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