioni di terzi che sono state trasmesse all'NCSC nell'ambito dell'obbligo di segnalazione o di cui l'NCSC è venuto a conoscenza tramite l'analisi di tali segnalazioni non possono essere rese accessibili al pubblico secondo la LTras.

L'IFPDT non condivide questa disposizione. A suo parere, questa eccezione violerebbe il principio della trasparenza, precludendo ai cittadini l'accesso a informazioni direttamente correlate all'adempimento di un compito centrale dell'NCSC e rendendo più difficile il controllo pubblico in un settore sensibile. Inoltre ritiene l'elevato numero di eccezioni previste dalla LTras sufficiente a tutelare i differenti interessi, cosicché l'introduzione di una nuova eccezione risulta superflua. L'IFPDT non vede

come l’applicazione della LTras possa compromettere la funzione dell’NCSC quale servizio di segnalazione.