Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Il Consiglio federale

Avvio della procedura di consultazione concernente l'introduzione dell'obbligo di notifica dei ciberattacchi

Berna, 12.01.2022 - Nella seduta del 12 gennaio 2022 il Consiglio federale ha avviato la procedura di consultazione concernente l'introduzione dell'obbligo di notifica dei ciberattacchi per i gestori di infrastrutture critiche. Il progetto pone le basi legali necessarie per l'obbligo di notifica e definisce i compiti del Centro nazionale per la cibersicurezza (NCSC), che fungerà da servizio centrale per la notifica dei ciberattacchi. La procedura di consultazione termina il 14 aprile 2022.

I ciberattacchi sono diventati una seria minaccia per la sicurezza e l'economia della Svizzera. Imprese e autorità sono oggetto di attacchi ogni giorno. In media ogni settimana giungono al NCSC oltre 300 segnalazioni di ciberattacchi, tentati o riusciti. Le segnalazioni provenienti da imprese, autorità e privati avvengono su base volontaria e permettono alle competenti autorità federali di valutare le minacce e individuare tempestivamente il tipo di attacco. Il Consiglio federale intende rafforzare il sistema di notifica obbligando i gestori di infrastrutture critiche a segnalare i ciberattacchi al NCSC. L'obbligo di notifica ha lo scopo di garantire a quest'ultimo la possibilità di avere un quadro della situazione più chiaro grazie alle informazioni complete ricevute e informare tempestivamente altri gestori di infrastrutture critiche.

Obbligo di notifica per le infrastrutture critiche

L'obbligo di notifica per i gestori di infrastrutture critiche deve applicarsi ai ciberattacchi che possono arrecare notevoli danni, in particolare a quelli che rischiano di compromettere il funzionamento delle infrastrutture critiche o connessi al reato di estorsione, minaccia o coazione. La funzione di servizio centrale di notifica verrebbe assunta dal NCSC. Per semplificare la notifica il più possibile, il NCSC metterà a disposizione un modulo elettronico che permetterà, se lo si desidera, di trasmettere la notifica direttamente ad altri servizi.

Obbligo di sostegno della Confederazione in caso di ciberattacchi

Il progetto non soltanto obbliga le imprese a collaborare nella protezione dai ciberattacchi, ma definisce anche i compiti della Confederazione a sostegno dell'economia e della popolazione. A tal fine, il NCSC è incaricato di avvertire il pubblico riguardo alle ciberminacce e di sensibilizzarlo sui rischi. Inoltre, deve ricevere le notifiche di ciberincidenti e vulnerabilità, elaborare analisi tecniche e fornire raccomandazioni sul modo di procedere alle persone che notificano incidenti. Il NCSC sostiene i gestori di infrastrutture critiche (incluse le autorità cantonali e comunali) nella gestione di ciberincidenti. Questo sostegno è inteso come un servizio di pronto intervento e non deve entrare in concorrenza con altri servizi disponibili sul mercato.

Finora i compiti di protezione dai ciber-rischi sono stati adempiuti dalla Confederazione sulla base dei mandati esistenti, ma non erano ancora stati sanciti a livello di legge. Con l'introduzione dell'obbligo di notifica nella legge sulla sicurezza delle informazioni (LSIn), ora si devono definire nella stessa LSIn anche i compiti del NCSC, in particolare la sua competenza in qualità di servizio di notifica.

La procedura di consultazione termina il 14 aprile 2022.

Indirizzo cui rivolgere domande

Comunicazione,
Dipartimento federale delle finanze DFF
Tel. +41 58 462 60 33, info@gs-efd.admin.ch

Documenti

Legge (PDF, 352 kB)

Rapporto esplicativo (PDF, 686 kB)

Lettera ai cantoni (PDF, 168 kB)

Lettera alle organizzazioni (PDF, 162 kB)

Liste der Vernehmlassungsadressaten - Liste des destinataires - Elenco dei destinatari (PDF, 172 kB)

Pubblicato da

Il Consiglio federale
https://www.admin.ch/gov/it/pagina-iniziale.html

Dipartimento federale delle finanze

https://www.efd.admin.ch/efd/it/home.html

Dipartimento federale della difesa, della protezione della popolazione e dello sport
http://www.vbs.admin.ch

https://www.admin.ch/content/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-86768.html

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Centro nazionale per la cibersicurezza (NCSC)

Berna, 12 gennaio 2022

Procedura di consultazione

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

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

Rapporto esplicativo

Indice

Compendio

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

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

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

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

Rapporto esplicativo

1 Situazione iniziale

1.1 Necessità di agire e obiettivi

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

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

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

1.2 Alternative esaminate e opzione scelta

1.2.1 Potenziamento dello scambio di informazioni su base volontaria

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.2.3 Applicazione dell'obbligo di notifica attraverso incentivi e sanzioni

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

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

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

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

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

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

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

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

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

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

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

2 Diritto comparato, in particolare rapporto con il diritto europeo

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

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

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

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

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

3 Punti essenziali del progetto

3.1 La normativa proposta

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

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

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

3.2 Compatibilità tra compiti e finanze

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

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

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

3.3 Attuazione

3.3.1 Necessità di una base legale

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

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

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

3.3.2 La LSIn come base giuridica adatta

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

3.3.3 Disposizioni di esecuzione

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

3.3.4 Attuabilità dell'obbligo di notifica

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

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

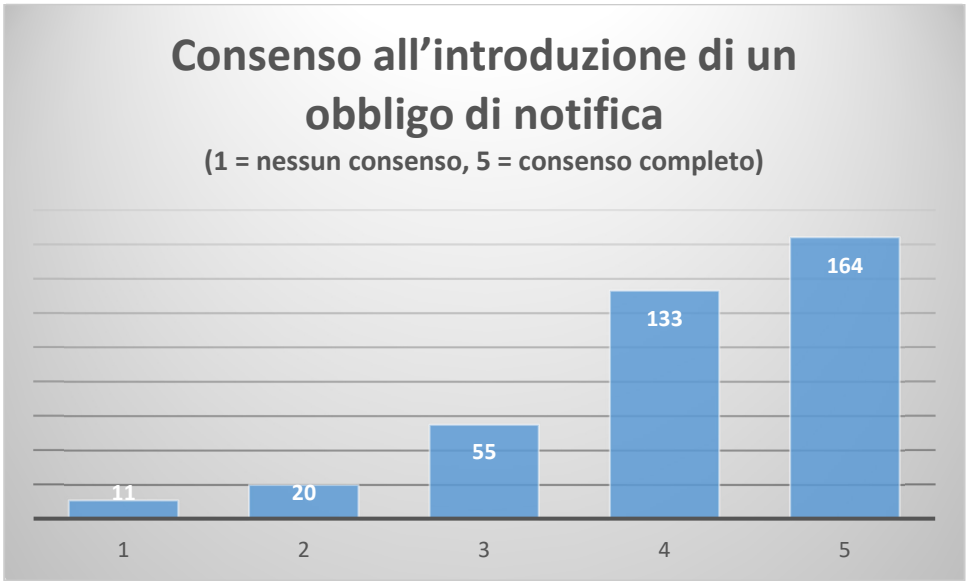

Figura 1 Valutazione della proposta di introdurre un obbligo di notifica

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

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

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

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

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

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

4 Commento ai singoli articoli

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

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

Capitolo 1: Disposizioni generali

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

Articolo 1 Scopo

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

Articolo 2 Autorità e organizzazioni assoggettate

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

Articolo 5 Definizioni

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

Lettera d

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

Lettera e

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

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

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

Sezione 1: Disposizioni generali

Articolo 73a Principio

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

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

Articolo 73b Trattamento delle notifiche di ciberincidenti e vulnerabilità

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

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

Capoverso 1

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

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

Capoverso 2

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

Capoverso 3

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

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

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

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

Articolo 73c Inoltro di informazioni

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

Capoverso 1

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

Capoverso 2

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

Capoverso 3

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

Capoverso 4

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

Articolo 74 Sostegno ai gestori di infrastrutture critiche

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

Capoverso 2

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

Lettera a

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

Lettera b

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

Lettera c

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

Capoverso 3

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

Capoverso 4

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

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

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

Sezione 2: Obbligo di notifica di ciberattacchi a infrastrutture critiche

Articolo 74a Obbligo di notifica

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

Articolo 74b Settori

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

Lettera a: scuole universitarie

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

Lettera b: autorità

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

Lettera c: organizzazioni cui sono affidati compiti di diritto pubblico

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

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

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

Lettera e: banche, assicurazioni e infrastrutture del mercato finanziario

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

Lettera f: servizi digitali

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

Lettera g: ospedali

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

Lettera h: laboratori medici

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

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

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

Lettera j: assicurazioni sociali

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

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

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

Lettera k: fornitori di servizi di telecomunicazione

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

Lettera l: Società svizzera di radiotelevisione (SSR)

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

Lettera m: agenzie di stampa d'importanza nazionale

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

Lettera n: fornitori di servizi postali

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

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

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

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

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

Lettera p: imprese dell'aviazione civile

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

Lettera q: navigazione sul Reno

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

Lettera r: approvvigionamento di beni indispensabili di uso quotidiano

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

Lettera s: produttori di hardware e software

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

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

Articolo 74c Eccezioni all'obbligo di notifica

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

34 RS **747.30**

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

Articolo 74d Ciberattacchi da notificare

Capoverso 1

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

Capoverso 2

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

Articolo 74e Contenuto della notifica

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

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

Articolo 74f Trasmissione della notifica

Capoverso 1

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

Capoverso 2

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

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

Capoverso 3

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

Articolo 74g Obbligo d'informazione

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

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

Capoverso 1

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

Capoverso 2

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

Articolo 74i Infrazioni contro le decisioni del NCSC

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

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

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

Capoverso 1

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

Capoversi 2 e 3

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

Capoverso 4

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

Sezione 3: Protezione dei dati e scambio di informazioni

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

Articolo 75 Trattamento di dati personali

Capoverso 1

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

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

Capoverso 2

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

Capoverso 3

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

Articolo 76 Cooperazione a livello nazionale

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

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

Capoversi 1 e 2

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

Capoversi 3 e 4

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

Articolo 76a Sostegno alle autorità

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

Capoverso 1

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

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

Capoversi 2, 3 e 4

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

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

Articolo 77 Cooperazione a livello internazionale

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

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

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

Articolo 79 Conservazione e archiviazione dei dati

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

Articolo 80 Disposizioni del Consiglio federale

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

Allegato 1 (Articolo 89 Modifica di altri atti normativi)

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

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

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

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

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

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

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

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

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

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

5 Ripercussioni

5.1 Ripercussioni per la Confederazione

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

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

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

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

5.2 Ripercussioni per i Cantoni e i Comuni

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

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

5.3 Ripercussioni sull'economia e sulla società

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

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

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

6 Aspetti giuridici

6.1 Costituzionalità

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

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

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

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

6.2 Compatibilità con gli impegni internazionali della Svizzera

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

6.3 Forma dell'atto

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

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

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

6.4 Subordinazione al freno alle spese

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

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

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

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

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

6.6 Delega di competenze legislative

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

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

6.7 Protezione dei dati

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

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

«$$QrCode»

Legge federale sulla sicurezza delle informazioni in seno alla Confederazione

(Legge sulla sicurezza delle informazioni, LSIn)

Modifica del …

L'Assemblea federale della Confederazione Svizzera,
visto il messaggio del Consiglio federale del …,
decreta:

I

La legge del 18 dicembre 2020[1] sulla sicurezza delle informazioni è modificata come segue:

Art. 1 cpv. 1

[1] La presente legge ha lo scopo di:

a. garantire il trattamento sicuro delle informazioni di competenza della Confederazione nonché l'impiego sicuro dei mezzi informatici della Confederazione;

b. aumentare la resilienza ai ciber-rischi della Svizzera.

Art. 2 cpv. 5

[5] Alle organizzazioni di diritto pubblico o privato che gestiscono infrastrutture critiche ma che non sono contemplate ai capoversi 1–3 si applicano gli articoli 73*a*–79. La legislazione speciale può dichiarare applicabili altre disposizioni della presente legge.

RS **126**
1 RS **126** [FF **2020** 8755]

Art. 5 lett. d ed e

Ai sensi della presente legge s'intende per:

d. *ciberincidente:* un evento che si verifica nell'esercizio di mezzi informatici e che può compromettere la confidenzialità, l'integrità o l'accessibilità delle informazioni o la tracciabilità del loro trattamento;

e. *ciberattacco:* un ciberincidente provocato intenzionalmente da persone non autorizzate.

Titoli prima dell'art. 73a

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

Sezione 1: Disposizioni generali

Art. 73a Principio

Ai fini della protezione della Svizzera contro i ciber-rischi, il Centro nazionale per la cibersicurezza (NCSC) svolge in particolare i seguenti compiti:

a. sensibilizzare il pubblico sui ciber-rischi;

b. avvertire riguardo ai ciber-rischi e alle vulnerabilità nei mezzi informatici;

c. pubblicare informazioni sulla cibersicurezza e istruzioni per l'adozione di misure preventive e reattive contro i ciber-rischi;

d. elaborare analisi tecniche per valutare i ciber-rischi e difendersi da essi;

e. ricevere e trattare le notifiche di ciberincidenti e vulnerabilità nei mezzi informatici;

f. sostenere i gestori di infrastrutture critiche.

Art. 73b Trattamento delle notifiche di ciberincidenti e vulnerabilità

[1] Se gli sono notificati ciberincidenti o vulnerabilità nei mezzi informatici, il NCSC analizza la loro rilevanza ai fini della protezione della Svizzera contro i ciber-rischi. Su richiesta della persona che presenta la notifica, il NCSC fornisce raccomandazioni su come procedere, sempre che a tal fine non siano necessari ulteriori analisi e chiarimenti.

[2] Il NCSC può pubblicare o inoltrare alle autorità e alle organizzazioni interessate informazioni sui ciberincidenti, sempre che ciò serva a prevenire o a contrastare eventuali ciberattacchi. Tali informazioni possono contenere dati personali o dati di persone giuridiche, a condizione che si tratti di caratteristiche identificative ed elementi di indirizzo utilizzati abusivamente e la persona interessata vi acconsenta.

[3] Se gli viene segnalata una vulnerabilità, il NCSC informa immediatamente il produttore e gli impartisce un congruo termine per eliminarla. Se il produttore non la elimina entro il termine impartito, il NCSC pubblica la vulnerabilità indicando i software o gli hardware interessati, sempre che ciò contribuisca alla protezione contro i ciber-rischi.

Art. 73c Inoltro di informazioni

[1] Se dalla notifica di un ciberincidente o dalla sua analisi emergono informazioni rilevanti per individuare tempestivamente e sventare minacce per la sicurezza interna o esterna, valutare la situazione di minaccia o assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche conformemente all'articolo 6 capoversi 1 lettera a, 2 e 5 della legge federale del 25 settembre 2015[2] sulle attività informative (LAIn), il NCSC inoltra queste informazioni al SIC.

[2] L'obbligo di denuncia di cui all'articolo 22*a* della legge sul personale federale[3] non si applica ai collaboratori del NCSC che constatano indizi di un possibile reato nell'ambito della notifica di un ciberincidente o delle relative analisi. Il responsabile del NCSC può sporgere denuncia, sempre che ciò appaia opportuno in considerazione della gravità del possibile reato.

[3] Le informazioni rese note da una persona nel quadro di una notifica al NCSC possono essere usate in un procedimento penale contro detta persona soltanto con il suo consenso.

[4] Il NCSC può inoltrare informazioni che rivelano segreti protetti dalla legislazione penale esclusivamente secondo quanto disposto dall'articolo 320 del Codice penale[4].

Art. 74 Sostegno ai gestori di infrastrutture critiche

[1] Il NCSC sostiene i gestori di infrastrutture critiche nella protezione contro i ciber-rischi.

[2] A tal fine mette a loro disposizione in particolare i seguenti strumenti:

a. un sistema di comunicazione per lo scambio sicuro delle informazioni;

b. informazioni tecniche sui ciber-rischi e sulle vulnerabilità attuali nonché raccomandazioni per l'adozione di misure preventive;

c. strumenti tecnici e istruzioni per l'individuazione di ciberincidenti che si basano sul bisogno di protezione elevato delle infrastrutture critiche.

[3] Il NCSC consiglia e sostiene i gestori di infrastrutture critiche nella gestione di ciberincidenti e nell'eliminazione di vulnerabilità se per l'infrastruttura critica sussiste il rischio imminente di conseguenze gravi e, nel caso si tratti di gestori privati, non vi è la possibilità di procurarsi per tempo un sostegno equivalente sul mercato.

2 RS **121**
3 RS **172.220.1**
4 RS **311.0**

[4] Con il consenso dei gestori interessati, può accedere alle loro informazioni e ai loro mezzi informatici al fine di analizzare un ciberincidente. Tale consenso può essere accordato indipendentemente da eventuali obblighi di tutela del segreto.

Titolo prima dell'art. 74a

Sezione 2: Obbligo di notifica di ciberattacchi a infrastrutture critiche

Art. 74a Obbligo di notifica

I gestori di infrastrutture critiche che scoprono eventuali ciberattacchi devono notificarli il prima possibile al NCSC affinché quest'ultimo riconosca tempestivamente i modelli di attacco, avverta i potenziali interessati e possa raccomandare loro opportune misure di prevenzione e difesa.

Art. 74b Settori

L'obbligo di notifica si applica:

a. alle scuole universitarie secondo l'articolo 2 capoverso 2 della legge federale del 30 settembre 2011[5] sulla promozione e sul coordinamento del settore universitario svizzero;

b. alle autorità federali, cantonali o comunali nonché alle organizzazioni intercantonali, cantonali e intercomunali;

c. alle organizzazioni cui sono affidati compiti di diritto pubblico nei settori della sicurezza e del salvataggio, dell'approvvigionamento di acqua potabile, del trattamento delle acque di scarico e dello smaltimento dei rifiuti;

d. alle imprese attive nel settore dell'approvvigionamento energetico secondo l'articolo 6 capoverso 1 della legge federale del 30 settembre 2016[6] sull'energia nonché nel commercio, nella misurazione e nella gestione dell'energia;

e. alle imprese che sottostanno alla legge dell'8 novembre 1934[7] sulle banche, alla legge del 17 dicembre 2004[8] sulla sorveglianza degli assicuratori e alla legge del 22 giugno 2007[9] sulla vigilanza dei mercati finanziari;

f. ai fornitori di piattaforme per il commercio elettronico, di servizi di cloud computing, di motori di ricerca e di altri servizi digitali nonché ai centri di registrazione di nomi di dominio e ai gestori di centri di calcolo, che in Svizzera:

    1. sono utilizzati da un gran numero di utenti,

    2. rivestono un'importanza notevole per l'economia digitale, o

5 RS **414.20**
6 RS **730.0**
7 RS **952.0**
8 RS **961.01**
9 RS **956.1**

3. offrono servizi di sicurezza e fiduciari;

g. agli ospedali che figurano nell'elenco compilato dal Cantone di cui all'articolo 39 capoverso 1 lettera e della legge federale del 18 marzo 1994[10] sull'assicurazione malattie;

h. ai laboratori medici che dispongono di un'autorizzazione secondo l'articolo 16 capoverso 1 della legge del 28 settembre 2012[11] sulle epidemie;

i. alle imprese che dispongono di un'autorizzazione secondo la legge del 15 dicembre 2000[12] sugli agenti terapeutici (LATer) per la fabbricazione, l'immissione in commercio e l'importazione di medicamenti o che fabbricano o smerciano dispositivi medici di cui all'articolo 4 capoverso 1 lettera b LATer;

j. alle organizzazioni che forniscono prestazioni delle assicurazioni sociali volte a coprire le conseguenze di malattie, infortuni, incapacità al lavoro e al guadagno, vecchiaia, invalidità e grande invalidità;

k. ai fornitori di servizi di telecomunicazione secondo l'articolo 3 lettera b LTC;

l. alla Società svizzera di radiotelevisione;

m. alle agenzie di stampa d'importanza nazionale;

n. ai fornitori di servizi postali registrati presso la Commissione delle poste secondo l'articolo 4 capoverso 1 della legge del 17 dicembre 2010[13] sulle poste;

o. alle imprese di trasporto che sottostanno alla legge federale del 18 giugno 2010[14] sugli organi di sicurezza delle imprese di trasporto pubblico;

p. alle imprese dell'aviazione civile che dispongono di un'autorizzazione dell'Ufficio federale dell'aviazione civile;

q. alle imprese che trasportano merci sul Reno secondo la legge federale del 23 settembre 1953[15] sulla navigazione marittima sotto bandiera svizzera nonché alle imprese che gestiscono l'iscrizione, il carico o lo scarico nei porti basilesi;

r. alle imprese che riforniscono la popolazione di beni indispensabili di uso quotidiano;

s. ai produttori di hardware e software i cui prodotti sono utilizzati da infrastrutture critiche, sempre che tali hardware o software abbiano accesso al sistema per la manutenzione remota o siano impiegati per uno dei seguenti scopi:

1. tecnica di comando e monitoraggio di sistemi;
2. esercizio di dispositivi medici e di impianti di telecomunicazione;
3. garanzia della sicurezza pubblica;

10 RS **832.10**
11 RS **818.101**
12 RS **812.21**
13 RS **783.0**
14 RS **745.2**
15 RS **747.30**

4. sicurezza informatica, crittografia, identificazione, attribuzione di diritti di accesso a sistemi o luoghi.

Art. 74c Eccezioni all'obbligo di notifica

Il Consiglio federale esenta determinate categorie di gestori di infrastrutture critiche dall'obbligo di notifica se i guasti funzionali o i malfunzionamenti causati alle loro infrastrutture da ciberattacchi:

a. sono improbabili, in particolare a seguito di un basso grado di accoppiamento dei mezzi informatici; o

b. possono avere soltanto ripercussioni minime sul funzionamento dell'economia o il benessere della popolazione, in particolare perché:

1. riguardano unicamente un numero esiguo di persone,

2. sono neutralizzati dall'intervento di altre infrastrutture critiche, o

3. comporterebbero solo modesti danni potenziali per l'economia.

Art. 74d Ciberattacchi da notificare

[1] Un ciberattacco a un'infrastruttura critica deve essere notificato se vi sono indizi che:

a. il funzionamento dell'infrastruttura critica interessata o di un'altra infrastruttura critica è compromesso;

b. è stato eseguito o predisposto da uno Stato estero;

c. ha causato o potrebbe causare una fuga di informazioni o la loro manipolazione; o

d. non è stato individuato per più di 30 giorni.

[2] Un ciberattacco a un'infrastruttura critica deve sempre essere notificato se è connesso al reato di estorsione, minaccia o coazione nei confronti del gestore di un'infrastruttura critica o dei suoi collaboratori.

Art. 74e Contenuto della notifica

[1] La notifica deve contenere informazioni sull'infrastruttura critica, sul tipo di ciberattacco, sulla sua esecuzione, sulle sue ripercussioni e sull'ulteriore modo di procedere pianificato dal gestore di tale infrastruttura.

[2] Se al momento della notifica non sono ancora note tutte le informazioni necessarie, il gestore dell'infrastruttura critica completa la notifica non appena è a conoscenza di nuove informazioni.

Art. 74f Trasmissione della notifica

[1] Per la notifica elettronica di ciberattacchi, il NCSC mette a disposizione un sistema sicuro con cui trasmettergli le notifiche.

[2] Il sistema deve permettere al gestore di un'infrastruttura critica di trasmettere ad altri servizi e altre autorità la notifica del ciberattacco o delle sue ripercussioni sia nella sua totalità sia in parte.

[3] Se il servizio o l'autorità in questione necessita di informazioni supplementari rispetto a quelle menzionate all'articolo 74*e*, il gestore può trasmetterle direttamente a tale servizio o autorità attraverso il sistema.

Art. 74g Obbligo d'informazione

Il gestore dell'infrastruttura critica deve fornire al NCSC informazioni complementari sul contenuto della notifica di cui all'articolo 74*e* che gli occorrono per l'adempimento dei propri compiti volti a respingere ulteriori ciberattacchi alle infrastrutture critiche.

Art. 74h Violazione dell'obbligo di notifica o d'informazione

[1] Se vi sono indizi di una violazione dell'obbligo di notifica o d'informazione, il NCSC ne informa il gestore dell'infrastruttura critica.

[2] Se, nonostante questa informazione, il gestore non adempie il suo obbligo, il NCSC emana una decisione sugli obblighi da adempiere, fissando un termine con la comminatoria della multa di cui all'articolo 74*i*.

Art. 74i Infrazioni contro le decisioni del NCSC

[1] Chiunque, intenzionalmente, non ottempera a una decisione del NCSC passata in giudicato intimatagli con la comminatoria della pena prevista dal presente articolo o a una decisione dell'autorità di ricorso è punito con la multa sino a 100 000 franchi.

[2] Alle infrazioni commesse nell'azienda è applicabile l'articolo 6 della legge federale del 22 marzo 1974[16] sul diritto penale amministrativo (DPA).

[3] Se la multa applicabile non supera i 20 000 franchi e se la determinazione delle persone punibili secondo l'articolo 6 DPA esige provvedimenti d'inchiesta sproporzionati all'entità della pena, l'autorità può prescindere da un procedimento contro dette persone e, in loro vece, condannare l'azienda al pagamento della multa.

[4] In caso di infrazione contro una decisione del NCSC, il perseguimento e il giudizio sono demandati ai Cantoni.

16 RS **313.0**

Titolo prima dell'art. 75

Sezione 3: Protezione dei dati e scambio di informazioni

Art. 75 Trattamento di dati personali

[1] Per l'adempimento dei propri compiti, il NCSC può trattare dati personali, ivi compresi elementi di indirizzo di cui all'articolo 3 lettera f LTC[17] e i relativi dati personali degni di particolare protezione, che contengono informazioni su:

a. opinioni religiose, filosofiche o politiche; il trattamento è ammesso unicamente qualora sia necessario per la valutazione di minacce e pericoli concreti nell'ambito della cibersicurezza;

b. procedimenti e sanzioni di carattere amministrativo o penale.

[2] Può trattare i dati personali all'insaputa delle persone interessate, se altrimenti lo scopo del trattamento sarebbe compromesso o l'informazione della persona interessata comporterebbe un onere sproporzionato.

[3] In caso di indizi concreti di usurpazione d'identità o di utilizzazione non autorizzata di elementi di indirizzo, il NCSC informa le persone la cui identità è usurpata o i cui elementi di indirizzo sono utilizzati senza autorizzazione; sono fatti salvi gli articoli 18*a* capoverso 4 lettera b e 18*b* LPD[18].

Art. 76 Cooperazione a livello nazionale

[1] Il NCSC può comunicare dati personali ai gestori di infrastrutture critiche, sempre che ciò sia necessario per proteggere le infrastrutture critiche da ciber-rischi.

[2] I gestori di infrastrutture critiche possono comunicare dati personali al NCSC, sempre che ciò sia necessario per proteggere le infrastrutture critiche da ciber-rischi.

[3] Il NCSC può comunicare ai fornitori di servizi di telecomunicazione elementi di indirizzo e i relativi dati personali, sempre che ciò sia necessario per proteggere le infrastrutture critiche da ciber-rischi.

[4] I fornitori di servizi di telecomunicazione possono comunicare al NCSC elementi di indirizzo e i relativi dati personali, sempre che ciò sia necessario per proteggere le infrastrutture critiche da ciber-rischi.

Art. 76a Sostegno alle autorità

[1] Il NCSC sostiene il SIC nell'individuare tempestivamente e nello sventare minacce per la sicurezza interna o esterna, nel valutare la situazione di minaccia e nell'assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche conformemente all'articolo 6 capoversi 1 lettera a, 2 e 5 LAIn[19] con valutazioni sul

17 RS **784.10**
18 RS **235.1**
19 RS **121**

numero, sul tipo e sulla portata dei ciberattacchi nonché con analisi tecniche dei ciber-rischi.

2 Concede al SIC mediante procedura di richiamo l'accesso a informazioni che permettono di risalire all'identità e al modo di operare degli autori di ciberattacchi.

3 Il NCSC concede alle autorità di perseguimento penale mediante procedura di richiamo l'accesso a informazioni che permettono di risalire all'identità e al modo di operare degli autori di ciberattacchi.

4 Può concedere ai servizi cantonali competenti per la cibersicurezza mediante procedura di richiamo l'accesso alle informazioni necessarie per proteggere le autorità cantonali e le infrastrutture critiche cantonali da ciber-rischi.

Art. 77 Cooperazione a livello internazionale

1 Il NCSC può scambiare informazioni con servizi esteri e internazionali competenti per la cibersicurezza se questi ultimi necessitano di tali dati per l'adempimento di compiti corrispondenti a quelli del NCSC. Se lo scambio di informazioni concerne anche dati personali di cui all'articolo 75 si applica l'articolo 6 LPD[20].

2 Lo scambio di informazioni secondo il capoverso 1 è ammesso soltanto se i servizi esteri e internazionali garantiscono che i dati sono trattati esclusivamente per i fini previsti da tale disposizione.

3 Se le informazioni sono necessarie per un procedimento legale all'estero, si applicano le disposizioni in materia di assistenza amministrativa e di assistenza giudiziaria.

Art. 78
Abrogato

Art. 79 cpv. 1

1 Il NCSC conserva i dati personali soltanto fino a che sono utili per prevenire minacce o individuare incidenti, ma al massimo per cinque anni dall'ultimo utilizzo; per i dati personali degni di particolare protezione il termine è di due anni.

Art. 80
Abrogato

20 RS **235.1**

II

Gli atti normativi qui appresso sono modificati come segue:

1. Legge del 23 marzo 200721 sull'approvvigionamento elettrico

Art. 8a Protezione contro i ciber-rischi

[1] I gestori di rete, i produttori e i gestori di impianti di stoccaggio adottano misure per proteggere adeguatamente i loro impianti dai ciber-rischi.

[2] Il Consiglio federale può estendere tale obbligo ad altri partecipanti.

2. Legge federale del 25 settembre 2020[22] sulla protezione dei dati

Art. 24 cpv. 5[bis]

[5bis] L'IFPDT può inoltrare la notifica al Centro nazionale per la cibersicurezza con il consenso del titolare del trattamento soggetto all'obbligo di notifica, per un'analisi dell'incidente. La comunicazione può contenere dati personali, ivi compresi dati personali degni di particolare protezione concernenti sanzioni e procedimenti amministrativi o penali riguardanti il titolare del trattamento soggetto all'obbligo di notifica.

III

[1] La presente legge sottostà a referendum facoltativo.

[2] Il Consiglio federale ne determina l'entrata in vigore.

21 RS **734.7**
22 RS **235.1**; FF **2020** 6695

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Il capo del Dipartimento federale delle finanze DFF

Berna, 12 gennaio 2022

Destinatari:
i partiti politici
le associazioni mantello dei Comuni, delle città e delle regioni di montagna
le associazioni mantello dell'economia
gli ambienti interessati

Obbligo di notifica di ciberattacchi per i gestori di infrastrutture critiche: avvio della procedura di consultazione

Gentili Signore e Signori,

il 12 gennaio 2022 il Consiglio federale ha incaricato il Dipartimento federale delle finanze (DFF) di svolgere presso i Cantoni, i partiti politici, le associazioni mantello nazionali dei Comuni, delle Città e delle regioni di montagna, le associazioni mantello nazionali dell'economia e gli ambienti interessati una procedura di consultazione concernente l'introduzione di un obbligo di notifica di ciberattacchi e la relativa modifica della legge sulla sicurezza delle informazioni (LSIn).

La consultazione terminerà il **14 aprile 2022**.

I ciber-rischi sono diventati una delle principali minacce per la sicurezza e l'economia della Svizzera. È estremamente importante poter individuare tempestivamente gli attacchi alle imprese e alle autorità elvetiche nonché valutare il più precisamente possibile la situazione di minaccia. A tal fine, il progetto posto in consultazione mira a introdurre un obbligo di notifica per i gestori di infrastrutture critiche. Tale obbligo intende permettere al Centro nazionale per la cibersicurezza (NCSC) di avere una migliore visione d'insieme dei ciberattacchi in Svizzera, di sostenere gli interessati nella gestione di questi attacchi e di avvertire tutti gli altri gestori di infrastrutture critiche. Grazie all'introduzione di un obbligo di notifica, il nostro Paese colma una lacuna nel dispositivo in materia di cibersicurezza. Questo tipo di obbligo è già previsto in molti Paesi e dal 2018 si applica a tutti gli Stati membri dell'UE.
Il progetto si basa sugli obblighi di notifica esistenti (in particolare sull'obbligo di notifica appena introdotto nella legislazione in materia di protezione dei dati) ed è concepito in modo da ridurre al minimo l'onere supplementare per le imprese e le autorità interessate. In questo contesto, la creazione di un servizio centrale di notifica a livello federale (NCSC) è indispensabile perché soltanto un servizio centrale può garantire che l'obbligo di notifica adempia il suo scopo, ossia permettere di individuare precocemente gli attacchi e di ottenere una migliore visione d'insieme della situazione di minaccia. Il progetto crea inoltre la base per la collaborazione del NCSC con altri servizi, in particolare con le autorità di perseguimento penale.

Vi invitiamo ad esprimervi in merito alle considerazioni contenute nel rapporto esplicativo e, in particolare, all'attuazione della normativa proposta.

La procedura di consultazione si svolge in forma elettronica. I documenti relativi alla consultazione sono disponibili all'indirizzo Internet:

https://www.fedlex.admin.ch/it/consultation-procedures/ongoing

Ai sensi della legge del 13 dicembre 2002 sui disabili (LDis; RS *151.3*), ci adoperiamo per pubblicare documenti accessibili anche ai disabili. Vi invitiamo dunque a inviarci entro il termine indicato il vostro parere in forma elettronica **(in versione PDF e Word)** al seguente indirizzo:

ncsc@gs-efd.admin.ch

Vi preghiamo di indicare il nome e il numero di telefono delle persone a cui possiamo rivolgerci in caso di domande.

Per domande ed eventuali informazioni sono a vostra disposizione Manuel Suter della Segreteria del NCSC (tel. 058 461 43 20) e Angelika Spiess del Servizio giuridico della Segreteria generale del DFF (tel. 058 467 68 03).

Vi ringraziamo della preziosa collaborazione e cogliamo l'occasione per porgervi distinti saluti.

Ueli Maurer

Liste der Vernehmlassungsadressaten
Liste des destinataires consultés
Elenco dei destinatari della consultazione

Art. 4 Abs. 3 Vernehmlassungsgesetz (SR 172.061)

1. Kantone / Cantons / Cantoni

Staatskanzlei des Kantons Zürich	Neumühlequai 10 Postfach 8090 Zürich
Staatskanzlei des Kantons Bern	Postgasse 68 3000 Bern 8
Staatskanzlei des Kantons Luzern	Bahnhofstrasse 15 6002 Luzern
Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf
Staatskanzlei des Kantons Schwyz	Regierungsgebäude Bahnhofstrasse 9 Postfach 1260 6431 Schwyz
Staatskanzlei des Kantons Obwalden	Rathaus 6061 Sarnen
Staatskanzlei des Kantons Nidwalden	Dorfplatz 2 Postfach 1246 6371 Stans
Staatskanzlei des Kantons Glarus	Rathaus 8750 Glarus
Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug
Chancellerie d'Etat du Canton de Fribourg	Rue des Chanoines 17 1701 Fribourg
Staatskanzlei des Kantons Solothurn	Rathaus Barfüssergasse 24 4509 Solothurn
Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel
Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal

Staatskanzlei des Kantons Schaffhausen	Beckenstube 7 8200 Schaffhausen
Kantonskanzlei des Kantons Appenzell Ausserrhoden	Regierungsgebäude 9102 Herisau
Ratskanzlei des Kantons Appenzell Innerrhoden	Marktgasse 2 9050 Appenzell
Staatskanzlei des Kantons St. Gallen	Regierungsgebäude 9001 St. Gallen
Standeskanzlei des Kantons Graubünden	Reichsgasse 35 7001 Chur
Staatskanzlei des Kantons Aargau	Regierungsgebäude 5001 Aarau
Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld
Cancelleria dello Stato del Cantone Ticino	Piazza Governo 6 6501 Bellinzona
Chancellerie d'Etat du Canton de Vaud	Place du Château 4 1014 Lausanne
Chancellerie d'Etat du Canton du Valais	Planta 3 1950 Sion
Chancellerie d'Etat du Canton de Neuchâtel	Le Château Rue de la Collégiale 12 2000 Neuchâtel
Chancellerie d'Etat du Canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3
Chancellerie d'Etat du Canton du Jura	2, rue de l'Hôpital 2800 Delémont
Konferenz der Kantonsregierungen (KdK) Conférence des gouvernements cantonaux (CdC) Conferenza dei Governi cantonali (CdC)	Sekretariat Haus der Kantone Speichergasse 6 Postfach 3001 Bern

2. In der Bundesversammlung vertretene politische Parteien / partis politiques représentés à l'Assemblée fédérale / partiti rappresentati nell'Assemblea federale

Die Mitte Le Centre Alleanza del Centro	Generalsekretariat Hirschengraben 9 Postfach 3001 Bern
Eidgenössisch-Demokratische Union EDU Union Démocratique Fédérale UDF Unione Democratica Federale UDF	Postfach 3602 Thun
Ensemble à Gauche EAG	Case postale 2070 1211 Genève 2
Evangelische Volkspartei der Schweiz EVP Parti évangélique suisse PEV Partito evangelico svizzero PEV	Nägeligasse 9 Postfach 3001 Bern
FDP. Die Liberalen PLR. Les Libéraux-Radicaux PLR. I Liberali Radicali	Generalsekretariat Neuengasse 20 Postfach 3001 Bern
Grüne Partei der Schweiz GPS Parti écologiste suisse PES Partito ecologista svizzero PES	Waisenhausplatz 21 3011 Bern
Grünliberale Partei Schweiz glp Parti vert'libéral Suisse pvl Partito verde liberale svizzero pvl	Monbijoustrasse 30 3011 Bern
Lega dei Ticinesi (Lega)	Via Monte Boglia 3 Case postale 4562 6904 Lugano
Partei der Arbeit PDA Parti suisse du travail PST	Postfach 8721 8036 Zürich
Schweizerische Volkspartei SVP Union Démocratique du Centre UDC Unione Democratica di Centro UDC	Generalsekretariat Postfach 8252 3001 Bern
Sozialdemokratische Partei der Schweiz SPS Parti socialiste suisse PSS Partito socialista svizzero PSS	Zentralsekretariat Theaterplatz 4 Postfach 3001 Bern

3. Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete / associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national / associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna

Schweizerischer Gemeindeverband Association des Communes Suisses Associazione dei Comuni Svizzeri	Laupenstrasse 35 3008 Bern
Schweizerischer Städteverband Union des villes suisses Unione delle città svizzere	Monbijoustrasse 8 Postfach 3001 Bern
Schweizerische Arbeitsgemeinschaft für die Berggebiete Groupement suisse pour les régions de montagne Gruppo svizzero per le regioni di montagna	Seilerstrasse 4 Postfach 3001 Bern

4. Gesamtschweizerische Dachverbände der Wirtschaft / associations faîtières de l'économie qui œuvrent au niveau national / associazioni mantello nazionali dell'economia

economiesuisse Verband der Schweizer Unternehmen Fédération des entreprises suisses Federazione delle imprese svizzere Swiss business federation	Hegibachstrasse 47 Postfach 8032 Zürich
Schweizerischer Gewerbeverband (SGV) Union suisse des arts et métiers (USAM) Unione svizzera delle arti e mestieri (USAM)	Schwarztorstrasse 26 Postfach 3001 Bern
Schweizerischer Arbeitgeberverband Union patronale suisse Unione svizzera degli imprenditori	Hegibachstrasse 47 Postfach 8032 Zürich
Schweiz. Bauernverband (SBV) Union suisse des paysans (USP) Unione svizzera dei contadini (USC)	Laurstrasse 10 5201 Brugg
Schweizerische Bankiervereinigung (SBV) Association suisse des banquiers (ASB) Associazione svizzera dei banchieri (ASB) Swiss Bankers Association	Postfach 4182 4002 Basel
Schweiz. Gewerkschaftsbund (SGB) Union syndicale suisse (USS) Unione sindacale svizzera (USS)	Monbijoustrasse 61 Postfach 3000 Bern 23

Kaufmännischer Verband Schweiz Société suisse des employés de commerce Società svizzera degli impiegati di commercio	Hans-Huber-Strasse 4 Postfach 1853 8027 Zürich
Travail.Suisse	Hopfenweg 21 Postfach 5775 3001 Bern

5. Weitere interessierte Kreise / autres milieux concernés / altre cerchie interessate

Schweizerische Informatikkonferenz (SIK) Conférence suisse sur l'informatique (CSI) Conferenza svizzera sull'informatica (CSI)	Haus der Kantone Speichergasse 6 3011 Bern sekretariat@sik.swiss
Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)	Haus der Kantone Speichergasse 6 3011 Bern info@kkjpd.ch
Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (GDK)	Haus der Kantone Speichergasse 6 3011 Bern office@gdk-cds.ch
Regierungskonferenz Militär, Zivilschutz, Feuerwehr	Haus der Kantone Speichergasse 6 3011 Bern Alexander.Krethlow@rkmzf.ch
Schweizerische Staatsanwälte-Konferenz	Haus der Kantone Speichergasse 6 3011 Bern info@ssk-cps.ch
Bau-, Planungs- und Umweltdirektoren-Konferenz BPUK	Haus der Kantone Speichergasse 6 3011 Bern info@bpuk.ch
Verein eCH Association eCH	Mainaustrasse 30 Postfach 8034 Zürich info@ech.ch
Geschäftsstelle eJustice.CH Secrétariat eJustice.CH Segreteria eJustice.CH	Postfach 3134 3001 Bern info@eJustice.ch
digitalswitzerland	Waisenhausplatz 14 3011 Bern info@digitalswitzerland.ch

Schweizer Informatik Gesellschaft SI	Schwarztorstrasse 31 3007 Bern admin@s-i.ch
Geschäftsstelle Digitale Schweiz (GDS) Direction opérationnelle Suisse numérique (GDS) Direzione operativa Svizzera digitale (GDS)	Zukunftstrasse 44 2501 Biel / Bienne www.digitaldialog.swiss
privatim, Konferenz der schweizerischen Datenschutzbeauftragten privatim, Conférence des Préposé(e) suisses à la protection des données	c/o Dr. Beat Rudin, Advokat, Postfach 205 4010 Basel kommunikation@privatim.ch
eHealth Suisse	Schwarzenburgstrasse 157 3003 Bern info@e-health-suisse.ch
asut – Schweizerischer Verband der Telekommunikation	Hirschengraben 8 3011 Bern info@asut.ch
ASIP – Schweizerischer Pensionskassenverband	Kreuzstrasse 26 8008 Zürich info@asip.ch
Stiftung Auffangeinrichtung BVG	Elias-Canetti-Strasse 2 8050 Zürich
Verein Vorsorge Schweiz VVS	Aeschengraben 29 4051 Basel info@verein-vorsorge.ch
Inter-pension Interessengemeinschaft autonomer Sammel- und Gemeinschaftseinrichtungen	Gartenstrasse 2 3063 Ittigen info@inter-pension.ch
PK-Netz 2. Säule	Monbijoustrasse 61 3007 Bern info@pk-netz.ch
Konferenz der kantonalen BVG- und Stiftungsaufsichtsbehörden	Sekretariat Monica Schiesser Aeberhard m.schiesser@gmx.ch
IV-Stellen-Konferenz (IVSK)	Sempacherstrasse 15 6003 Luzern Schweiz
Konferenz der kantonalen Ausgleichskassen (KKAK)	Genfergasse 10 3011 Bern info@ahvch.ch
Vereinigung der Verbandsausgleichskassen (VVAK)	Kapellenstrasse 14 Postfach 3001 Bern info@vvak.ch

Seilbahnen Schweiz	Giacomettistrasse 1 3006 Bern info@seilbahnen.org
Verband Schweizerischer Schifffahrtsunternehmen VSSU	Mythenquai 333 8038 Zürich info@vvssu.ch
RAILplus AG	Hintere Bahnhofstrasse 85 5001 Aarau info@railplus.ch
swissnuclear	Postfach 1663 4601 Olten info@swissnuclear.ch
SwissGrid AG	Bleichemattstrasse 31 5001 Aarau info@swissgrid.ch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Berna, 2 dicembre 2022

Avamprogetto di modifica della legge federale del 18 dicembre 2020 sulla sicurezza delle informazioni in seno alla Confederazione

(Legge sulla sicurezza delle informazioni, LSIn)

Rapporto sui risultati della consultazione

Indice

1 Situazione iniziale

Il 12 gennaio 2022 il Consiglio federale ha adottato l'avamprogetto di modifica della legge federale del 18 dicembre 2020 sulla sicurezza delle informazioni (LSIn) e il rispettivo rapporto esplicativo, incaricando il Dipartimento federale delle finanze (DFF) di svolgere una procedura di consultazione, che ha avuto luogo dal 12 gennaio al 14 aprile 2022. In allegato è disponibile l'elenco dei partecipanti alla consultazione, con le abbreviazioni utilizzate nel presente rapporto.
Sono pervenuti complessivamente 102 pareri.

102	Totale dei pareri pervenuti
25	Governi cantonali
5	Conferenze cantonali
8	Partiti
1	Associazione mantello nazionale dei Comuni, delle città e delle regioni di montagna
4	Associazioni mantello nazionali dell'economia
21	Imprese interessate
37	Altri ambienti interessati

I pareri sono consultabili sulla piattaforma di pubblicazione del diritto federale Fedlex[1].

2 Oggetto dell'avamprogetto posto in consultazione

L'avamprogetto mira a introdurre nella legge sulla sicurezza delle informazioni (LSIn), adottata dal Parlamento il 18 dicembre 2020, la base legale necessaria per l'obbligo di notifica dei ciberattacchi contro le infrastrutture critiche.

L'obbligo di notifica riguarderebbe soltanto i ciberattacchi che potenzialmente possono arrecare notevoli danni. I ciberincidenti provocati da un comportamento errato, ad esempio un'operazione sbagliata compiuta involontariamente da un collaboratore, non sarebbero invece sottoposti a obbligo di notifica. Si è rinunciato anche alla possibilità di estendere l'obbligo di notifica alle vulnerabilità riscontrate negli strumenti informatici. L'obbligo di notifica si applicherebbe ai gestori di infrastrutture critiche nei sottosettori critici. La funzione di servizio centrale di notifica verrebbe assunta dal Centro nazionale per la cibersicurezza (NCSC), che raccoglie anche le segnalazioni volontarie di ciberincidenti e vulnerabilità riscontrate negli strumenti informatici.

Le basi legali dell'obbligo di notifica di ciberattacchi, fatti salvi alcuni adeguamenti al capitolo 1, verrebbero introdotte nel capitolo 5 della LSIn. Il capitolo 5 è stato completamente rielaborato in modo da integrare anche i compiti dell'NCSC, che attualmente sono definiti solo nell'ordinanza sui ciber-rischi (Ociber),[2] oltre alla funzione di centrale di notifica dei ciberattacchi che sarebbe assunta dall'NCSC.

L'introduzione di tale obbligo di notifica permetterebbe di individuare precocemente i ciberattacchi, analizzare le modalità con cui vengono sferrati e avvisare tempestivamente gli altri gestori di infrastrutture critiche. L'obbligo di notifica permetterebbe dunque di aumentare notevolmente la cibersicurezza in Svizzera.

L'avamprogetto non verte né sull'introduzione di norme minime vincolanti in materia di cibersicurezza per i gestori di infrastrutture critiche né sulle esigenze in materia di sicurezza dei prodotti informatici.

1 www.fedlex.admin.ch > Procedure di consultazione > Procedure di consultazione concluse > 2022 > DFF
2 RS **120.73**

3 Risultati della procedura di consultazione

3.1 Valutazione complessiva del progetto

94 partecipanti alla consultazione, vale a dire più del 90 per cento, **approvano** nella sostanza gli **obiettivi e l'orientamento dell'avamprogetto**, pur esprimendo alcune riserve.

Pareri positivi (sui 102 totali)	**94**
Governi cantonali	25
Conferenze cantonali	4
Partiti	6
Associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna	1
Associazioni mantello nazionali dell'economia	3
Imprese interessate	18
Altri ambienti interessati	37

Sette partecipanti alla consultazione hanno espresso parere **contrario all'avamprogetto**.

Pareri negativi (sui 102 totali)	**7**
Governi cantonali	-
Conferenze cantonali	-
Partiti	1
Associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna	-
Associazioni mantello nazionali dell'economia	1
Imprese interessate	2
Altri ambienti interessati	3

Il Cantone di Obvaldo, la Conferenza dei procuratori della Svizzera e la Fondazione istituto collettore LPP hanno espressamente rinunciato ad assumere posizione. Il Ministero pubblico della Confederazione ha proposto alcune modifiche materiali, senza tuttavia valutare il progetto.

3.2 Sintesi delle risposte alla consultazione e principali critiche

Tutti i Cantoni (eccetto il Cantone di Obvaldo che ha rinunciato a prendere posizione), 4 conferenze cantonali (CDDGP, CCPCS, CGMPP, CDS), sei partiti (PS, UDC, PLR, Alleanza del Centro, I Verdi, PVL), l'Unione delle città svizzere, quattro associazioni mantello nazionali dell'economia (economiesuisse, Swiss Banking, USS, USAM), 35 organizzazioni interessate (AEROSUISSE, asut, Associazione delle banche estere in Svizzera, Centre Patronal, CH++, Digitale Gesellschaft, digitalswitzerland, eAVS/AI, eGov-Schweiz, economiesuisse, FER, GEM, IG eHealth, Inter-pension, ASIP, Operation Libero, Pour Demain, privatim, Santésuisse, Swiss Banking, ISSS, RAILplus, USS, ASA, Swico, swissICT, Swissmem, Trust Valley, UniBE, VUD, UTP, AES, UZH, UNIL, PNR 77) e 15 imprese (Abraxas, Axpo, gli aeroporti di Ginevra e Zurigo, Helvetia Assicurazioni, Migros, La Posta, Raiffeisen, Romande Energie, Sunrise, Suva, Swisscom, Swissgrid, SWITCH, TPG) e il Comune di Gachnang **approvano l'obiettivo e l'orientamento del progetto**.

Nella maggioranza delle prese di posizione a favore del presente progetto si chiede espressamente che l'obbligo di notifica **non generi costi elevati** per l'economia pubblica e privata (segnatamente le imprese che notificano un ciberincidente), che l'attuazione dell'obbligo di notifica non

sia burocratica e che gli **oneri amministrativi siano contenuti**. Tuttavia, tutti i partecipanti desiderano precisazioni ed esprimono riserve su alcune disposizioni.

Le richieste di **precisazioni** riguardano soprattutto le definizioni (art. 5), l'elenco dei settori soggetti all'obbligo di notifica (art. 74*b*) e i criteri di eccezione (art. 74*c*), la definizione dei ciberattacchi da notificare (art. 74*d*) e le modalità di trasmissione della notifica (art. 74*f*).

Le **riserve** concernono in particolare le sanzioni in caso di violazione dell'obbligo di notifica (art. 74*h* e 74*i*). 24 partecipanti alla consultazione **respingono qualsiasi possibilità di sanzione**, sostenendo che le multe non sono il mezzo adeguato a far rispettare l'obbligo di notifica. Secondo loro, l'attuazione dell'obbligo di notifica dovrebbe invece essere incoraggiata mediante incentivi, come servizi di supporto

Dalla consultazione è emersa anche la grande importanza attribuita alla protezione delle informazioni ottenute con le notifiche, in particolare i dati personali. Lo dimostra la preoccupazione espressa da più parti in merito alla **trasmissione dei dati personali** ai servizi informativi e alle autorità di perseguimento penale.

Inoltre, alcuni partecipanti alla consultazione desiderano che il progetto non resti limitato all'introduzione di un obbligo di notifica, bensì venga esteso. L'NCSC dovrebbe altresì attuare un **servizio centrale di notifica**, poter **imporre standard minimi** ai gestori di infrastrutture critiche ed esigere l'attuazione di misure come l'**installazione degli aggiornamenti di sicurezza**. In tale contesto è stato anche proposto di assoggettare i gestori di infrastrutture critiche agli articoli 6–10 LSIn.

I partecipanti approvano la possibilità di notificare le vulnerabilità anche all'NCSC, che dovrà informare in primo luogo i produttori dei prodotti interessati secondo i principi della «coordinated vulnerability disclosure», imponendo loro un **termine per eliminare la vulnerabilità**. È auspicato che i soggetti che notificano le vulnerabilità non possano essere perseguiti penalmente e che i produttori che non eliminano tali vulnerabilità entro il termine fissato dall'NCSC possano essere esclusi dalle commesse pubbliche.

L'avamprogetto, nella versione presentata, è **respinto** da UDC, USAM, scienceindustries, swissuniversities, Coop, SWISS e da una singola persona. Il MPC non ha preso espressamente posizione né a favore né contro l'avamprogetto.

3.3 Richieste e osservazioni concernenti l'avamprogetto

3.3.1 Osservazione preliminare

Di seguito sono illustrate le osservazioni, le proposte di modifica e le critiche concernenti le varie disposizioni. Sono citate unicamente le argomentazioni principali espresse nelle prese di posizione. I pareri particolarmente dettagliati sono trascritti soltanto se vengono formulate richieste di modifiche materiali concrete. Per maggiori dettagli si rimanda alle prese di posizione pubblicate su Internet.
Il presente rapporto non dà conto del tacito consenso o dell'assenza di commenti agli articoli. Pertanto, nonostante le numerose osservazioni riguardanti le disposizioni riferite nel presente rapporto, si osserva che la maggioranza dei partecipanti alla consultazione approva sostanzialmente ampie parti della legge. Nessun partecipante si è espresso sulla sistematica della legge.

3.3.2 Richieste e osservazioni concernenti le disposizioni

3.3.2.1 Titolo

Il Cantone **TG** propone di modificare il titolo della legge, sostenendo che quello attuale suggerisce che il campo di applicazione è limitato alla Confederazione, mentre non sarebbe più così dopo l'introduzione dell'obbligo di notifica.

3.3.2.2 Articolo 1 capoverso 1 (scopo)

> [1] La presente legge ha lo scopo di:
>
> a. garantire il trattamento sicuro delle informazioni di competenza della Confederazione nonché l'impiego sicuro dei mezzi informatici della Confederazione;
>
> b. aumentare la resilienza ai ciber-rischi della Svizzera.

Questo articolo ha suscitato quattro reazioni che vertono sostanzialmente su adeguamenti concettuali.

❖ **Osservazioni generali sull'articolo 1 capoverso 1**

Migros propone di completare l'articolo 1 disciplinando il campo d'azione territoriale.

Il Cantone **TG** ritiene che la separazione in lettera *a* e *b* non sia opportuna.

❖ **Approvazione dell'articolo 1 capoverso 1**

Swiss Banking approva che l'articolo 1 includa espressamente «la resilienza ai ciber-rischi della Svizzera». L'articolo 1 rafforza così i compiti dell'NCSC definiti all'articolo 73*a* e segg.

❖ **Richieste di modifica e suggerimenti concernenti l'articolo 1 capoverso 1**

- **Lettera *a***

ISSS e Härting Rechtsanwälte chiedono di completare l'articolo 1 per precisare che la lettera *a* si applica a condizione che una legge speciale non preveda una competenza diversa.

- **Lettera *b***

Swico ritiene che il termine «ciber-rischi» non possa essere definito e pertanto chiede di sostituirlo con «minaccia».

3.3.2.3 Articolo 2 capoverso 5 (campo di applicazione)

> [5] Alle organizzazioni di diritto pubblico o privato che gestiscono infrastrutture critiche ma che non sono contemplate ai capoversi 1–3 si applicano gli articoli 73*a*–79. La legislazione speciale può dichiarare applicabili altre disposizioni della presente legge.

Riguardo al campo di applicazione proposto sono state formulate cinque osservazioni di carattere generale.

❖ **Osservazioni generali sull'articolo 2 capoverso 5**

Swissmem, UZH, UNIL e PNR 77 sottolineano la necessità di tenere conto dell'articolo 6 LSIn in aggiunta agli articoli 73*a*–79.

UZH, UNIL e PNR 77 ritengono opportuno prevedere la possibilità di rivolgersi all'NCSC per appurare se un gestore è soggetto o meno alla legge o all'obbligo di notifica, analogamente a quanto previsto per esempio dalla OSCPT (si veda in particolare l'art. 51 OSCPT).

Il Cantone **GE** chiede una definizione del termine «critiche».

- **Richieste di modifica e suggerimenti concernenti l'articolo 2 capoverso 5**

ISSS e Härting Rechtsanwälte chiedono che l'articolo 2 capoverso 5 si applichi anche alle infrastrutture critiche *di cui all'articolo 74b*, per precisare che le infrastrutture tipiche cui si fa riferimento sono quelle definite nella LSIn.

3.3.2.4 Articolo 5 lettera *d* ed *e* (definizioni)

Ai sensi della presente legge s'intende per:

d. *ciberincidente*: un evento che si verifica nell'esercizio di mezzi informatici e che può compromettere la confidenzialità, l'integrità o l'accessibilità delle informazioni o la tracciabilità del loro trattamento;

e. *ciberattacco:* un ciberincidente provocato intenzionalmente da persone non autorizzate.

Sulle due definizioni si sono espressi 23 partecipanti alla consultazione, tutti hanno proposto delle modifiche.

- **Osservazioni generali sull'articolo 5**

Economiesuisse, IG eHealth, La Posta e VUD ritengono necessario definire con maggiore precisione i termini «ciberincidente» e «ciberattacco» nell'articolo 5.

Il **Centro di competenza in diritto digitale dell'Università di Ginevra** chiede che le definizioni di «ciberattacco» e «ciberincidente» vengano precisate in modo da poter classificare questi eventi come tali anche in assenza di qualsiasi violazione della sicurezza dei dati o di altre disposizioni legali o normative.

- **Richieste di modifica e suggerimenti concernenti l'articolo 5**

IG eHealth, ISSS, Härting Rechtsanwälte, il Cantone GE e La Posta auspicano l'aggiunta di una definizione delle nozioni di «vulnerabilità» e «ciber-rischio» nell'articolo 5.
Il **Comune di Gachnang** ritiene necessario definire il prefisso «ciber».

- **Lettera *d***

Pour Demain suggerisce di menzionare esplicitamente l'intelligenza artificiale nell'ambito della definizione di «ciberincidente».

Migros, Sunrise, TPG e digitalswitzerland chiedono di modificare la formulazione «e che può compromettere». **Migros** chiede una migliore definizione mentre gli altri tre propongono di sostituirla con «e che compromette».

Santésuisse è del parere che la definizione non sia sufficientemente precisa, poiché eventi simili possono verificarsi anche indipendentemente da un ciberattacco, per esempio a seguito di un guasto funzionale dei componenti informatici o di errori di programmazione. Pertanto, l'obbligo di notifica non dovrebbe applicarsi a tali eventi.

UZH, UNIL e PNR 77 ritengono necessario armonizzare la definizione di «ciberincidente» con quella prevista all'articolo 3 lettera *b* Ociber. Inoltre sono del parere che la formulazione «nell'esercizio di mezzi informatici» non sia ottimale poiché potrebbe essere considerata troppo restrittiva, escludendo qualsiasi comportamento passivo.

- **Lettera *e***

Swissgrid chiede se nella definizione di «persone non autorizzate» vi rientrino esclusivamente le persone esterne o anche quelle interne.

3.3.2.5 Articolo 73*a* Principio

Ai fini della protezione della Svizzera contro i ciber-rischi, il Centro nazionale per la cibersicurezza (NCSC) svolge in particolare i seguenti compiti:

a. sensibilizzare il pubblico sui ciber-rischi;
b. avvertire riguardo ai ciber-rischi e alle vulnerabilità nei mezzi informatici;
c. pubblicare informazioni sulla cibersicurezza e istruzioni per l'adozione di misure preventive e reattive contro i ciber-rischi;
d. elaborare analisi tecniche per valutare i ciber-rischi e difendersi da essi;
e. ricevere e trattare le notifiche di ciberincidenti e vulnerabilità nei mezzi informatici;
f. sostenere i gestori di infrastrutture critiche.

Sui principi proposti si sono espressi 16 partecipanti alla consultazione, alcuni anche molto dettagliatamente: 2 sono soddisfatti dell'articolo 73*a* nella sua stesura attuale, 5 chiedono di aggiungere un compito alla lista e altri 9 hanno espresso commenti e chiesto altre modifiche.

- **Osservazioni generali sull'articolo 73*a***

CH++ è favorevole all'articolo, ma auspica che l'NCSC si occupi anche dell'individuazione attiva delle vulnerabilità e delle minacce.

Pur approvando l'articolo 73*a*, il **Comune di Gachnang** ritiene che tra i compiti ivi elencati debba essere incluso un reporting regolare per assicurare la qualità e il monitoraggio dei risultati.

Migros chiede un elenco non esaustivo di esempi a sostegno dell'intento dell'articolo 73*a*.

Il Cantone **BE** chiede l'aggiunta di un secondo capoverso all'articolo 73*a*, in cui sia specificato che l'NCSC svolge i propri compiti in collaborazione con le autorità di polizia cantonali.

Swisscom è favorevole all'articolo, ma auspica che la legge precisi, oltre alle competenze e ai compiti citati, che l'NCSC supporta non soltanto la Confederazione ma anche l'economia e la società.

- **Approvazione dell'articolo 73*a***

Swico e swissICT approvano espressamente la creazione di basi legali per i compiti dell'NCSC.

- **Richieste di modifica e suggerimenti concernenti l'articolo 73*a***

- **Lettera *b***

Pour Demain desidera che i compiti dell'NCSC includano i rischi legati all'intelligenza artificiale.

- **Lettera *c***

Swiss Banking e Raiffeisen sono favorevoli all'articolo, ma pensano che le «istruzioni per l'adozione di misure preventive e reattive contro i ciber-rischi» siano opportune solo se non obbligatorie.

- **Lettera *f***

I Verdi chiedono di configurare il «sostegno ai gestori di infrastrutture critiche» (art. 73*a* lett. *f*) in modo più ampio di quanto previsto dalle spiegazioni e dalle definizioni attuali.

3.3.2.6 Articolo 73*b* Trattamento delle notifiche di ciberincidenti e vulnerabilità

[1] Se gli sono notificati ciberincidenti o vulnerabilità nei mezzi informatici, il NCSC analizza la loro rilevanza ai fini della protezione della Svizzera contro i ciber-rischi. Su richiesta della persona che presenta la notifica, il NCSC fornisce raccomandazioni su come procedere, sempre che a tal fine non siano necessari ulteriori analisi e chiarimenti.

[2] Il NCSC può pubblicare o inoltrare alle autorità e alle organizzazioni interessate informazioni sui ciberincidenti, sempre che ciò serva a prevenire o a contrastare eventuali ciberattacchi. Tali informazioni possono contenere dati personali o dati di persone giuridiche, a condizione che si tratti di caratteristiche identificative ed elementi di indirizzo utilizzati abusivamente e la persona interessata vi acconsenta.

[3] Se gli viene segnalata una vulnerabilità, il NCSC informa immediatamente il produttore e gli impartisce un congruo termine per eliminarla. Se il produttore non la elimina entro il termine impartito, il NCSC pubblica la vulnerabilità indicando i software o gli hardware interessati, sempre che ciò contribuisca alla protezione contro i ciber-rischi.

Si sono espressi 21 partecipanti alla consultazione. In generale, il capoverso 3 è quello che ha suscitato le reazioni più intense.

❖ **Osservazioni generali sull'articolo 73*b***

Scienceindustries è del parere che l'attuazione dell'obbligo di notifica dovrebbe rappresentare un valore aggiunto per le imprese interessate, seguire un approccio proporzionato e sussidiario così come funzionare su base cooperativa, senza generare costi aggiuntivi per l'economia svizzera.

I Verdi, Digitale Gesellschaft e il Partito Pirata sono favorevoli all'articolo 73*b* e ritengono che, per poter svolgere i compiti in esso indicati, l'NCSC debba soddisfare determinate esigenze minime, vale a dire disporre di competenze più ampie in caso di incidenti gravi e attuare una procedura di «responsible disclosure» per le infrastrutture critiche.

I Verdi e CH++ auspicano che l'NCSC possa emanare direttive con termini vincolanti che obblighino le organizzazioni dei produttori e dei gestori a eliminare celermente le vulnerabilità e a ridurre i danni.

Il Cantone **VD** chiede che l'articolo 73*b* sia coordinato con l'ordinanza relativa ai dispositivi medici (ODmed).

❖ **Richieste di modifica e suggerimenti**

- **<u>Capoverso 1</u>**

Secondo **UZH, UNIL e PNR 77**, la formulazione «sempre che a tal fine non siano necessari ulteriori analisi e chiarimenti» non è chiara. Raccomandano di sostituirla con «qualora ciberincidenti o vulnerabilità siano resi noti all'NCSC» onde evitare di limitarsi a una notifica che potrebbe essere confusa con la notifica di ciberattacchi da parte della persona interessata.

- **<u>Capoverso 2</u>**

Secondo **I Verdi e CH++**, salvo eccezioni giustificate l'NCSC dovrebbe attuare un obbligo del principio di pubblicazione al fine di rispettare il principio della trasparenza. Al contrario, **ISSS, Härting Rechtsanwälte, AES, UTP, Swissgrid, il Cantone GE e RAILplus** sottolineano che i dati personali e quelli delle persone giuridiche dovrebbero essere pubblicati solo previo esplicito consenso. Ritengono inoltre opportuno regolamentare con maggiore precisione le circostanze in cui occorre pubblicare un ciberincidente e quali informazioni vadano menzionate, sulla base dei principi di protezione dei dati e di segretezza delle informazioni riservate.

UZH, UNIL e PNR 77 ritengono che il consenso vada richiesto alla persona che condivide i dati e non alle persone interessate, in quanto ottenere il consenso di tutte le persone interessate potrebbe richiedere sforzi sproporzionati.

- **Capoverso 3**

Il **Partito Pirata** apprezza che l'articolo 73*b* capoverso 3 preveda l'immediata condivisione delle falle di sicurezza con i gestori di infrastrutture critiche e chiede di aggiungere che essi non possono abusarne per cibergiochi offensivi secondo la LAIn. Allo stesso modo, agli hacker deve essere automaticamente concessa l'impunità nell'ambito della «responsible disclosure».

CH++ propone che i produttori che non reagiscono alle notifiche delle vulnerabilità possano essere esclusi dalle commesse pubbliche.

UZH, UNIL e PNR 77 ritengono opportuno completare il capoverso 3 con la possibilità di sanzioni in aggiunta alla pubblicazione, mentre al contrario **La Posta** è del parere che le sanzioni avrebbero un effetto nefasto sul numero di notifiche.
Il Cantone **GE** chiede di sostituire «il produttore» con «il produttore e/o l'editore».

Secondo **Digitale Gesellschaft**, se l'NCSC è a conoscenza di una falla di sicurezza riguardante un prodotto, ma non si può presumere che sia già nota al produttore, l'NCSC deve immediatamente notificarla al produttore interessato nell'ambito di una procedura di «responsible disclosure». Sempre secondo **Digitale Gesellschaft**, l'NCSC dovrebbe disporre di mezzi che gli consentano di insistere presso le organizzazioni che segnalano una falla di sicurezza affinché venga corretta.

Secondo **ISSS e Härting Rechtsanwälte**, le notifiche delle vulnerabilità da parte dell'NCSC ai produttori dovrebbero essere escluse dal principio di trasparenza.

Pour Demain e Operation Libero ritengono inoltre necessario fissare dei termini per i gestori al fine di garantire l'effettiva implementazione degli aggiornamenti di sicurezza.

Secondo **UCS e VUD**, la pubblicazione prematura della vulnerabilità, corredata dall'indicazione del software o dell'hardware interessato, potrebbe esporre a rischi ulteriori l'autore della notifica. Di conseguenza **VUD** propone di consentire all'NCSC di diffondere informazioni e adottare misure di comunicazione solo a condizione di non incoraggiare o facilitare i ciberattacchi.

3.3.2.7 Articolo 73*c* Inoltro di informazioni

[1] Se dalla notifica di un ciberincidente o dalla sua analisi emergono informazioni rilevanti per individuare tempestivamente e sventare minacce per la sicurezza interna o esterna, valutare la situazione di minaccia o assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche conformemente all'articolo 6 capoversi 1 lettera a, 2 e 5 della legge federale del 25 settembre 2015 sulle attività informative (LAIn), il NCSC inoltra queste informazioni al SIC.
[2] L'obbligo di denuncia di cui all'articolo 22*a* della legge sul personale federale non si applica ai collaboratori del NCSC che constatano indizi di un possibile reato nell'ambito della notifica di un ciberincidente o delle relative analisi. Il responsabile del NCSC può sporgere denuncia, sempre che ciò appaia opportuno in considerazione della gravità del possibile reato.
[3] Le informazioni rese note da una persona nel quadro di una notifica al NCSC possono essere usate in un procedimento penale contro detta persona soltanto con il suo consenso.
[4] Il NCSC può inoltrare informazioni che rivelano segreti protetti dalla legislazione penale esclusivamente secondo quanto disposto dall'articolo 320 del Codice penale.

Sono 25 i partecipanti alla consultazione che si sono espressi su questo articolo, che è stato molto discusso e ha suscitato numerose proposte di modifica. Due partecipanti approvano l'articolo 73*c* capoverso 3, mentre altri tre respingono l'articolo 73*c* capoverso 2.

- **Osservazioni generali sull'articolo 73*c***

Privatim chiede che i dati inoltrati al Servizio delle attività informative della Confederazione (SIC) o alle autorità di perseguimento penale siano eliminati dai server dell'NCSC dopo l'inoltro.
Il Cantone **GR** chiede di rendere più esplicito il collegamento tra la nozione di obbligo di tutela del segreto dei gestori e quella di inoltro delle informazioni nell'ambito dell'obbligo di notifica.

Swico approva l'articolo, ma chiede di precisare che vengono comunicate solo le informazioni relative alla sicurezza.

❖ Approvazione dell'articlo 73*c*

AEROSUISSE è favorevole a questa disposizione.

Il cantone **AG** approva che il personale dell'NCSC non sia soggetto all'obbligo di denuncia e che il NCSC possa denunciare le violazioni.

I Verdi e CH++ approvano l'articolo 73*c* capoverso 3.

❖ Bocciatura dell'articolo 73*c*

Il **Partito Pirata ed eGov-Schweiz** non approvano che il SIC possa trattare i dati inoltrati all'NCSC nell'ambito dell'obbligo di notifica.

Il Cantone **BE e la CCPCS** chiedono la soppressione dell'articolo 73*c* capoverso 2, ritenendo che l'NCSC debba continuare a inoltrare tutte le infrazioni ufficiali alle autorità di perseguimento penale.

Il Cantone **NW** chiede che l'articolo 73*c* capoverso 2 sia soppresso in quanto potenzialmente arbitrario.

❖ Richieste di modifica e suggerimenti concernenti l'articolo 73*c*

- **<u>Capoverso 1</u>**

Il **PVL** chiede che l'articolo 73*c* capoverso 1 preveda espressamente la possibilità di una notifica anonima all'NCSC.

I Verdi e VUD auspicano che i dati possano essere inoltrati all'NCSC in modo anonimo e che tale possibilità sia disciplinata giuridicamente.

- **<u>Capoverso 2</u>**

Secondo il Cantone **SZ**, l'NCSC deve garantire che le infrazioni gravi vengano sistematicamente portate in tribunale.

In generale, i Cantoni **BL, NW e SZ** sollevano preoccupazioni riguardo al potenziale arbitrario di una simile disposizione.

- **<u>Capoverso 3</u>**

Secondo il parere di **Digitalswitzerland, Sunrise, VUD, swissICT e asut**, la persona che effettua la notifica rischia di autoincriminarsi e per questo chiedono di modificare il testo.
Digitalswitzerland chiede che l'articolo 73*c* capoverso 3 precisi che le informazioni comunicate all'NCSC da una persona nell'ambito di una notifica, e *che potrebbero incriminare tale persona*, possano essere usate in un procedimento penale contro detta persona solo con il suo consenso.

VUD propone che l'obbligo del consenso sia esteso a tutto il personale e a tutti gli organi di un'impresa o di un'organizzazione che notifica un ciberincidente.

3.3.2.8 Articolo 74 Sostegno ai gestori di infrastrutture critiche

[1] Il NCSC sostiene i gestori di infrastrutture critiche nella protezione contro i ciber-rischi.
[2] A tal fine mette a loro disposizione in particolare i seguenti strumenti:
a. un sistema di comunicazione per lo scambio sicuro delle informazioni;
b. informazioni tecniche sui ciber-rischi e sulle vulnerabilità attuali nonché raccomandazioni per l'adozione di misure preventive;
c. strumenti tecnici e istruzioni per l'individuazione di ciberincidenti che si basano sul bisogno di protezione elevato delle infrastrutture critiche.
[3] Il NCSC consiglia e sostiene i gestori di infrastrutture critiche nella gestione di ciberincidenti e nell'eliminazione di vulnerabilità se per l'infrastruttura critica sussiste il rischio imminente di conseguenze gravi e, nel caso si tratti di gestori privati, non vi è la possibilità di procurarsi per tempo un sostegno equivalente sul mercato.
[4] Con il consenso dei gestori interessati, può accedere alle loro informazioni e ai loro mezzi informatici al fine di analizzare un ciberincidente. Tale consenso può essere accordato indipendentemente da eventuali obblighi di tutela del segreto.

Su queta disposizione si sono espressi concretamente 22 partecipanti alla consultazione. La maggior parte degli interventi vertono su richieste di modifica del testo e di chiarimenti. Un solo partecipante è contrario all'articolo 74.

❖ **Osservazioni generali sull'articolo 74**

I Verdi sono favorevoli al sostegno dell'NCSC ai gestori in materia di ciberrischi.

L'**UCS** chiede maggiori chiarimenti sul modus operandi delle città, in particolare in merito all'attuazione dei mezzi di individuazione e identificazione dei ciberattacchi e al loro finanziamento.

Secondo **Raiffeisen** l'utilizzo degli strumenti messi a disposizione dall'NCSC deve restare volontario ed è pertanto contraria all'obbligo di utilizzo di tali strumenti.

UniBE chiede che l'NCSC informi i gestori delle infrastrutture critiche in merito ai ciberattacchi notificati sferrati contro altri gestori di infrastrutture critiche.

❖ **Bocciatura dell'articolo 74**

Scienceindustries è scettica in merito all'obbligo di notifica e respinge in linea di principio le sanzioni previste dal progetto.

❖ **Richieste di modifica e suggerimenti concernenti l'articolo 74**

- **Capoverso 2 lettera a**

ISSS, Härting Rechtsanwälte e La Posta chiedono che oltre a mettere a disposizione un sistema di comunicazione per lo scambio di informazioni, l'NCSC garantisca la conservazione protetta dei dati.

- **Capoverso 2 lettera b**

Il Cantone **SH** insiste sulla necessità di attuare una piattaforma comune di scambio delle informazioni.

- **Capoverso 2 lettera c**

La Posta auspica una riformulazione per garantire senza ambiguità che l'utilizzo di tali tecniche, benché raccomandato, sia in fin dei conti facoltativo e non obbligatorio.

- **Capoverso 3**

L'**AES** apprezza la volontà di non porsi in concorrenza con le offerte dell'economia privata, tuttavia suggerisce che l'NCSC, in quanto GovCERT, sia a capo dei CERT del settore privato e li sostenga nella gestione delle crisi in funzione della situazione e delle esigenze. Inoltre l'**AES** chiede che

vengano definiti criteri di distinzione più pertinenti in merito a chi ha diritto o meno al sostegno dell'NCSC e propone di sopprimere la seconda parte della frase («Il NCSC consiglia e sostiene i gestori di infrastrutture critiche nella gestione di ciberincidenti e nell'eliminazione di vulnerabilità se per l'infrastruttura critica sussiste il rischio imminente di conseguenze gravi»).

UZH, UNIL e PNR 77 ritengono che la disposizione dovrebbe estendere le conseguenze dannose ai collaboratori, ai beneficiari e alle prestazioni dell'infrastruttura critica così come alla società o a parte di essa.

La Posta e il Cantone **GE** chiedono precisazioni sui termini «rischio imminente» e anche La Posta chiede che sia precisato il termine «conseguenze gravi».

- **<u>Capoverso 4</u>**

Digitalswitzerland chiede spiegazioni più chiare sul modo in cui l'NCSC protegge gli obblighi di tutela del segreto.

ISSS e Härting Rechtsanwälte chiedono una modifica del secondo periodo di questo capoverso, per precisare che l'accesso può essere concesso senza violare eventuali obblighi di tutela del segreto.

UZH, UNIL e PNR 77 ritengono necessario riformulare questa disposizione per prevedere che l'NCSC garantisca la riservatezza e che il gestore non violi alcun segreto trasmettendo le informazioni e fornendo l'accesso ai propri strumenti informatici per analizzare un incidente.

3.3.2.9 Articolo 74*a* Obbligo di notifica

I gestori di infrastrutture critiche che scoprono eventuali ciberattacchi devono notificarli il prima possibile al NCSC affinché quest'ultimo riconosca tempestivamente i modelli di attacco, avverta i potenziali interessati e possa raccomandare loro opportune misure di prevenzione e difesa.

Su questo articolo si sono espressi 27 partecipanti alla consultazione, 14 dei quali hanno sottolineato l'importanza della definizione di un termine di notifica.

❖ Richieste di modifica e suggerimenti concernenti l'articolo 74*a*

I Verdi, AEROSUISSE ed economiesuisse chiedono espressamente che l'obbligo di notifica non generi costi supplementari né per l'economia nazionale né per i soggetti notificanti. Inoltre desiderano che l'onere amministrativo del processo di notifica sia ridotto al minimo.

I Verdi, PVL, ISSS, Härting Rechtsanwälte e Pour Demain ritengono che l'obbligo di notifica dovrebbe essere applicato anche ai ciberattacchi e ai ciberincidenti generali così come alle vulnerabilità.

Sunrise e SWITCH sostengono che l'obbligo di notifica dovrebbe applicarsi soltanto alle imprese che hanno subito ciberattacchi alla propria infrastruttura (nessuna dichiarazione di terzi).

Digitale Gesellschaft propone l'estensione dell'obbligo di notifica a tutti i settori dell'economia svizzera, alle autorità statali e alle ONG, mentre il **Partito Pirata** auspica che l'obbligo sia esteso quanto meno alle organizzazioni che eseguono compiti per conto dello Stato, così come a tutte le imprese che sono tenute a svolgere un controllo ordinario o a dichiarare una collezione di dati ai sensi dell'articolo 11*a* LPD.

eAVS/AI ritiene necessario specificare che una notifica può comprendere anche tutte le organizzazioni interessate e che può essere fatta esplicitamente da terzi.

Il **Partito Pirata e I Verdi** sono del parere che il testo della legge dovrebbe trattare anche il tema dell'intelligenza artificiale.

Il **PS** chiede che le persone interessate dai ciberattacchi siano avvertite in tempo reale dall'NCSC.

L'**asut** sottolinea la difficoltà di obbligare un fornitore di accessi a Internet a notificare tutti i ciberattacchi subiti dai gestori di infrastrutture attraverso la propria rete. Inoltre la dichiarazione da parte del fornitore di accessi a Internet potrebbe non essere possibile a causa delle disposizioni della legge sulla protezione dei dati o degli accordi contrattuali.

L'**Associazione delle banche estere in Svizzera, CH++, Pour Demain, Swiss Banking, scienceindustries, i Cantoni FR, GR e UR, Raiffeisen, SWITCH e I Verdi** insistono sull'importanza di fissare dei termini espliciti per la comunicazione delle informazioni dettagliate all'NCSC. **Swiss Banking** ritiene che questo articolo debba essere completato da un capoverso 2 che definisca un termine di notifica, mentre **Raiffeisen e il Centro di competenza in diritto digitale dell'UNIGE** raccomandano di adottare i termini in due tempi della comunicazione prudenziale 05/2020 della FINMA.

Digitalswitzerland propone di introdurre la nozione di «persone assoggettate all'obbligo di notifica» («Meldepflichtigen») per ottenere una maggiore precisione ed evitare qualsiasi malinteso. Inoltre, **digitalswitzerland ed economiesuisse** ritengono necessario rafforzare la fiducia dell'economia sull'utilità dell'articolo 74*a*, spiegando che i vantaggi di tale disposizione sono immediati e superiori agli obblighi, dato che la proporzionalità delle misure è un criterio importante, soprattutto per le PMI e le start up.

L'**aeroporto di Zurigo e Raiffeisen** chiedono che l'obbligo di notifica si concentri sugli attacchi riusciti. In tale ambito, l'**aeroporto di Zurigo** propone di completare il testo come segue «im Sinne von Art. 74d» (ai sensi dell'art. 74*d*).

UZH, UNIL e PNR 77 chiedono di sostituire i termini «scoprono» con «individuano» e «celui-ci» con «ce dernier» (nel testo italiano «quest'ultimo» è già presente).

3.3.2.10 Articolo 74*b* Settori

L'obbligo di notifica si applica:

a. alle scuole universitarie secondo l'articolo 2 capoverso 2 della legge federale del 30 settembre 2011 sulla promozione e sul coordinamento del settore universitario svizzero;
b. alle autorità federali, cantonali o comunali nonché alle organizzazioni intercantonali, cantonali e intercomunali;
c. alle organizzazioni cui sono affidati compiti di diritto pubblico nei settori della sicurezza e del salvataggio, dell'approvvigionamento di acqua potabile, del trattamento delle acque di scarico e dello smaltimento dei rifiuti;
d. alle imprese attive nel settore dell'approvvigionamento energetico secondo l'articolo 6 capoverso 1 della legge federale del 30 settembre 2016 sull'energia nonché nel commercio, nella misurazione e nella gestione dell'energia;
e. alle imprese che sottostanno alla legge dell'8 novembre 1934 sulle banche, alla legge del 17 dicembre 2004 sulla sorveglianza degli assicuratori e alla legge del 22 giugno 2007 sulla vigilanza dei mercati finanziari;
f. ai fornitori di piattaforme per il commercio elettronico, di servizi di cloud computing, di motori di ricerca e di altri servizi digitali nonché ai centri di registrazione di nomi di dominio e ai gestori di centri di calcolo, che in Svizzera:
    1. sono utilizzati da un gran numero di utenti,
    2. rivestono un'importanza notevole per l'economia digitale, o
    3. offrono servizi di sicurezza e fiduciari;
g. agli ospedali che figurano nell'elenco compilato dal Cantone di cui all'articolo 39 capoverso 1 lettera e della legge federale del 18 marzo 1994 sull'assicurazione malattie;
h. ai laboratori medici che dispongono di un'autorizzazione secondo l'articolo 16 capoverso 1 della legge del 28 settembre 2012 sulle epidemie;

i. alle imprese che dispongono di un'autorizzazione secondo la legge del 15 dicembre 2000 sugli agenti terapeutici (LATer) per la fabbricazione, l'immissione in commercio e l'importazione di medicamenti o che fabbricano o smerciano dispositivi medici di cui all'articolo 4 capoverso 1 lettera b LATer;
j. alle organizzazioni che forniscono prestazioni delle assicurazioni sociali volte a coprire le conseguenze di malattie, infortuni, incapacità al lavoro e al guadagno, vecchiaia, invalidità e grande invalidità;
k. ai fornitori di servizi di telecomunicazione secondo l'articolo 3 lettera b LTC;
l. alla Società svizzera di radiotelevisione;
m. alle agenzie di stampa d'importanza nazionale;
n. ai fornitori di servizi postali registrati presso la Commissione delle poste secondo l'articolo 4 capoverso 1 della legge del 17 dicembre 2010 sulle poste;
o. alle imprese di trasporto che sottostanno alla legge federale del 18 giugno 2010 sugli organi di sicurezza delle imprese di trasporto pubblico;
p. alle imprese dell'aviazione civile che dispongono di un'autorizzazione dell'Ufficio federale dell'aviazione civile;
q. alle imprese che trasportano merci sul Reno secondo la legge federale del 23 settembre 1953 sulla navigazione marittima sotto bandiera svizzera nonché alle imprese che gestiscono l'iscrizione, il carico o lo scarico nei porti basilesi;
r. alle imprese che riforniscono la popolazione di beni indispensabili di uso quotidiano;
s. ai produttori di hardware e software i cui prodotti sono utilizzati da infrastrutture critiche, sempre che tali hardware o software abbiano accesso al sistema per la manutenzione remota o siano impiegati per uno dei seguenti scopi:
    1. tecnica di comando e monitoraggio di sistemi;
    2. esercizio di dispositivi medici e di impianti di telecomunicazione;
    3. garanzia della sicurezza pubblica;
    4. sicurezza informatica, crittografia, identificazione, attribuzione di diritti di accesso a sistemi o luoghi.

Questo articolo ha suscitato molte reazioni: 39 partecipanti alla consultazione si sono espressi sui settori interessati dall'obbligo di notifica.

❖ **Osservazioni generali sull'articolo 74*b***

Il **Partito Pirata** ritiene che ai settori indicati nell'articolo 74*b* vadano aggiunte le grandi imprese dei media.

Il **PS** chiede di riesaminare questo elenco ogni cinque anni per mantenerlo aggiornato.

Economiesuisse chiede di limitare l'obbligo di notifica ai soli settori in cui un guasto funzionale o un danneggiamento genererebbero carenze di approvvigionamento durature, disagi rilevanti per la sicurezza pubblica o altre conseguenze drammatiche.

Digitalswitzerland chiede un'analisi d'impatto e un approccio di regolazione scaglionato in funzione delle criticità riscontrate nelle imprese.

Scienceindustries, USAM, il Cantone UR e Swico auspicano che l'elenco sia più esplicito e che in particolare definisca chiaramente cosa si intende per «infrastruttura critica». In tal senso, **swissICT** propone una differenziazione qualitativa tra infrastrutture critiche e infrastrutture altamente critiche.

Il Cantone **ZG e swissuniversities** chiedono una revisione e una riduzione dell'elenco.

Coop e Migros propongono di limitare l'obbligo di notifica alle attività ritenute critiche dall'azienda.

Il Cantone **AG** chiede di comprendere nell'elenco anche il settore di oggetti, organizzazioni e imprese che i servizi competenti della Confederazione o del Cantone hanno classificato come infrastrutture critiche ai sensi della legislazione sulla protezione della popolazione.

Il Cantone di **GR** propone di agevolare l'attuazione dell'articolo 74*b* valutando la possibilità di stabilire delle priorità e di scaglionare le scadenze di conseguenza, per ridurre l'elenco durante una fase pilota.

Il Cantone **SZ** chiede che siano assoggettati all'obbligo di notifica anche i gestori delle cartelle informatizzate dei pazienti, ai sensi dell'articolo 10 della legge federale del 19 giugno 2015 sulla cartella informatizzata del paziente (RS *816.1*).

Il Cantone **UR** propone che, in aggiunta all'obbligo di notifica, per tutte le altre organizzazioni sia raccomandata anche la notifica dei ciberincidenti.

I Verdi suggeriscono di estendere l'ambito alla democrazia (partiti politici in Parlamento e politici in posizioni di rilievo), oltre ai servizi postali, alla navigazione sul Reno o alle agenzie di stampa.

- ❖ **Approvazione dell'articolo 74*b***

EGov-Schweiz, i Cantoni AI, GR e BE e privatim ritengono appropriata la disposizione proposta.

- ❖ **Bocciatura dell'articolo 74*b***

VUD respinge l'articolo 74*b* ritenendolo sproporzionato. L'associazione propone di limitare di primo acchito l'obbligo di notifica ai ciberattacchi che rappresentano una grave minaccia per le infrastrutture critiche ai sensi dell'articolo 5 lettera c LSIn e che quindi sono di interesse nazionale. Per **VUD**, per l'obbligo di notifica dovrebbe essere determinante la natura critica di un ciberattacco da un punto di vista nazionale.

- ❖ **Richieste di modifica e suggerimenti concernenti l'articolo 74*b***

- **Lettera *b* (autorità)**

L'**UCS** chiede di chiarire la responsabilità dell'obbligo di notifica che ricade sulle autorità comunali.

- **Lettera *c* (salvataggio, acqua potabile, acque di scarico, rifiuti)**

Secondo il Cantone **AI**, se le attività cantonali e comunali si servono dello stesso gestore informatico, dovrebbe essere sufficiente una sola notifica.

- **Lettera *f* (servizi digitali)**

Per una maggiore chiarezza, alla lettera *f* **Digitalswitzerland** propone di sopprimere «di piattaforme per il commercio elettronico».

SwissICT chiede che la lettera *f* definisca più chiaramente le cifre 1, 2 e 3.

Swissmem approva la disposizione, ma desidera una distinzione più chiara tra gestore o fornitore di servizi e fornitore di infrastrutture di dati (servizi in cloud).

Migros chiede che questa definizione sia formulata in modo più neutro dal punto di vista tecnologico.

SWITCH così come UZH, UNIL e PNR 77 chiedono che sia trattato l'aspetto extraterritoriale di questa disposizione, soprattutto in merito all'applicazione del diritto svizzero.

UZH, UNIL e PNR 77 auspicano maggiori precisazioni sui fornitori di servizi di telecomunicazione derivati, parimenti interessati.

Il Cantone **GE** chiede una definizione più precisa del concetto di «servizi di sicurezza e fiduciari».

Switch chiede che anche la gestione dei nomi di dominio .ch si integrata in questa disposizione.

Secondo **I Verdi e CH++**, il numero di utenti non è appropriato per determinare l'importanza dell'obiettivo.

I Verdi e CH++ chiedono che il termine «digitale» sia soppresso dalla lettera *f* cifra 2.

- **Lettera *g* (ospedali)**

Il Cantone **GE così come UZH, UNIL e PNR 77** chiedono che sia corretto l'errore tipografico nella versione francese: la lettera *g* deve rimandare all'articolo 39 e non all'articolo 9 LAMal.

Il Cantone **GL** chiede precisazioni sugli ospedali (dimensione delle infrastrutture) considerati infrastrutture critiche. Inoltre desidera che anche le piattaforme utilizzate per la cartella informatizzata del paziente siano assoggettate all'obbligo di notifica.

- **Lettera *i* (medicamenti)**

Scienceindustries chiede una definizione esatta e una designazione specifica delle imprese assoggettate a questa disposizione.

- **Lettera *j* (assicurazioni sociali)**

Per **Inter-pension** il concetto di assicurazione sociale non è chiaramente definito nella previdenza professionale (prestazioni sovraobbligatorie). **Inter-pension** chiede anche se le fondazioni di investimento rientrino in questa disposizione.

- **Lettera *k* (servizi di telecomunicazione)**

Per **UZH, UNIL e PNR 77** la lettera *k* comporta un aspetto extraterritoriale e di conseguenza sarebbe necessario prevedere l'applicazione del diritto svizzero (si veda ad es. la teoria degli effetti dell'art. 3 revisione LPD).

- **Lettera *p* (aviazione civile)**

AEROSUISSE e gli aeroporti di Ginevra e Zurigo sostengono che sia necessario modificare il testo in modo che la disposizione non verta esclusivamente sulle compagnie aeree che dispongono dell'autorizzazione dell'Ufficio federale dell'aviazione civile.

- **Lettera *r* (approvvigionamento di base)**

Migros chiede di introdurre criteri facilmente misurabili, come il numero di collaboratori o la cifra d'affari, in base ai quali prevedere direttamente nella legge determinate agevolazioni o eccezioni.

Il Cantone **GE e TPG** chiedono di usare nella versione francese di questa disposizione il termine «chiffrement» al posto di «cryptage».

- **Lettera *s* (produttori di hardware e software)**

I Verdi e CH++ ritengono appropriata la disposizione e propongono di menzionare le catene di approvvigionamento.

Per **eAVS/AI** occorrerebbe menzionare anche i fornitori di tecnologie informatiche degli organi esecutivi, la cui situazione non è definita chiaramente nel progetto.

Economiesuisse ritiene che il riferimento ai produttori accresca la mancanza di chiarezza in merito alle istanze interessate dall'obbligo di notifica.

L'**UCS** esprime preoccupazioni sull'applicabilità di questa disposizione, in particolare perché molti produttori di hardware e software non hanno sede in Svizzera**.**

Swico propone la soppressione delle cifre 1–4 della disposizione per sostituirle con la definizione di manutenzione remota, per trattare la problematica delle catene di approvvigionamento.

SwissICT chiede che alla lettera *s* venga precisato che i fornitori di software-as-a-service (SaaS) non gestiscono infrastrutture critiche.

Swissmem chiede la soppressione dell'articolo 74*b* lettera s.

3.3.2.11 Articolo 74*c* Eccezioni all'obbligo di notifica

Il Consiglio federale esenta determinate categorie di gestori di infrastrutture critiche dall'obbligo di notifica se i guasti funzionali o i malfunzionamenti causati alle loro infrastrutture da ciberattacchi:

a. sono improbabili, in particolare a seguito di un basso grado di accoppiamento dei mezzi informatici; o
b. possono avere soltanto ripercussioni minime sul funzionamento dell'economia o il benessere della popolazione, in particolare perché:
   1. riguardano unicamente un numero esiguo di persone,
   2. sono neutralizzati dall'intervento di altre infrastrutture critiche, o
   3. comporterebbero solo modesti danni potenziali per l'economia.

In totale, sulle eccezioni si sono espressi 20 partecipanti alla consultazione. Principalmente hanno sottoposto commenti generali e numerose proposte di adattamento della formulazione. Solo cinque partecipanti alla consultazione si sono pronunciati contro l'inserimento di questa disposizione nella legge.

❖ Osservazioni generali sull'articolo 74*c*

Swiss Banking propone di modificare questa disposizione in modo da prevedere che il Consiglio federale definisca, mediante ordinanza, criteri chiari in base ai quali assoggettare all'obbligo di notifica le infrastrutture critiche. L'obiettivo di tali criteri sarebbe di esentare i gestori dall'obbligo di notifica qualora i guasti funzionali o i malfunzionamenti provocati dai ciberattacchi soddisfino le condizioni elencate alle lettere *a* e *b*.

Swico è del parere che i criteri citati in questo articolo saranno difficilmente applicabili e propone di sostituirli con il criterio delle ripercussioni potenziali di un danno.
Inoltre, **Swico** propone di aggiungere un'ulteriore lettera alla disposizione, per prevedere l'esenzione anche nel caso in cui un attacco venga reso inoffensivo dalle misure di mitigazione.

VUD ritiene che le disposizioni dell'articolo 74*c* lettera *a* e *b* siano contraddittorie o poco chiare e chiede che vengano precisate, in particolare le espressioni «di un basso grado di accoppiamento dei mezzi informatici» e «possono avere soltanto ripercussioni minime sul funzionamento dell'economia o il benessere della popolazione».

Il Cantone **BE** chiede di aggiungere una disposizione 74*c*^{bis} per disciplinare la possibilità dei Cantoni, previa consultazione con l'NCSC e nel rispetto delle condizioni previste all'articolo 74*c*, di esentare dall'obbligo di notifica le autorità o gli organismi preposti ai compiti pubblici a livello cantonale o comunale. Il Cantone **BE** auspica che tale articolo 74*c*^{bis} preveda inoltre che i Cantoni possano designare i responsabili della notifica presso le autorità preposte ai compiti pubblici a livello cantonale o comunale.

Migros critica l'assenza di una regolamentazione basata sui rischi.

Il Cantone **LU e SWITCH** chiedono che le piccole organizzazioni siano esentate dall'obbligo di notifica perché, secondo il Cantone **LU**, il processo sarebbe troppo costoso.

❖ Approvazione dell'articolo 74*c*

EGov-Schweiz e i Cantoni AI e NW ritengono questo articolo appropriato.

❖ **Bocciatura dell'articolo 74*c***

I Verdi, CH++, Operation Libero e i Cantoni TG e UR chiedono l'eliminazione di questo articolo.

❖ **Richieste di modifica e suggerimenti concernenti l'articolo 74*c***

- **Lettera *a***

Secondo **I Verdi, Operation Libero e Pour Demain**, un basso grado di accoppiamento con i mezzi informatici appare sempre meno probabile nel XXI secolo. Pertanto chiedono l'eliminazione della lett. a.

Per il Cantone **GE**, tale disposizione è in contraddizione con la LPD.

- **Lettera *b***

Secondo **VUD** è determinante solo sapere se un ciberattacco compromette gravemente la sicurezza nazionale.

Il Cantone **GE** ritiene questa disposizione in contraddizione con l'obiettivo dell'articolo 74*b* che elenca le organizzazioni di maggiore importanza.

Migros considera inapplicabile la deroga prevista alla lettera *b*.

3.3.2.12 Articolo 74*d* Ciberattacchi da notificare

[1] Un ciberattacco a un'infrastruttura critica deve essere notificato se vi sono indizi che:
a. il funzionamento dell'infrastruttura critica interessata o di un'altra infrastruttura critica è compromesso;
b. è stato eseguito o predisposto da uno Stato estero;
c. ha causato o potrebbe causare una fuga di informazioni o la loro manipolazione; o
d. non è stato individuato per più di 30 giorni.

[2] Un ciberattacco a un'infrastruttura critica deve sempre essere notificato se è connesso al reato di estorsione, minaccia o coazione nei confronti del gestore di un'infrastruttura critica o dei suoi collaboratori.

La definizione dei ciberattacchi da notificare ha generato un gran numero di reazioni, principalmente osservazioni generali o proposte concrete di modifica.
Si sono pronunciati in totale 36 partecipanti; 1 si è espressamente dichiarato favorevole a questa proposta mentre 4 l'hanno esplicitamente respinta.

❖ **Osservazioni generali sull'articolo 74*d***

Per **AEROSUISSE**, ai fini della certezza del diritto delle imprese interessate, è importante stabilire chiaramente che l'articolo 74*d* è il criterio per determinare se un attacco contro un'infrastruttura critica deve essere segnalato.

Secondo **economiesuisse, eGov-Schweiz, il Cantone ZH e santésuisse**, l'articolo 74*d* deve necessariamente essere riveduto, in particolare perché i criteri sono troppo ampi e difficilmente comprensibili o applicabili per le imprese. Perciò, secondo **economiesuisse**, sarebbe più opportuno rendere disponibile un elenco (positivo) più limitato di incidenti da notificare e limitare l'obbligo di notifica ai tentativi riusciti o particolarmente gravi.

Il cantone **GR** chiede un elenco chiaro dei casi da notificare.

ISSS, Härting Rechtsanwälte così come UZH, UNIL e PNR 77 chiedono che nel titolo dell'articolo 74*d* siano menzionati anche i ciberincidenti.

Privatim auspica una definizione più precisa di ciò che si intende per «grave», poiché, secondo questa conferenza, è qui sottinteso che gli incidenti debbano essere notificati anche se la loro gravità non è ancora valutabile. Pertanto, se l'NCSC stabilisce che l'incidente non è grave e non c'è il consenso della persona o delle persone interessate, le informazioni personali devono essere immediatamente eliminate o trattate in forma anonima.

Scienceindustries chiede di specificare espressamente nell'articolo 74*d* che l'obbligo di notifica è limitato agli attacchi contro installazioni in Svizzera, escludendo gli attacchi contro gli impianti situati all'estero, mentre **UZH, UNIL e PNR 77** desiderano che la disposizione copra anche gli impianti all'estero.

Per **Coop**, la definizione proposta è troppo generica e non permette di differenziare in modo chiaro tra gli incidenti che influiscono minimamente o per niente sui processi commerciali e quelli che riguardano direttamente la gestione delle infrastrutture critiche o che presentano un rischio elevato. Non permette neppure di sapere quali ciberattacchi notificare, tra quelli riusciti e quelli falliti.

L'**aeroporto di Zurigo** chiede di assoggettare all'obbligo di notifica solo i ciberattacchi riusciti.

Secondo il Cantone **AG**, la cernita degli attacchi da notificare dovrebbe essere svolta dall'NCSC, perché possono rivelarsi importanti anche le notifiche degli attacchi considerati irrilevanti.

❖ Approvazione dell'articolo 74*d*

L'**AES** è favorevole alla disposizione.

❖ Bocciatura dell'articolo 74*d*

Swiss Banking e Raiffeisen propongono di sopprimere l'articolo 74*d* e di sostituirlo con una formulazione corrispondente a quella della FINMA: chiedono di rendere obbligatoria la notifica dei ciberattacchi che hanno conseguenze considerevoli per l'attività dell'azienda, in particolare gli attacchi interamente o parzialmente riusciti, così come per le funzioni di importanza cruciale, il cui guasto o malfunzionamento potrebbe compromettere la protezione delle persone o il buon funzionamento dei mercati.

SwissICT chiede l'eliminazione della presente disposizione, in quanto in pratica dovrà essere segnalato qualsiasi attacco.

VUD boccia la soluzione legislativa proposta, che definisce gli eventi da notificare nel modo più ampio possibile (art. 5 lett. *d* ed *e* LSIn) per poi limitare l'obbligo di notifica (art. 74*d* LSIn).

❖ Richieste di modifica e suggerimenti concernenti l'articolo 74*d*

- **<u>Capoverso 1</u>**

Secondo l'**ISSS,** il fatto che gli indizi di un ciberattacco siano già assoggettati all'obbligo di notifica ai sensi dell'articolo 74*d* è contrario alla ratio legis. L'ISSS propone quindi di modificare la frase introduttiva in modo che, da un lato, verta anche sui ciberincidenti e, dall'altro, che l'obbligo si applichi in caso di *seri timori* e non semplici indizi.

- **<u>Capoverso 1 lettera *a*</u>**

Swissmem chiede di modificare la condizione di cui alla lett. a specificando che il livello di compromissione deve essere *considerevole*.

Gli **aeroporti di Ginevra e Zurigo, Swissgrid, santésuisse e il Cantone GE** propongono di stralciare il passaggio «o di un'altra infrastruttura critica», perché spesso le imprese non sono in grado di valutare una simile minaccia.

- **<u>Capoverso 1 lettera b</u>**

Economiesuisse, Coop, IG eHealth, SWITCH, il Cantone TG, ISSS, aeroporto di Zurigo, Axpo, UZH, UNIL e PNR 77, scienceindustries, VUD, UTP e RAILplus esprimono dubbi sulla pertinenza di questa seconda condizione, in quanto spesso l'individuazione degli attacchi compiuti dagli Stati è troppo complessa e la loro attribuzione implica un processo politico complicato. Per questi motivi, **ISSS, aeroporto di Zurigo, Axpo, UZH, UNIL e PNR 77, scienceindustries, VUD, UTP e RAILplus** propongono di eliminare questa condizione. **RAILplus** suggerisce di sostituirla con un criterio cumulativo riferito all'impatto (per es. il numero di utenti o di sistemi colpiti).

- **Capoverso 1 lettera *c***

Swissgrid ritiene necessario sviluppare i punti seguenti: dati sensibili, informazioni sui sistemi critici, dati relativi alla gestione della rete elettrica, infrastrutture e sistemi di gestione principale.

- **Capoverso 1 lettera *d***

Economiesuisse, aeroporto di Zurigo, ASA, VUD e Coop ritengono inappropriato il termine di 30 giorni.

IG eHealth propone di esentare dall'obbligo di notifica i ciberattacchi passati inosservati per più di 30 giorni se non sono soddisfatte le condizioni di cui alle lettere *a* (compromissione del funzionamento) e *c* (possibile fuga o manipolazione di informazioni), ovvero in caso di attacco di lieve entità o di gravità medio-bassa.

L'**ASA** ritiene il termine irrealistico, poiché creerebbe un obbligo di reazione a un evento di cui non si è a conoscenza e di cui si potrebbe ignorare quando si è verificato. L'**ASA** propone di sostituire la lettera *d* con il testo seguente: «über einen längeren Zeitraum unentdeckt blieb» (non è stato individuato per un lungo periodo).

Il **Cantone TG** propone di sostituire la lettera *d* con il testo seguente: «*d. die direkt und unmittelbar für das Ziel des Cyberangriffs verwendeten Instrumente länger als 30 Tage unentdeckt blieben*» (d. gli strumenti usati direttamente per l'obiettivo del ciberattacco non sono stati individuati per più di 30 giorni).

Secondo **Migros, UZH, UNIL e PNR 77**, un termine di mancata individuazione non dovrebbe essere l'unico criterio per la notifica.

- **Capoverso 2**

Secondo **scienceindustries,** l'obbligo di notifica deve limitarsi all'estorsione, alle minacce o alla coazione, in quanto acquista efficacia solo in presenza di un legame con l'attività commerciale.

L'UVS ritiene che la formulazione esaustiva dell'elenco ponga la questione se l'obbligo di notifica non debba applicarsi anche quando un ciberattacco è legato a estorsione, minaccia o coazione nei confronti dei clienti o dei pazienti di un gestore.

Il Cantone **BL** suggerisce di completare il testo aggiungendo i reati di danneggiamento dei dati, commessi attraverso crittografia o introduzione di dati (malware).

Il Cantone **GE** fa presente che le istituzioni che violassero questo articolo si esporrebbero a un rischio di duplice sanzione.

UZH, UNIL e PNR 77 ritengono necessario modificare il testo in modo da prevedere un obbligo di notifica non appena vengono commesse «azioni penalmente rilevanti» e non solo nei «casi di reati contro la libertà».

3.3.2.13 Articolo 74*e* Contenuto della notifica

[1] La notifica deve contenere informazioni sull'infrastruttura critica, sul tipo di ciberattacco, sulla sua esecuzione, sulle sue ripercussioni e sull'ulteriore modo di procedere pianificato dal gestore di tale infrastruttura.

[2] Se al momento della notifica non sono ancora note tutte le informazioni necessarie, il gestore dell'infrastruttura critica completa la notifica non appena è a conoscenza di nuove informazioni.

In fase di consultazione si sono espressi su questa disposizione 15 partecipanti. La maggioranza chiede chiarimenti e una descrizione più dettagliata delle informazioni necessarie ai sensi dell'articolo 74*e*.

❖ **Osservazioni generali sull'articolo 74*e***

I Verdi giudicano necessario rivedere l'articolo 74*e* per rendere possibile l'automazione delle notifiche.

L'**Associazione delle banche estere in Svizzera** ritiene necessario poter redigere le notifiche in inglese e nelle lingue nazionali.

Economiesuisse chiede che le esigenze in materia di notifica siano semplici per limitare gli ostacoli per le imprese. Inoltre occorrerebbe definire chiaramente i limiti dei fatti da notificare.

SwissICT, La Posta e i Cantoni GR e TG chiedono che le informazioni necessarie ai sensi dell'articolo 74*e* siano descritte in modo più preciso, eventualmente con un elenco.

SwissICT e La Posta chiedono che le informazioni richieste dall'articolo 74*e* siano coordinate con altre autorità (ad es. la FINMA).

Secondo **Axpo,** la notifica deve essere immediata, indipendentemente dall'entità delle informazioni.

❖ **Approvazione dell'articolo 74*e***

Swiss Banking è favorevole a questa disposizione.

❖ **Richieste di modifica e suggerimenti concernenti l'articolo 74*e***

- **<u>Capoverso 1</u>**

ISSS e Härting Rechtsanwälte chiedono che la disposizione sia modificata come segue: «Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, des Cybervorfalles, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten» (La notifica deve contenere informazioni sull'infrastruttura critica, sul tipo di ciberattacco o ciberincidente, sulla sua esecuzione, sulle sue ripercussioni e sull'ulteriore modo di procedere pianificato dal gestore di tale infrastruttura).

Il Cantone **GE** propone di sostituire «e sull'ulteriore modo di procedere pianificato dal gestore di tale infrastruttura» con «o che l'entità interessata ha iniziato a attuare».

UZH, UNIL e PNR 77 propongono di modificare la formulazione per specificare che la notifica deve contenere informazioni in merito alle misure «assunte o previste».

- **<u>Capoverso 2</u>**

Il Cantone **GE** chiede di modificare il capoverso 2 in modo che il gestore sia tenuto a completare la notifica non solo dal momento in cui viene a conoscenza delle informazioni necessarie, ma anche dal momento in cui tali informazioni possono essere ottenute.

3.3.2.14 Articolo 74*f* Trasmissione della notifica

[1] Per la notifica elettronica di ciberattacchi, il NCSC mette a disposizione un sistema sicuro con cui trasmettergli le notifiche.

[2] Il sistema deve permettere al gestore di un'infrastruttura critica di trasmettere ad altri servizi e altre autorità la notifica del ciberattacco o delle sue ripercussioni sia nella sua totalità sia in parte.

[3] Se il servizio o l'autorità in questione necessita di informazioni supplementari rispetto a quelle menzionate all'articolo 74*e*, il gestore può trasmetterle direttamente a tale servizio o autorità attraverso il sistema.

L'articolo 74*f* è stato commentato da 34 partecipanti alla consultazione, 4 di questi (RAILplus, santésuisse, UniBE e La Posta) hanno accettato il testo così com'è. Nessun partecipante ha respinto del tutto l'articolo. La grande maggioranza dei pareri riguardano la centralizzazione dei canali di trasmissione delle informazioni all'NCSC e alle autorità autorizzate dalla legge.

- **Osservazioni generali sull'articolo 74*f***

CH++ ritiene che l'articolo 74*f* debba essere adeguato citando esplicitamente la trasmissione dei dati mediante un'interfaccia protetta. Inoltre l'NCSC dovrebbe adottare un approccio basato sull'API, come accade per le reti dei partner di Meta/Facebook o AT&T. CH++ ritiene che a tale scopo debba essere creata una base legale appropriata.

Pour Demain e Operation Libero ritengono che debba essere attuata anche un'interfaccia informatica (API) per permettere l'invio di messaggi automatizzati all'NCSC.

UCS, swissuniversities, il Cantone ZH e Swico chiedono che la notifica possa essere trasmessa in modo semplice.

Il Cantone **GR** chiede di chiarire quali informazioni sono trasmesse, a quali autorità e chi può consultarle.

UZH, UNIL e PNR 77 chiedono che le autorità non possano accedere alle informazioni destinate ad altri servizi.

Swico auspica un meccanismo di notifica quanto più libero possibile, per permettere, per esempio, notifiche automatiche mediante RSS feed o AP o mediante scambio di dati attraverso il sistema MISP, di cui dispongono numerose infrastrutture critiche. Inoltre, **Swico** chiede che per la notifica dei ciberattacchi all'NCSC sia possibile continuare a usare il canale di trasmissione delle informazioni tra GovCERT e le infrastrutture critiche attualmente impiegato.

SwissICT ritiene che la trasmissione di informazioni ad altre autorità oltre all'NCSC sia obbligatoria solo per le autorità e non per le imprese.

Raiffeisen è favorevole alla disposizione e chiede l'aggiunta di un capoverso in cui si precisi che il sistema in questione deve anche essere usato dalle altre autorità federali che impongono obblighi di notifica nell'ambito dei ciberattacchi.

Swissgrid auspica che il sistema permetta un invio simultaneo dei dati di notifica all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).

SWITCH chiede che le notifiche possano anche essere trasmesse tramite CERT settoriale comune. Dato che la legge non lo esclude espressamente, **SWITCH** presuppone che le organizzazioni interessate siano libere di organizzarsi di conseguenza.

- **Approvazione dell'articolo 74*f***

RAILplus, santésuisse, UniBE e La Posta approvano l'articolo 74*f*, in particolare la possibilità di trasmettere le informazioni mediante la piattaforma protetta, rispettando le più elevate norme di sicurezza, così come la possibilità di usare altri mezzi per effettuare la notifica, in particolare il modulo esistente dell'NCSC, la posta elettronica o il telefono.

❖ **Richieste di modifica e suggerimenti concernenti l'articolo 74*f***

- **Capoverso 1**

Il Cantone **GE** chiede di precisare che il sistema è gratuito.

- **Capoverso 2**

Secondo l'**Associazione delle banche estere in Svizzera, Swiss Banking, I Verdi, CH++, asut, ISSS e PVL** è bene garantire, al momento dell'attuazione, che gli obblighi di notifica che si sovrappongono (LPD, FINMA ecc.) possano essere adempiuti con un'unica procedura di notifica. **PVL, AES, digitalswitzerland, economiesuisse e Digitale Gesellschaft** si spingono oltre proponendo l'attuazione di uno sportello federale di notifica presso cui adempiere tutti gli obblighi di notifica mediante un unico modulo online.

ISSS e Härting Rechtsanwälte sono favorevoli alla creazione di uno sportello unico, ma chiedono chiarimenti sulle informazioni che possono essere trasmesse, a chi e con quale contenuto. Per esempio, ritengono necessario chiarire se anche le informazioni fornite all'NCSC e da questi trasmesse all'IFPDT rientreranno nel campo dell'articolo 24 capoverso 6 della revisione della LPD (nessuna incriminazione nel procedimento penale). Poiché l'articolo74*g* LSIn permette all'NCSC di chiedere informazioni supplementari, il campo della comunicazione a terzi si amplia. Tale comunicazione, spesso molto informale a livello tecnico, non deve divenire oggetto di procedimento penale secondo la revisione della LPD qualora siano coinvolti dati personali. Occorre dunque una regolamentazione più dettagliata per sapere quali informazioni possono essere condivise e con chi, e quali possano essere le conseguenze.

UZH, UNIL e PNR 77 sottolineano la necessità di modificare l'articolo 73*c* inserendo un rimando esplicito in caso di effettiva volontà di applicare l'articolo 73*c* capoverso 1–3 dell'avamprogetto LSIn alle comunicazioni sui ciberattacchi notificati, affinché l'NCSC possa, in modo pienamente legale, trasmettere ad altre autorità le informazioni di cui all'articolo 73*c* capoversi 1 e 2.

- **Capoverso 3**

ISSS e Härting Rechtsanwälte chiedono che il capoverso 3 sia soppresso per garantire che le altre istituzioni e autorità ricevano unicamente le informazioni cui hanno legalmente diritto o che sono giustificate nell'ambito della finalità della legislazione applicabile.

Il Cantone **GE** chiede di precisare in questo capoverso che il servizio o l'autorità deve avere «legittimamente» necessità delle informazioni interessate,

3.3.2.15 Articolo 74*g* Obbligo d'informazione

Il gestore dell'infrastruttura critica deve fornire al NCSC informazioni complementari sul contenuto della notifica di cui all'articolo 74*e* che gli occorrono per l'adempimento dei propri compiti volti a respingere ulteriori ciberattacchi alle infrastrutture critiche.

Su questo articolo si sono espressi nove partecipanti alla procedura di consultazione, nessuno lo ha accettato nella sua versione attuale.

❖ **Osservazioni generali sull'articolo 74*g***

Secondo **ISSS e Härting Rechtsanwälte**, questa disposizione amplia il campo della comunicazione con i terzi. Pertanto sarebbe bene definire la portata dell'obbligo d'informazione.

Inoltre, **scienceindustries** ritiene opportuno definire chiaramente le informazioni complementari che l'NCSC è autorizzato a chiedere.

Secondo **swissICT**, per non gravare ulteriormente su imprese, istituti, autorità e Comuni in periodi di difficoltà, le informazioni complementari dovrebbero essere richieste durante la crisi solo se assolutamente necessario per la sicurezza dell'approvvigionamento interessato.

Il Cantone **TG** chiede che l'articolo sia più particolareggiato in modo che anche i Cantoni possano rispettare le loro direttive in materia di cibersicurezza.

UniBE auspica chiarimenti sulle attese in termini di contenuto e di tempistiche legate a questo obbligo.

- **Bocciatura dell'articolo 74*g***

Secondo **VUD**, questa disposizione è troppo imprecisa e ne richiede la soppressione senza sostituzione poiché il contenuto della notifica è già disciplinato esaustivamente nell'articolo 74*e* LSIn.

- **Richieste di modifica e suggerimenti concernenti l'articolo 74*g***

Scienceindustries chiede di modificare questa disposizione per prevedere che i gestori siano tenuti a fornire le informazioni in questione solo nella misura possibile.

Il Cantone **GE** chiede che le informazioni siano fornite all'NCSC «il prima possibile».

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

[1] Se vi sono indizi di una violazione dell'obbligo di notifica o d'informazione, il NCSC ne informa il gestore dell'infrastruttura critica.
[2] Se, nonostante questa informazione, il gestore non adempie il suo obbligo, il NCSC emana una decisione sugli obblighi da adempiere, fissando un termine con la comminatoria della multa di cui all'articolo 74*i*.

Solo quattro partecipanti alla consultazione hanno affrontato la questione della violazione dell'obbligo di notifica o d'informazione.

- **Approvazione dell'articolo 74*h***

Il **Centre Patronal** approva l'articolo.

- **Bocciatura dell'articolo 74*h***

Scienceindustries, aeroporto di Ginevra e digitalswitzerland sono contrari all'articolo perché ritengono che l'obbligo di notifica potrebbe indurre un'impresa a violare le leggi sulla protezione dei dati nel paese in cui ha sede o a violare l'obbligo di notifica in Svizzera.

- **Richieste di modifica e suggerimenti concernenti l'articolo 74*h***

UZH, UNIL e PNR 77 chiedono che questo articolo garantisca ai soggetti interessati il rispetto del diritto di essere ascoltati.

3.3.2.17 Articolo 74*i* Infrazioni contro le decisioni dell'NCSC

[1] Chiunque, intenzionalmente, non ottempera a una decisione del NCSC passata in giudicato intimatagli con la comminatoria della pena prevista dal presente articolo o a una decisione dell'autorità di ricorso è punito con la multa sino a 100 000 franchi.

[2] Alle infrazioni commesse nell'azienda è applicabile l'articolo 6 della legge federale del 22 marzo 1974 sul diritto penale amministrativo (DPA)[3].

[3] Se la multa applicabile non supera i 20 000 franchi e se la determinazione delle persone punibili secondo l'articolo 6 DPA esige provvedimenti d'inchiesta sproporzionati all'entità della pena, l'autorità può prescindere da un procedimento contro dette persone e, in loro vece, condannare l'azienda al pagamento della multa.

[4] In caso di infrazione contro una decisione del NCSC, il perseguimento e il giudizio sono demandati ai Cantoni.

30 partecipanti alla procedura di consultazione si sono espressi sull'articolo 74*i*; 13 ne richiedono la soppressione.

❖ Osservazioni generali sull'articolo 74*i*

Secondo **I Verdi e CH++**, il testo dell'articolo deve esprimere in modo più esplicito che le sanzioni previste si applicano al livello della direzione delle organizzazioni, non degli specialisti.

RAILplus propone che siano punibili soltanto le persone giuridiche (indipendentemente dall'ammontare della sanzione). **RAILplus** chiede di disciplinare i casi in cui i subappaltatori sono situati al di fuori del territorio elvetico.

Il **Partito Pirata** e il **Cantone GE** dichiarano che, per garantire la proporzionalità delle multe, il legislatore dovrebbe definirle in misura proporzionale alla cifra d'affari dell'azienda (ad es. il 4 % della cifra d'affari annua).

Il **PS** ritiene opportune le misure previste dall'articolo 74*i*. Tuttavia suggerisce di verificare dopo cinque anni se le sanzioni citate nell'articolo 74*i* LSIn sono sufficienti e se sono stati rispettati i principi di uguaglianza del trattamento e della proporzionalità.

Swissgrid chiede se il termine «intenzionalmente» copre anche l'eventuale dolo.

I Cantoni **SO e UR** chiedono che la multa sia applicata solo previa consultazione (scritta) dell'NCSC con il trasgressore.

UZH, UNIL e PNR 77 non ritengono che l'importo della multa abbia forza dissuasiva, in particolare in confronto all'importo previsto nella LPD.

❖ Bocciatura dell'articolo 74*i*

AEROSUISSE, La Posta, Raiffeisen, Swisscom, Sunrise, SWITCH, Coop, asut, economiesuisse e Helvetia Assicurazioni non vedono l'utilità di imporre i nuovi obblighi mediante disposizioni penali, che respingono per principio.

Digitalswitzerland e Swico ritengono che gli articoli 74*h* e 74*i* LSIn siano contrari allo spirito di cooperazione tra Stato ed economia.

ISSS, Härting Rechtsanwälte e Swiss Banking considerano l'articolo in oggetto controproducente in quanto potrebbe ostacolare le notifiche volontarie che vadano oltre il semplice obbligo.

[3] RS **313.0**

Scienceindustries chiede la soppressione degli articoli 74*h* e 74*i* perché la loro formulazione concentra inevitabilmente l'attenzione delle imprese sul controllo dei rischi legali potenziali connessi alla notifica dei ciberattacchi.

Inoltre, secondo **scienceindustries, i Cantoni SO e TG, UTP e USAM** l'importo massimo delle multe inflitte crea un pericolo esistenziale sul piano amministrativo, in quando la multa sarebbe esageratamente elevata e sproporzionata, in particolare per le piccole e medie imprese.

L'**aeroporto di Ginevra** respinge la disposizione ritenendola troppo coercitiva.

❖ **Richieste di modifica e suggerimenti concernenti l'articolo 74*i***

- **Capoverso 1**

L'**UTP** chiede che l'importo della multa prevista al capoverso 1 sia stabilito in un massimo di 10 000 franchi.

- **Capoverso 3**

Secondo **swissICT**, l'importo previsto al capoverso 3 dovrebbe essere aumentato da 20 000 a 50 000 franchi. Ciò consentirebbe, da un lato, di evitare spese d'inchiesta sproporzionate nei casi di minore importanza e, dall'altro, di allinearsi all'articolo 64 capoverso 2 della revisione della LPD.

L'**UTP** chiede che l'importo della multa prevista al capoverso 3 sia stabilito in un massimo di 5000 franchi.

3.3.2.18 Articolo 75 Trattamento di dati personali

[1] Per l'adempimento dei propri compiti, il NCSC può trattare dati personali, ivi compresi elementi di indirizzo di cui all'articolo 3 lettera f LTC[4] e i relativi dati personali degni di particolare protezione, che contengono informazioni su:

a. opinioni religiose, filosofiche o politiche; il trattamento è ammesso unicamente qualora sia necessario per la valutazione di minacce e pericoli concreti nell'ambito della cibersicurezza;
b. procedimenti e sanzioni di carattere amministrativo o penale.

[2] Può trattare i dati personali all'insaputa delle persone interessate, se altrimenti lo scopo del trattamento sarebbe compromesso o l'informazione della persona interessata comporterebbe un onere sproporzionato.

[3] In caso di indizi concreti di usurpazione d'identità o di utilizzazione non autorizzata di elementi di indirizzo, il NCSC informa le persone la cui identità è usurpata o i cui elementi di indirizzo sono utilizzati senza autorizzazione; sono fatti salvi gli articoli 18*a* capoverso 4 lettera b e 18*b* LPD[5].

Nessuno dei partecipanti desidera mantenere l'articolo nella sua versione attuale.

❖ **Osservazioni generali sull'articolo 75**

Privatim è favorevole all'articolo 75 ma chiede che il trattamento sia effettuato con dati anonimizzati, se sono sufficienti dati che non fanno riferimento alle persone.

Per la trasmissione dei dati personali, **Scienceindustries** chiede di considerare e di disciplinare giuridicamente le eventuali incompatibilità con le varie legislazioni estere in materia di protezione dei dati.

[4] RS **784.10**
[5] RS **235.1**

La Posta chiede che il trattamento delle informazioni riservate sia disciplinato in modo più preciso al fine di garantire la riservatezza delle notifiche.

Swisscom e La Posta auspicano che nell'ambito dell'attuale progetto di revisione della LSIn sia introdotta una deroga che, quale *lex specialis*, prevalga sul principio di trasparenza secondo la LTrans.

Raiffeisen ritiene che le notifiche ai sensi della nuova regolamentazione debbano rispettare il segreto professionale e in tale ottica propone di aggiungere un capoverso in cui si stabilisca che le autorità debbano trattare le informazioni trasmesse in modo riservato e che le informazioni non possano essere trasmesse qualora ciò rappresenti un pericolo per la sicurezza dell'azienda o delle persone interessate.

❖ **Bocciatura dell'articolo 75**

Il Cantone **TG** ritiene che l'NCSC non debba avere accesso ai dati personali e quindi respinge l'articolo 75.

❖ **Richieste di modifica e suggerimenti concernenti l'articolo 75**

- **<u>Capoverso 1</u>**

EGov-Schweiz ritiene problematiche le competenze in materia di trattamento dei dati sensibili da parte dell'NCSC indicate nell'articolo 75, in particolare in relazione alle possibilità di trasmissione in Svizzera e all'estero secondo gli articoli 76 e 77. **EGov-Schweiz** muove dunque dal principio che, in caso di necessità, l'NCSC ricorra alla polizia e al SIC anziché tentare di trattare direttamente i dati.

Secondo **privatim**, tenuto conto che l'NCSC non svolge i compiti del SIC e non è un'autorità di perseguimento penale, il volume dei dati personali trattati conformemente all'articolo 75 capoverso 1 dell'avamprogetto LSIn non appare proporzionato senza ulteriori limitazioni (soprattutto riguardo alla tassativa necessità di adempiere i compiti). **Privatim** raccomanda di aggiungere le necessarie limitazioni.

- **<u>Capoverso 1 lettera a</u>**

Il Cantone **GE** chiede di modificare la lettera a per precisare che il trattamento si riferisce a «questi» dati.

Il Cantone **GR** auspica la soppressione di questa disposizione.

Il **PVL** critica l'entità dei dati personali che l'NCSC è autorizzato a trattare secondo l'avamprogetto e chiede che sia esplicitata la trasmissione di dati sensibili tra NCSC, autorità penali e SIC. A ciò si aggiunge il fatto che nel caso presente non è prevista nessuna vigilanza particolare. Pertanto non è possibile garantire che i dati non siano utilizzati illecitamente.

- **<u>Capoverso 2</u>**

Privatim ritiene che la separazione delle competenze tra NCSC, autorità penali e SIC debba ricevere maggiore attenzione. Pertanto, l'articolo 75 capoverso 2 LSIn (trattamento dei dati personali all'insaputa delle persone interessate) dovrebbe limitarsi ai casi di procedura penale in corso.

- **<u>Capoverso 3</u>**

Migros auspica che tale disposizione venga armonizzata con le disposizioni corrispondenti dell'articolo 24 della revisione della LPD.

3.3.2.19 Articolo 76 Cooperazione a livello nazionale

[1] Il NCSC può comunicare dati personali ai gestori di infrastrutture critiche, sempre che ciò sia necessario per proteggere le infrastrutture critiche da ciber-rischi.

[2] I gestori di infrastrutture critiche possono comunicare dati personali al NCSC, sempre che ciò sia necessario per proteggere le infrastrutture critiche da ciber-rischi.

[3] Il NCSC può comunicare ai fornitori di servizi di telecomunicazione elementi di indirizzo e i relativi dati personali, sempre che ciò sia necessario per proteggere le infrastrutture critiche da ciber-rischi.

[4] I fornitori di servizi di telecomunicazione possono comunicare al NCSC elementi di indirizzo e i relativi dati personali, sempre che ciò sia necessario per proteggere le infrastrutture critiche da ciber-rischi.

Sul presente testo della legge si sono espressi sette partecipanti.

❖ Osservazioni generali sull'articolo 76

Scienceindustries ritiene che i capoversi 1 e 2 debbano almeno prevedere in modo restrittivo che la trasmissione di tali informazioni, in particolare ai concorrenti che operano in mercati simili, non possa avere luogo senza il consenso del titolare dei dati.

Swico sottolinea l'importanza di mantenere i canali di comunicazione prestabiliti tra NCSC, infrastrutture critiche e altre parti coinvolte.

UTP chiede che il rapporto tra le disposizioni dell'articolo 76 capoverso 1, da un lato, e quelle degli articoli 73*b* capoverso 2 e 73*c*, dall'altro, sia chiarito specificando che l'NCSC comunica i dati personali ai gestori delle infrastrutture critiche a condizione che ciò sia necessario per la protezione delle stesse contro i ciber-rischi.

Il Cantone **GE** chiede di specificare che si tratta delle infrastrutture critiche secondo l'articolo 74*b* con (o senza) le eccezioni dell'articolo 74*c*. Chiede inoltre che sia menzionato l'IFPDT.

❖ Richieste di modifica e suggerimenti concernenti l'articolo 76

- **<u>Capoverso 1</u>**

UZH, UNIL e PNR 77 chiedono di sostituire, al capoverso 1, «utiles» con «nécessaires» (nel testo italiano è già presente «necessario»).

- **<u>Capoverso 2</u>**

L'**ISSS** chiede che il capoverso 2 sia modificato per specificare che i gestori di infrastrutture critiche possono comunicare dati personali all'NCSC, sempre che ciò sia necessario per proteggere le *loro* infrastrutture critiche da ciberrischi.

- **<u>Capoverso 3</u>**

L'**ISSS** chiede che il capoverso 3 sia modificato per specificare che si applica soltanto ai fornitori di servizi di telecomunicazione che non sono anche gestori di infrastrutture critiche.

- **<u>Capoverso 4</u>**

L'**ISSS** chiede che il capoverso 4 sia modificato per specificare che si applica soltanto ai fornitori di servizi di telecomunicazione che non sono anche gestori di infrastrutture critiche.

UZH, UNIL e PNR 77 chiedono che la disposizione preveda piuttosto che «i fornitori di servizi di telecomunicazione possono comunicare all'NCSC dati personali, compresi gli elementi di indirizzo».

3.3.2.20 Articolo 76*a* Sostegno alle autorità

[1] Il NCSC sostiene il SIC nell'individuare tempestivamente e nello sventare minacce per la sicurezza interna o esterna, nel valutare la situazione di minaccia e nell'assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche conformemente all'articolo 6 capoversi 1 lettera a, 2 e 5 LAIn[6] con valutazioni sul numero, sul tipo e sulla portata dei ciberattacchi nonché con analisi tecniche dei ciber-rischi.

[2] Concede al SIC mediante procedura di richiamo l'accesso a informazioni che permettono di risalire all'identità e al modo di operare degli autori di ciberattacchi

[3] Il NCSC concede alle autorità di perseguimento penale mediante procedura di richiamo l'accesso a informazioni che permettono di risalire all'identità e al modo di operare degli autori di ciberattacchi.

[4] Può concedere ai servizi cantonali competenti per la cibersicurezza mediante procedura di richiamo l'accesso alle informazioni necessarie per proteggere le autorità cantonali e le infrastrutture critiche cantonali da ciber-rischi.

Sul sostegno alle autorità si sono espressi sette partecipanti alla consultazione.

❖ Osservazioni generali sull'articolo 76*a*

Il Cantone **UR** chiede che le informazioni sugli autori dei ciberattacchi, sui metodi e sulle tattiche siano trasmesse integralmente.

Il Cantone **NW** ritiene che le informazioni condivise con il SIC debbano essere rese disponibili anche a tutte le autorità di perseguimento penale.

Il Cantone **ZG** ritiene che la cerchia dei destinatari delle valutazioni e delle analisi tecniche vada estesa anche alle autorità di perseguimento penale.

❖ Approvazione dell'articolo 76*a*

Swiss Banking approva la presente regolamentazione.

❖ Richieste di modifica e suggerimenti concernenti l'articolo 76*a*

- **<u>Capoverso 2</u>**

L'**UTP** chiede che il capoverso 2 sia modificato per specificare che le informazioni in questione possano riguardare *unicamente* l'identità e il modo di operare degli autori dei ciberattacchi.

- **<u>Capoverso 3</u>**

L'**UTP** chiede che il capoverso 3 sia modificato per specificare che le informazioni in questione possano riguardare *unicamente* l'identità e il modo di operare degli autori dei ciberattacchi.

Il Cantone **BE** auspica la soppressione della presente disposizione se l'articolo 73*c* viene abrogato.

Secondo p**rivatim**, l'accesso, mediante procedura di richiamo, alle informazioni ottenute dall'NCSC grazie all'obbligo di notifica deve essere limitato o conseguito mediante procedura «push». Ciò deve valere per il SIC (art. 76*a* cpv. 2 LSIn), per le autorità di perseguimento penale (art. 76*a* cpv. 3 LSIn) e per i servizi cantonali competenti per la cibersicurezza (art. 76*a* cpv. 3 LSIn).

- **<u>Capoverso 4</u>**

[6] RS **121**

Il Cantone **BE** auspica la soppressione del presente capoverso se l'articolo 73*c* viene abrogato.

3.3.2.21 Articolo 77 Cooperazione a livello internazionale

[1] Il NCSC può scambiare informazioni con servizi esteri e internazionali competenti per la cibersicurezza se questi ultimi necessitano di tali dati per l'adempimento di compiti corrispondenti a quelli del NCSC. Se lo scambio di informazioni concerne anche dati personali di cui all'articolo 75 si applica l'articolo 6 LPD[7].
[2] Lo scambio di informazioni secondo il capoverso 1 è ammesso soltanto se i servizi esteri e internazionali garantiscono che i dati sono trattati esclusivamente per i fini previsti da tale disposizione.
[3] Se le informazioni sono necessarie per un procedimento legale all'estero, si applicano le disposizioni in materia di assistenza amministrativa e di assistenza giudiziaria

In merito alla cooperazione a livello internazionale si sono espressi sette partecipanti alla consultazione. Nessuno ha bocciato la disposizione.

❖ Osservazioni generali sull'articolo 77

Swiss Banking è favorevole all'articolo 77 se le informazioni sono necessarie alla lotta contro i ciber-rischi e in particolare ai fini della LSIn (una restrizione prevista espressamente all'art. 77 cpv. 1 1° periodo). Se sono coinvolti dati personali ai sensi dell'articolo 75, in caso di trasmissione dei dati all'estero deve essere rispettato l'articolo 6 LPD.

Scienceindustries è critica riguardo alla trasmissione dei dati riservati, in particolare di quelli personali. Ritiene opportuno precisare, in modo restrittivo e con applicazione ai capoversi 1–3, che la trasmissione di tali informazioni non può avvenire senza il consenso del titolare dei dati.

VUD chiede che lo scambio di informazioni con le autorità estere secondo l'articolo 77 LSIn sia rigorosamente anonimo.

Secondo il **MPC**, l'articolo 77 LSIn dovrebbe rientrare nell'ambito delle disposizioni già esistenti in materia di cooperazione a livello internazionale, in particolare nel campo dell'assistenza giudiziaria.

❖ Richieste di modifica e suggerimenti concernenti l'articolo 77

- **Capoverso 1**

L'**UTP** non ritiene chiaro il rapporto tra le disposizioni dell'articolo 77 capoverso 1, da un lato, e quelle degli articoli 73*b* capoverso 2 e 73*c* dall'altro. Di conseguenza chiede che il capoverso 1 preveda che gli articoli 73*b* capoverso 2 e 73*c* LSIn siano applicabili in aggiunta all'articolo 6 LPD.

Privatim è favorevole al capoverso 1.

Secondo l'**ISSS** il capoverso 1 deve specificare che l'articolo 10*a* LPD è applicabile in aggiunta all'articolo 6 LPD.

- **Capoverso 2**

Per garantire che in caso di scambio di informazioni l'autorità estera utilizzi le informazioni ricevute soltanto per la lotta contro i ciber-rischi, **Swiss Banking** propone di completare la regolamentazione prevedendo che l'autorità in questione debba trattare le informazioni trasmesse in modo riservato e che non si possa trasmettere le informazioni qualora ciò rappresenti un pericolo per la sicurezza dell'azienda o delle persone interessate.

[7] RS **235.1**

L'**ISSS** chiede di aggiungere al capoverso 2 che lo scambio di informazioni è autorizzato soltanto se i servizi esteri o internazionali garantiscono l'utilizzo dei dati conformemente alla legislazione sulla protezione dei dati.

- **Capoverso 3**

Il **MPC** chiede di prevedere un meccanismo di coordinamento e propone quindi di aggiungere un secondo periodo al capoverso 3, per specificare che le informazioni trasmesse possono essere utilizzate per giustificare una richiesta di assistenza amministrativa o giudiziaria.

Considerato che l'NCSC non è un'autorità di perseguimento penale, **privatim** chiede maggiori precisazioni in merito alle disposizioni da cui derivano le competenze nazionali in materia di assistenza amministrativa e giudiziaria.

3.3.2.22 Articolo 79 capoverso 1(conservazione e archiviazione dei dati)

[1] Il NCSC conserva i dati personali soltanto fino a che sono utili per prevenire minacce o individuare incidenti, ma al massimo per cinque anni dall'ultimo utilizzo; per i dati personali degni di particolare protezione il termine è di due anni.

Sul termine di conservazione dei dati personali da parte dell'NCSC si sono espressi dieci partecipanti alla consultazione.

❖ Osservazioni generali sull'articolo 79 capoverso 1

CH++ propone di precisare la nozione di «utilizzo», specificando ad esempio «utilizzo obbligatorio». La semplice consultazione di una registrazione non può chiaramente determinare la proroga dei termini di conservazione autorizzati.

UTP, Migros così come UZH, UNIL e PNR 77 chiedono maggiori precisazioni in merito all'espressione «ultimo utilizzo».

ISSS, Härting Rechtsanwälte e privatim ritengono che, secondo il principio di proporzionalità in materia di protezione dei dati, i dati debbano essere conservati solo per il tempo necessario a raggiungere l'obiettivo. Dai dati personali è possibile generare modelli anonimizzati. **ISSS e Härting Rechtsanwälte** propongono di limitare a sei mesi la durata di conservazione dei dati sensibili e di autorizzare la conservazione per una durata illimitata di quanto appreso grazie ai dati personali, sotto forma di modelli identificati o in forma anonimizzata.

La **CCPCS** chiede che il termine di conservazione dei dati sia armonizzato con gli articoli 97 e 109 del codice penale.

Il Cantone **BE** auspica che la disposizione sia modificata in modo da impedire la cancellazione dei dati, in generale, prima della scadenza del termine di prescrizione dell'azione penale per le infrazioni interessate.

3.3.2.23 Modifica di altri atti normativi

Gli atti normativi qui appresso sono modificati come segue:

1. Legge del 23 marzo 2007 sull'approvvigionamento elettrico[8]

Art. 8*a* Protezione contro i ciber-rischi

[1] I gestori di rete, i produttori e i gestori di impianti di stoccaggio adottano misure per proteggere adeguatamente i loro impianti dai ciber-rischi.

[2] Il Consiglio federale può estendere tale obbligo ad altri partecipanti.

2. Legge federale del 25 settembre 2020 sulla protezione dei dati[9]

Art. 24 cpv. 5bis

[5bis] L'IFPDT può inoltrare la notifica al Centro nazionale per la cibersicurezza con il consenso del titolare del trattamento soggetto all'obbligo di notifica, per un'analisi dell'incidente. La comunicazione può contenere dati personali, ivi compresi dati personali degni di particolare protezione concernenti sanzioni e procedimenti amministrativi o penali riguardanti il titolare del trattamento soggetto all'obbligo di notifica.

Solo sei partecipanti alla consultazione hanno preso posizione in merito alla modifica della legge sull'approvvigionamento elettrico (LAEl) e della LPD. Nessuno ha richiesto la soppressione dell'articolo8*a* LAEl. **ISSS e Härting Rechtsanwälte** auspicano la soppressione dell'articolo 24 capoverso 5bis LPD.

- **Osservazioni generali sull'articolo 24 capoverso 5bis LPD**

L'**UTP** chiede di modificare l'articolo 24 capoverso 5bis LPD in modo che l'IFPDT possa trasmettere la notifica *unicamente* con il consenso del titolare del trattamento.

Il Cantone **GE** ritiene necessario prevedere una comunicazione vincolante da parte dell'NCSC all'IFPDT; la comunicazione dell'IFPDT non necessita dell'autorizzazione della persona responsabile della notifica, se questa soddisfa le condizioni della presente legge.

UZH, UNIL e PNR 77 propongono la seguente riformulazione: «… inoltrare [*la notifica*] al Centro nazionale… con il consenso [della persona tenuta a *notificare*]…».

Inoltre, **UZH, UNIL e PNR 77** sottolineano che deve essere possibile inoltrare tutti i dati sensibili, non solo alcuni di essi.

- **Bocciatura dell'articolo 24 capoverso 5bis LPD**

ISSS e Härting Rechtsanwälte chiedono l'abrogazione di questa disposizione perché, se viene creato un servizio centrale per registrare tutte le notifiche, questa aggiunta non è più necessaria.

3.4 Ulteriori richieste e suggerimenti concernenti l'avamprogetto

Swiss Banking chiede che l'attuale testo di legge sia armonizzato con la Comunicazione FINMA sulla vigilanza 05/20 – Obbligo di notificare i ciberattacchi secondo l'articolo 29 capoverso 2 LFINMA.

IG eHealth chiede che il Consiglio federale e il Parlamento garantiscano all'NCSC risorse sufficienti in termini di personale.

8 RS **734.7**
9 RS **235.1**; FF **2020** 6695

Il Cantone **ZH** propone di introdurre l'obbligo di segnalazione per tappe (per es. settore per settore), in modo da maturare gradualmente esperienza.

La **CCPCS** chiede di disciplinare il modo in cui le autorità di perseguimento penale devono trattare le notifiche che ricevono al posto dell'NCSC.

Secondo **asut, Swisscom e Sunrise** è necessario un coordinamento efficace tra questo progetto e la revisione dell'ordinanza sui servizi di telecomunicazione.

3.5 Richieste e suggerimenti su altri argomenti

CH++ e Pour Demain sono favorevoli alla trasformazione dell'NCSC in ufficio federale. Il **Partito Pirata** auspica la creazione di un dipartimento della trasformazione digitale.

Il Cantone **FR** chiede che oltre all'introduzione di un obbligo di notifica siano adottate altre misure di contrasto alla cibercriminalità (per es. misure di sensibilizzazione della popolazione).

Il **Partito Pirata** chiede che in futuro le infrastrutture critiche usino soltanto software *open source* (OSS). Inoltre ritiene necessario creare un fondo ampiamente dotato per finanziare le revisioni sulla sicurezza dei software di uso comune (ad es. OSS / FOSS). Infine auspica che nel lungo termine la Svizzera si doti delle risorse utili a sviluppare e produrre in proprio l'hardware e i software necessari per le infrastrutture critiche.

4 Allegato

4.1 Cantoni

ZH	Staatskanzlei des Kantons Zürich	Neumühlequai 10 Postfach 8090 Zürich staatskanzlei@sk.zh.ch
BE	Staatskanzlei des Kantons Bern	Postgasse 68 3000 Bern 8 info@sta.be.ch
LU	Staatskanzlei des Kantons Luzern	Bahnhofstrasse 15 6002 Luzern staatskanzlei@lu.ch
UR	Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf ds.la@ur.ch
SZ	Staatskanzlei des Kantons Schwyz	Regierungsgebäude Bahnhofstrasse 9 Postfach 1260 6431 Schwyz stk@sz.ch
OW	Staatskanzlei des Kantons Obwalden	Rathaus 6061 Sarnen staatskanzlei@ow.ch
NW	Staatskanzlei des Kantons Nidwalden	Dorfplatz 2 Postfach 1246 6371 Stans staatskanzlei@nw.ch
GL	Staatskanzlei des Kantons Glarus	Rathaus 8750 Glarus staatskanzlei@gl.ch
ZG	Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug info@zg.ch
FR	Chancellerie d'État du Canton de Fribourg	Rue des Chanoines 17 1701 Fribourg chancellerie@fr.ch
SO	Staatskanzlei des Kantons Solothurn	Rathaus Barfüssergasse 24 4509 Solothurn kanzlei@sk.so.ch
BS	Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel staatskanzlei@bs.ch
BL	Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal landeskanzlei@bl.ch
SH	Staatskanzlei des Kantons Schaffhausen	Beckenstube 7 8200 Schaffhausen

		staatskanzlei@ktsh.ch
AR	Kantonskanzlei des Kantons Appenzell Ausserrhoden	Regierungsgebäude 9102 Herisau Kantonskanzlei@ar.ch
AI	Ratskanzlei des Kantons Appenzell Innerrhoden	Marktgasse 2 9050 Appenzell info@rk.ai.ch
SG	Staatskanzlei des Kantons St. Gallen	Regierungsgebäude 9001 St. Gallen info.sk@sg.ch
GR	Standeskanzlei des Kantons Graubünden	Reichsgasse 35 7001 Chur info@gr.ch
AG	Staatskanzlei des Kantons Aargau	Regierungsgebäude 5001 Aarau staatskanzlei@ag.ch
TG	Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld staatskanzlei@tg.ch
TI	Cancelleria dello Stato del Cantone Ticino	Piazza Governo 6 6501 Bellinzona can-scds@ti.ch
VD	Chancellerie d'État du Canton de Vaud	Place du Château 4 1014 Lausanne info.chancellerie@vd.ch
VS	Chancellerie d'État du Canton du Valais	Planta 3 1950 Sion Chancellerie@admin.vs.ch
NE	Chancellerie d'État du Canton de Neuchâtel	Le Château Rue de la Collégiale 12 2000 Neuchâtel Secretariat.chancelle-rie@ne.ch
GE	Chancellerie d'État du Canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3 service-adm.ce@etat.ge.ch
JU	Chancellerie d'État du Canton du Jura	2, rue de l'Hôpital 2800 Delémont chancellerie@jura.ch
CCDJP	CCDJP Conférence des directrices et directeurs des départe-ments cantonaux de justice et police (CCDJP)	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@kkjpd.ch
CDS	CDS Conférence suisse des directeurs de la santé	Haus der Kantone Speichergasse 6 Postfach 3001 Bern office@gdk-cds.ch
CG MPS	CG MPS Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers	Haus der Kantone Speichergasse 6 Postfach

		3001 Bern
	CCPS Conférence des Commandants des Polices Cantonales de Suisse	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@kkpks.ch
CPS	Conférence des procureurs suisses	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@ssk-cps.ch

4.2 Partiti rappresentati nell'Assemblea federale

Le Centre	Le Centre	Generalsekretariat Hirschengraben 9 Postfach 3001 Bern info@die-mitte.ch
PLR	Les Libéraux-Radicaux	Generalsekretariat Neuengasse 20 Postfach 3001 Bern info@fdp.ch
Les VERT-E-S suisses	Les VERT-E-S suisses	Waisenhausplatz 21 3011 Bern gruene@gruene.ch
PVL	Parti vert'libéral Suisse	Monbijoustrasse 30 3011 Bern schweiz@grunliberale.ch
UDC	Union démocratique du centre	Generalsekretariat Postfach 8252 3001 Bern gs@svp.ch
PS	Parti socialiste suisse	Zentralsekretariat Theaterplatz 4 Postfach 3001 Bern verena.lo-embe@spschweiz.ch
Parti pirate suisse	Parti pirate suisse	Piratenpartei Bern, 3000 Bern info@be.piratenpartei.ch

4.3 Associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna

UVS	Union des villes suisses	Monbijoustrasse 8 Postfach 3001 Bern info@staedteverband.ch

4.4 Associazioni mantello nazionali dell'economia

economiesuisse	Fédération des entreprises suisses	Hegibachstrasse 47 Postfach 8032 Zürich info@economiesuisse.ch bern@economiesuisse.ch sandra.spieser@economiesuisse.ch
Swissbanking	L'Association suisse des banquiers	Hotelgasse 10, 3011 Bern
USAM	Union suisse des arts et métiers	Schwarztorstrasse 26 Postfach 3001 Bern info@sgv-usam.ch
USS	Union syndicale suisse	Monbijoustrasse 61, 3007 Bern, info@sgb.ch

4.5 Altri ambienti interessati – pareri espressi su invito

eGov-Schweiz	Association eGov-Schweiz	c/o mundi consulting ag Marktgasse 55 Postfach 3001 Bern info@eGov-Schweiz.ch
privatim	Conférence des Préposé(e)s suisses à la protection des données	c/o Dr. Beat Rudin, Advokat, Postfach 205 4010 Basel kommunikation@privatim.ch
Digitale Gesellschaft	Digitale Gesellschaft	4000 Basel office@digitale-gesellschaft.ch
eHealth	Interessengemeinschaft eHealth	Amthausgasse 18 3011 Bern info@ig-ehealth.ch
asut	ASSOCIATION SUISSE DES TÉLÉCOMMUNICATIONS	Hirschengraben 8 3011 Bern info@asut.ch
Interpension	Inter-pension Interessengemeinschaft autonomer Sammel- und Gemeinschaftseinrichtungen	Gartenstrasse 2 3063 Ittigen info@inter-pension.ch
RAILplus AG	RAILplus AG	Hintere Bahnhofstrasse 85 5001 Aarau info@railplus.ch
AEROSUISSE	Fédération faîtière de l'aéronautique et de l'aérospatiale suisses	Kapellenstrasse 14

		Postfach 3001 Bern info@aerosuisse.ch

4.6 Altri ambienti interessati – pareri spontanei

eAVS/AI	eAVS/AI	p.a. mundi consulting ag Marktgasse 55 Postfach 3001 Bern jerome.brugger@mundicon-sulting.com
ISSS	Information security society switzerland	Kochergasse 6 3011 Bern sekretariat@isss.ch

Centre Patronal	Centre Patronal	Route du Lac 2 1094 Paudex info@centrepatronal.ch
CH++	CH++	marcel.sa-lathe@chplusplus.org
FMH	Fédération des médecins suisses	Nussbaumstrasse 29 Postfach 300 3000 Bern 16 info@fmh.ch
Ausland-banken	Verband der Auslandsbanken in der Schweiz	Usteristrasse 23 8001 Zürich info@afbs.ch
MPC	Ministère public de la Confédération	Guisanplatz 1 3003 Bern info@ba.admin.ch
la Poste	La Poste Suisse SA	Wankdorfallee 4 Postfach 3030 Bern regulatoryaffairs@post.ch
digitals-witzer-land	digitalswitzerland	Waisenhausplatz 14 3011 Bern office@digitalswitzerland-bern.ch
FER	Fédération des entreprises romandes	98 rue de Saint-Jean 1211 Genève 11 yannic.forney@fer-ge.ch
Swico	Swico	Lagerstrasse 33 8004 Zürich info@Swico.ch
GEM	Groupement des Entreprises Multinationales	Rue de Saint-Jean 98 1211 Genève 3 info@gemonline.ch
Pour de-main	Pour demain	Marktgasse 46 3011 Berne info@pourdemain.ch

Santésuisse	Association de la branche de l'assurance-maladie sociale	Römerstrasse 20 Postfach CH-4502 Solothurn mail@santesuisse.ch
Swiss-sICT	SwissICT	Vulkanstr. 120 8048 Zürich info@swissict.ch
Swiss-mem	Association pour les PME et les grandes entreprises de l'industrie technologique suisse	Pfingstweidstrasse 102 Postfach CH-8037 Zürich r.rudolph@swissmem.ch
swissuniversities	Assocaition des des hautes écoles suisses	swissuniversities Effingerstrasse 15 Case Postale 3001 Berne weiss@swissuniversities.ch
VUD	Verein Unternehmendatenschutz	Verein Unternehmens-Daten-schutz VUD c/o IT & Law Consulting GmbH Sternenstrasse 18, 8002 Zürich info@vud.ch
UTP	Union des transports publics	Dählhölzliweg 12 CH-3000 Bern 6 info@voev.ch
AES	Association des entreprises électriques suisses	Hintere Bahnhofstrasse 10 5000 Aarau info@strom.ch
ASIP	Association Suisse des Institutions de Prévoyance	Kreuzstrasse 26 8008 Zurich info@asip.ch
Sci-encein-dustries	Association des Industries Chimie Pharma Life Sciences	Nordstrasse 15 Postfach 8021 Zürich Schweiz info@scienceindustries.ch
Suisse-digital	Association des réseaux de communication	Bollwerk 15 CH-3011 Bern info(at)suissedigital.ch
SSIGE	Société Suisse de l'Industrie du Gaz et des Eaux SSIGE	Grütlistrasse 44 | Postfach | 8027 Zürich info@svgw.ch
ASA	Association suisse d'assurances	Conrad-Ferdinand-Meyer-Strasse 14 Case postale CH-8022 Zurich info@svv.ch
ABG	Association de banques suisses de gestion	
Gachn-ang	Commune de Gachnang (TG)	Hôtel de ville de Gachnang Islikonerstrasse 7 8547 GACHNANG Suisse
NFP 77 ETHZ UNIL	Prise de position commune	

Operation Libero	Mouvement	OPERATION LIBERO CH-3000 Bern futur@operation-libero.ch
AEIS	Fondation institution supplétive LPP	Elias-Canetti-Strasse 2 Postfach 8050 Zurich urs.mueller(S)aeis.ch
Trust Valley	Fondation Trust Valley	Trust Valley EPFL Innovation Park, Bâtiment C CH-1015 Lausanne
UniBE	Université de Berne	Dr. Cord-Ulrich Fündeling Leiter Informatikdienste Hochschulstrasse 6 3012 Bern cord.fuendeling@unibe.ch
UniGE Digital Law Centre	Prise de position commune	Digital Law Center - Uni Mail - Bd du Pont d'Arve 40 - CH-1211 Genève 4 Suisse digitallawcenter@unige.ch
Abraxas	Entreprise Abraxas Informatik AG	The Circle 68 | CH-8058 Zürich-Flughafen peter.gassmann@abraxas.ch
Axpo	Axpo services AG	Axpo Services AG Parkstrasse 23 | 5401 Baden | Switzerland thomas.porchet@axpo.com
Beat Lehmann		Acting Counsel Alcan Holdings Switzerland AG Kongoweg 9 (Home Office) 5034 Suhr b.lehmann-aarau@bluewin.ch
Coop	Coop Genossenschaft	Thiersteinerallee 12 Postfach 2550 4002 Basel Damian.Misteli@coop.ch
Aéroport de ZH		Zürich Flughafen CH-8058 Andrew.karim@zurich-airport.ch
Aéroport de GE		Aéroport international de Genève CP100 CH 1215 Genève
Härting Rechtsanwälte		Landis Gyr Strasse 1 6300 Zug office@haerting.ch
Helvetia	Helvetia assurances AG	Helvetia Versicherungen Hauptsitz St. Alban-Anlage 26 4002 Basel martin.jara@helvetia.ch
Migros	Migros-Genossenschafts-Bund	
Raffeisen		cecile.kessler@raiffeisen.ch

Ro-mande Energei		Rue de Lausanne 53 1110 Morges Oscar.parado@romande-energie.ch
Salt		Salt Mobile SA Rue du Caudray 4 CH-1020 Renens 1
CFF		
Sunrise	Sunrise UPC	Sunrise UPC GmbH Thurgauerstrasse 101B, 8152 Glattpark (Opfikon) Marcel.Huber@sunrise.net
Suva		Fluhmattstrasse 1 Case postale 4358 6004 Luzern Marc.epelbaum@suva.ch
Swiss		Swiss International Air Lines AG P.O. Box ZRHS/V/ABRO CH-8 ronald.abegglen@swiss.com 058 Zürich-Flughafen
Swisscom		Alte Tiefenaustrasse 6 3048 Worblaufen Lorenz.Ing-lin@swisscom.com
Swiss-grid		Bleichemattstrasse 31 Postfach 5001 Aarau info@swissgrid.ch
Switch		Werdtstrasse 2 Postfach 8021 Zürich
TPG	Transports publics genevois	Route de la Chapelle 1 - Case postale 950 - 1212 Grand-Lancy 1 - Suisse Meyer.G@tpg.ch