Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS

Berna, 27 novembre 2024

Progetto dell'ordinanza sulla cibersicurezza (OCS)

Procedura di consultazione dal 22 maggio 2024 fino al 13 settembre 2024

Rapporto sui risultati della procedura di consultazione

Indice

1 Situazione iniziale

Il 22 maggio 2024 il Consiglio federale ha approvato il progetto dell'ordinanza sulla cibersicurezza (OCS) e il rapporto esplicativo e ha incaricato il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) di eseguire una procedura di consultazione, che si è svolta tra il 22 maggio 2024 e il 13 settembre 2024. La lista di tutti i partecipanti alla consultazione con le abbreviazioni utilizzate di seguito si trova in allegato.

Sono pervenuti 69 pareri:

69	Totale pareri
23	Governi cantonali
3	Conferenze cantonali e commissioni federali
4	Partiti
2	Associazioni mantello nazionali dei Comuni e delle città
19	Associazioni nazionali
12	Aziende interessate
7	Altri gruppi di interesse

I pareri sono pubblicati sulla piattaforma di pubblicazione del diritto federale «Fedlex».[1]

2 Oggetto del progetto in consultazione

L'11 dicembre 2020 il Consiglio federale ha incaricato il Dipartimento federale delle finanze (DFF) di elaborare le basi legali per l'introduzione di un obbligo di segnalare ciberattacchi a infrastrutture critiche. Il 2 dicembre 2022 il Consiglio federale ha poi approvato all'attenzione del Parlamento il disegno di queste basi legali e il messaggio concernente la modifica della legge federale sulla sicurezza delle informazioni in seno alla Confederazione (legge sulla sicurezza delle informazioni, LSIn) del 18 dicembre 2020[2] . Successivamente il 29 settembre 2023 il Parlamento ha approvato le modifiche della LSIn;[3] il termine di referendum è scaduto inutilizzato il 18 gennaio 2024.

Il progetto di ordinanza contiene, da un lato, le disposizioni d'esecuzione in merito al capitolo 5 della LSIn sottoposto a revisione relativo all'obbligo di segnalare ciberattacchi a infrastrutture critiche. Dall'altro lato, vengono disciplinati anche aspetti organizzativi legati alla cibersicurezza. L'ordinanza entrerà in vigore il 1° aprile 2025 insieme al capitolo 5 della LSIn sottoposto a revisione.

La LSIn è già entrata in vigore il 1° gennaio 2024, senza il capitolo 5 summenzionato, sottoposto a revisione, relativo ai compiti del nuovo Ufficio federale della cibersicurezza (UFCS) e all'obbligo di segnalare ciberattacchi a infrastrutture critiche. Inoltre in tale momento è stata abrogata l'ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale (ordinanza sui ciber-rischi, OCiber) del 27 maggio 2020[4] .[5] Le disposizioni ivi contenute, in particolare le definizioni dei termini, sono in parte state trasferite nella LSIn sottoposta a revisione. Le disposizioni che nell'OCiber disciplinavano la sicurezza informatica della Confederazione sono state riprese nell'ordinanza sulla sicurezza delle informazioni in seno all'Amministrazione federale e all'esercito (ordinanza sulla sicurezza delle informazioni, OSIn)[6]. I compiti del Centro nazionale per la cibersicurezza (NCSC) definiti nell'OCiber, in particolare i compiti nei confronti dell'economia e della popolazione, non sono disciplinati nell'OSIn, in quanto con la revisione della LSIn hanno ricevuto una nuova

1 www.fedlex.admin.ch > Procedure di consultazione > Procedure di consultazione concluse > 2024 > DDPS
2 RS **128**
3 FF **2023** 2296
4 RS **120.73**
5 RU **2023** 735 (allegato 2 numero I).
6 RS **128.1**

base legale. Inoltre il 1° gennaio 2024 l'NCSC è stato trasferito al DDPS in qualità di UFCS. Per questo motivo, le disposizioni organizzative relative all'UFCS si trovano nell'articolo 15*a* capoversi 1 e 2 lettere a–g OOrg-DDPS[7].

I compiti dell'UFCS vengono precisati e descritti in modo più concreto nel progetto di ordinanza, insieme all'obbligo di segnalare ciberattacchi a infrastrutture critiche. L'ordinanza oggetto di questo rapporto disciplina quindi i rapporti tra l'UFCS e le parti interessate esterne all'Amministrazione federale, mentre l'OSIn definisce i compiti e le competenze per la sicurezza delle informazioni all'interno dell'Amministrazione federale.

3 Risultati della procedura di consultazione

3.1 Valutazione complessiva del progetto

L'OCS ottiene un riscontro prevalentemente positivo. La grande maggioranza dei pareri valuta positivamente l'iniziativa per il rafforzamento della cibersicurezza in Svizzera. Molti attori accolgono con soddisfazione gli sforzi volti a migliorare la sicurezza in questo ambito.

Tuttavia, nonostante l'approvazione generale, ci sono varie critiche costruttive e proposte di miglioramento, che spesso riguardano aspetti specifici dell'ordinanza e mirano ad aumentarne la praticabilità e l'efficacia.

Le priorità sono l'armonizzazione e il coordinamento di varie procedure di segnalazione, le precisazioni di alcuni termini e processi nonché un adeguamento degli obblighi di segnalazione, per evitare un onere amministrativo troppo elevato. Anche la maggiore considerazione della collaborazione con le autorità di perseguimento penale nonché la flessibilità in termini di scadenze e deroghe sono dei punti importanti.

Inoltre vari settori, come quello finanziario, quello sanitario e quello delle telecomunicazioni, esprimono le loro richieste specifiche del settore, che rispecchiano le relative esigenze e sfide.

Dal punto di vista federale, i Cantoni sottolineano la necessità di una collaborazione tra Confederazione e Cantoni nonché la considerazione delle strutture cantonali.

Anche gli aspetti economici sono importanti. In linea di principio le associazioni economiche e le aziende sostengono l'ordinanza, ma fanno appello al principio di proporzionalità e chiedono soluzioni sostenibili dal punto di vista economico.

Nel complesso, vi è un ampio consenso sulla necessità di emanare l'OCS, accompagnato dal desiderio di adeguamenti pratici e precisazioni nell'attuazione.

3.2 Pareri concernenti l'OCS raggruppati in base alla valutazione e all'orientamento

3.2.1 Panoramica dei pareri positivi sull'OCS senza proposte di modifica notevoli

Nella procedura di consultazione l'OCS è stata approvata pienamente da alcuni partecipanti:

- Diversi *Cantoni* si sono espressi in modo particolarmente positivo (*BS, OW, SZ, SG, NW* e *TI*).

- Per quanto riguarda i *gestori di infrastrutture*, *Transitgas SA* ha espresso un giudizio molto positivo e ha considerato l'ordinanza come un passo importante per garantire la sicurezza delle infrastrutture critiche. Anche *RAILplus* ha dichiarato che il testo soddisfa le aspettative e non ha aggiunto commenti significativi. La *FAMH* è favorevole all'OCS. L'associazione sottolinea che non tutti i laboratori

7 RS **172.214.1**

medici sono toccati dall'obbligo di segnalare ciberattacchi e raccomanda ai suoi membri di segnalarli volontariamente, anche se non rientrano nella definizione legale.

3.2.2 Valutazione positiva con proposte di miglioramento o osservazioni

L'OCS è stata accolta prevalentemente in modo positivo. Molti partecipanti alla consultazione l'hanno approvata aggiungendo proposte di miglioramento o osservazioni:

- A *livello cantonale* il sostegno è stato ampio. I Cantoni di *AG, BE, FR, GE, GL, GR, LU, SH, SO, UR, VD, VS, ZG* e *ZH* hanno accolto con favore l'ordinanza, ma allo stesso tempo hanno sollevato diverse questioni, tra cui, ad esempio, proposte di miglioramento per le eccezioni all'obbligo di segnalazione (*AG*) nonché richieste di precisazioni e maggiore considerazione della catena di fornitura (*ZH*).

- Alcune *autorità federali* come l'*MPC* e l'*UFDC* hanno in linea di principio sostenuto l'ordinanza, ma hanno chiesto una maggiore considerazione del perseguimento penale o una limitazione dell'onere per le segnalazioni iniziali.

- Diversi *partiti politici* come *il Centro, il PLR* e il *PS* hanno approvato l'ordinanza, ma hanno indicato diversi aspetti da considerare. *Il Centro* ha sottolineato la necessità di strutture nazionali forti, mentre il *PLR* ha messo in guardia da un onere amministrativo eccessivo.

- Anche *associazioni e gruppi d'interesse* come *asut, AES, CH++, digitalswitzerland, economiesuisse, ISSS, PourDemain, usam, Swiss Banking, Swiss FS-CSC, SwissICT, Swico, SUISSEDIGITAL, scienceindustries, ASA, H+, NEDIK, CPS, swissuniversities, PNR 77/PFZ/UNIL e eAVS/AI* hanno ampiamente sostenuto l'ordinanza, ma allo stesso tempo hanno richiamato l'attenzione sul potenziale di miglioramento. Sono stati spesso citati la necessità di un'armonizzazione con i regolamenti esistenti, la richiesta di adeguamenti basati maggiormente su situazioni realistiche e il desiderio di scadenze più flessibili.

- Anche *aziende e gestori di infrastrutture* come *l'aeroporto di Zurigo, FER, Primeo, Migros, FFS, La Posta Svizzera SA, Sunrise, SUVA, Salt, Swissgrid* e *Switch* hanno accolto con favore l'ordinanza, ma hanno in parte sollevato questioni specifiche dei loro settori. Hanno chiesto precisazioni in merito all'obbligo di segnalazione e criticato la complessità dell'ordinanza e i processi di segnalazione non coordinati.

Nel complesso l'OCS gode di un'ampia approvazione, ma allo stesso tempo in molti ambiti vi è un potenziale di miglioramento. Riassumendo, le osservazioni più frequenti riguardano la necessità di precisazioni, l'armonizzazione con i regolamenti esistenti, la considerazione delle esigenze specifiche dei settori e la garanzia di un'attuazione realistica e sostenibile dal punto di vista economico.

3.2.3 Valutazione neutrale o mista

Nell'ambito della procedura di consultazione sull'OCS alcuni partecipanti hanno espresso valutazioni neutrali o miste. Tali feedback sono caratterizzati da pareri cauti o mirati:

- L'*aeroporto di Ginevra* ha assunto una posizione neutrale si è astenuto dal valutare il contenuto dell'ordinanza. Si è limitato a nominare gli adeguamenti dei processi previsti, senza fare alcun commento specifico sull'ordinanza stessa.

- La *CDDGP* ha optato per una posizione neutrale astenendosi completamente dal fornire un parere in merito ai contenuti e lasciando ai singoli Cantoni il compito di esprimersi in merito al progetto.

- Il *Partito Pirata Svizzero* non esprime alcun giudizio sull'OCS, ma nel suo parere si concentra su una questione principale specifica in merito alla divulgazione coordinata delle vulnerabilità.

- *ASIP* si è posizionata in modo molto mirato e si è espressa esclusivamente in merito a un'eccezione all'obbligo di segnalazione per il settore che rappresenta.

3.3 Proposte e osservazioni sull'avamprogetto

3.3.1 Osservazioni preliminari

Di seguito vengono elencate le osservazioni, le proposte di modifica e le critiche in merito alle singole disposizioni del progetto dell'OCS. Vengono citati solo gli argomenti principali espressi in un parere. I pareri particolarmente dettagliati vengono rappresentati unicamente se richiedono modifiche materiali concrete. Ulteriori dettagli sono disponibili nei pareri pubblicati su Internet.

Il presente rapporto non cita approvazioni tacite o rinunce a rispondere in merito a un articolo. Tuttavia i lettori non devono dimenticare che in linea di principio la maggior parte dei partecipanti alla consultazione approva gran parte delle disposizioni dell'ordinanza proposte, nonostante le numerose critiche a singole disposizioni. Non ci sono stati pareri sulla sistematica dell'ordinanza in quanto tale.

3.3.2 Proposte e osservazioni sulle singole disposizioni

3.3.2.1 Articolo 1 (Oggetto)

Art. 1

La presente ordinanza disciplina:

a. la Ciberstrategia nazionale e il suo Comitato direttivo;

b. i compiti dell'Ufficio federale della cibersicurezza (UFCS);

c. lo scambio di informazioni per la protezione dai ciberincidenti e dalle ciberminacce tra l'UFCS e le autorità nonché le organizzazioni;

d. l'obbligo di segnalare ciberattacchi.

In merito al presente articolo sono pervenuti tre pareri, focalizzati principalmente sulla precisazione del campo d'applicazione e sulla delimitazione dell'ambito di validità rispetto ad altri regolamenti:

- *FER* segnala l'assenza di una regolamentazione in materia di ciberdifesa;

- *BL* chiede che si consideri la Rete integrata Svizzera per la sicurezza (RSS):

- *BE* sollecita una chiara distinzione tra i compiti dell'UFCS sanciti specificatamente dalla OCS e le mansioni generali previste dalla OSIn.

3.3.2.2 Articolo 2 (Ciberstrategia nazionale)

Art. 2 Ciberstrategia nazionale
[1] La Ciberstrategia nazionale (CSN) stabilisce il quadro strategico per la prevenzione nell'ambito della cibersicurezza, l'individuazione tempestiva delle ciberminacce, le possibilità di reazione e la resilienza in caso di incidenti, nonché la lotta alla cibercriminalità.
[2] Viene definita d'intesa con i Cantoni.

In merito al campo d'applicazione proposto sono pervenute 13 reazioni.

❖ **Inclusione di ulteriori stakeholder**

- *asut, Salt* e *Switch* chiedono l'inclusione di economia, scienza e società civile nell'elaborazione della CSN. Conseguentemente l'articolo 2 capoverso 2 dev'essere modificato come segue: «Viene definita d'intesa con i Cantoni e con il coinvolgimento del settore economico, scientifico e dei rappresentanti della società civile».

- *ZG* e *Swissgrid* lamentano il mancato coinvolgimento di altri gruppi di interesse, in particolare dei gestori di infrastrutture critiche, nell'elaborazione della CSN.

- *sgv/usam* chiede il coinvolgimento delle rappresentanze comunali nell'elaborazione della CSN.

- *UCS* critica il mancato coinvolgimento delle città/dei Comuni maggiori nell'elaborazione della CSN.

❖ **Ruolo e coinvolgimento di autorità/organizzazioni specifiche**

- *BL* chiede un'integrazione del rapporto esplicativo in cui si specifichi che le attività inerenti alla CSN devono svolgersi in stretto coordinamento con i Cantoni.

- *UR* sottolinea l'importanza della Rete integrata Svizzera per la sicurezza (RSS) che, come tale, dovrà continuare a collaborare in maniera determinante alla futura definizione della CSN.

- *ZH* chiede che nell'aspetto della «lotta alla cibercriminalità» si garantisca il coinvolgimento del Ministero pubblico e della polizia quali autorità competenti in materia.

- *La Posta Svizzera SA* propone di considerare e includere nella composizione anche i rappresentanti di infrastrutture critiche. La formulazione «rappresentanti del settore economico» è troppo poco chiara da questo punto di vista.

❖ **Integrazioni e critiche a livello dei contenuti**

- *ISSS* critica il fatto che nel testo dell'ordinanza non si tenga conto della collaborazione internazionale, nonostante debba avere un ruolo determinante secondo la CSN.

- Le *FFS* chiedono di aggiungere all'elenco dell'articolo 2 capoverso 1 l'«individuazione di minacce» («identity»), in modo tale da riflettere tutte le cinque funzioni del NIST Cybersecurity Framework.

- *ASA* dubita che la base di riferimento della LSIn sia sufficiente per l'emanazione degli articoli 2 segg. della bozza di ordinanza sulla cibersicurezza.

❖ **Valutazioni positive**

- *ZH* approva la definizione coordinata di una CSN.

- *Swico* approva il quadro strategico centrale per la prevenzione, l'individuazione tempestiva e la reazione alle ciberminacce.

3.3.2.3 Articolo 3 (Istituzione e organizzazione del Comitato direttivo)

Art. 3 Istituzione e organizzazione del CD CSN
[1] Il Consiglio federale istituisce un Comitato direttivo della Ciberstrategia nazionale (CD CSN).
[2] Il CD CSN dispone di una segreteria che viene gestita dall'Ufficio federale della cibersicurezza (UFCS).

Due partecipanti alla procedura di consultazione si sono espressi a favore dell'istituzione e organizzazione del CD CSN.

❖ **Sostegno al CD CSN**

- *ISSS* e *La Posta Svizzera SA* sostengono l'istituzione del CD CSN.

3.3.2.4 Articolo 4 (Composizione del CD CSN)

Art. 4 Composizione del CD CSN
[1] Il CD CSN si compone di rappresentanti dei dipartimenti, della Cancelleria federale, dei Cantoni, del settore economico, della società e delle scuole universitarie.
[2] Il Consiglio federale nomina ogni cinque anni i membri del CD CSN, ad eccezione dei rappresentanti dei Cantoni che vengono designati dalla Conferenza dei Governi cantonali.
[3] Nomina il presidente tra i rappresentanti del settore economico, della società o delle scuole universitarie.

I 27 partecipanti alla procedura di consultazione si sono espressi in merito alla composizione del CD CSN.

❖ **Articolo 4 capoverso 1**

- *CH++* approva la composizione estesa del CD CSN, ma chiede chiari criteri di selezione dei membri e un'adeguata rappresentanza di esperti in materia di sicurezza.

- *Swiss Banking e Swiss FS-CSC* propongono di cancellare nel testo dell'ordinanza le parole «della società».

- *economiesuisse* e *scienceindustries* criticano la preventiva definizione della composizione e insieme a *digitalswitzerland, l'aeroporto di ZH, H+, ISSS, VS, Primeo, Swiss Banking, Swiss FS-CSC, VSE, La Posta Svizzera SA, ASA e Swissgrid* chiedono che nel CD CSN siano inclusi i rappresentanti delle infrastrutture critiche e che il testo dell'ordinanza venga modificato di conseguenza.

- *L'aeroporto di ZH* approva il coinvolgimento del settore economico e si candida quale rappresentante.

- *BL* vorrebbe che si precisasse la composizione fisica del CD CSN e che quest'ultimo venisse integrato con rappresentanti dei Comuni e delle infrastrutture critiche.

- *FR* propone una rappresentanza obbligatoria del settore energetico nel CD CSN.

- *GE* propone di aggiungere «civile» a «société» all'articolo 4 capoverso 1 per riflettere meglio l'intenzione di rappresentare gli interessi della cittadinanza.

- *VD* e *SGV* suggeriscono l'aggiunta di rappresentanti comunali nel CD CSN.

- *Migros* propone di comporre il CD CSN in maniera tale che le principali imprese critiche per l'approvvigionamento del Paese con beni e servizi siano rappresentate direttamente e non attraverso le associazioni.

- Le *FFS* criticano il fatto che i dati relativi alle dimensioni e alla composizione del CD CSN siano insufficienti. Chiedono una precisazione di termini generici quali «settore economico», onde garantire un'adeguata rappresentanza dei settori interessati.

- *sgv/usam* chiede una rappresentanza diretta nel CD CSN.

- *UCS* critica la mancata rappresentanza delle città/dei Comuni nel CD CSN.

- *Swico* ritiene che la composizione mista del CD CSN sia efficace e propone l'esplicito coinvolgimento del settore TIC e Internet.

- *swissuniversities* si offre di collaborare alla ricerca di un rappresentante adeguato delle scuole universitarie nel CD CSN e segnala la necessità di chiarire il ruolo di *Switch* in tale contesto.

- *Il Centro* approva la composizione estesa del CD CSN.

❖ **Articolo 4 capoverso 2**

- *Swiss Banking* e *Swiss FS-CSC* propongono di integrare l'articolo 4 capoverso 2 specificando la necessità di esperienze o conoscenze adeguate in ambito ciber: «Nel designare i membri del CD CSN si terrà conto di esperienze o conoscenze adeguate in ambito ciber».

❖ **Articolo 4 capoverso 3**

- *GE* propone di aggiungere «civile» a «société» all'articolo 4 capoversi 1 e 3 per riflettere meglio l'intenzione di rappresentare gli interessi della cittadinanza.

- *Swissgrid* chiede che si citino esplicitamente i gestori di infrastrutture critiche quali possibili candidati alla presidenza.

3.3.2.5 Articolo 5 (Compiti del CD CSN)

Art. 5 Compiti del CD CSN

Il CD CSN ha i seguenti compiti:

a. verificare la CSN almeno ogni cinque anni, contribuire al suo ulteriore sviluppo ed elaborare, se necessario, proposte di adeguamento;

b. elaborare le proposte relative alle priorità e alle tempistiche per l'attuazione delle misure della CSN d'intesa con gli attori indicati nella CSN;

c. valutare costantemente l'attuazione delle misure e informare il Consiglio federale e i Cantoni su eventuali ritardi;

d. presentare se necessario al Consiglio federale proposte per misure complementari;

e. presentare ogni anno al Consiglio federale, ai Cantoni e al pubblico un rapporto sull'attuazione della CSN.

Dieci partecipanti si sono espressi in merito ai compiti del CD CSN. In generale, la maggior parte delle reazioni ha riguardato il capoverso 1 lettera a relativamente all'intervallo di verifica della CSN.

❖ **Proposte e integrazioni generali**

- Sia *SH* che *PNR 77 ETHZ UNIL* chiedono un *ampliamento delle competenze del CD CSN*. *SH* sollecita a introdurre nell'articolo 5 una disposizione d'emergenza affinché il CD CSN non abbia soltanto la facoltà di formulare piani e raccomandazioni, ma anche il potere, in caso d'urgenza, di adottare prontamente le misure del caso. *PNR 77 ETHZ UNIL* raccomanda un ampliamento delle competenze riguardanti la responsabilità in materia di coerenza e attuazione della CSN.

- Alcuni partecipanti chiedono di *migliorare il coordinamento*. *ZG* propone pertanto di introdurre consultazioni periodiche tra il CD CSN e i Cantoni. In tale contesto *PNR 77 ETHZ UNIL* chiede un migliore coordinamento tra gli attori della CSN e un allineamento con altre strategie nazionali.

- Tra le richieste di *PNR 77 ETHZ UNIL* ve ne sono anche alcune riguardanti *aspetti organizzativi*, tra cui il chiarimento dell'organigramma e dello status dell'UFCS nell'ambito dell'articolo 5 e l'eventuale precisazione delle competenze di altri organi.

❖ **Articolo 5 lettera a (intervallo di verifica della CSN)**

- L'*intervallo di verifica* attualmente proposto è stato criticato da numerosi partecipanti alla consultazione perché troppo lungo. *ISSS* e *Il Centro* trovano che cinque anni siano troppi, ma non specificano di quanti anni debba essere ridotto. Le *FFS* chiedono una verifica annuale con un controllo approfondito ogni due anni. *UR* chiede che si effettui una verifica almeno una volta ogni tre anni e *l'aeroporto di ZH* almeno una volta ogni quattro anni.

- Nei pareri sono state formulate anche proposte in merito al *tipo di verifica*. *ISSS*, ad esempio, chiede ulteriori correzioni di rotta in base ai rischi e in funzione degli eventi. *GE* propone di sostituire, all'articolo 5 lettera a, la parola «contrôle» con «audite» per indicare una verifica più dettagliata e precisa.

3.3.2.6 Articolo 6 (Richieste sui titolari)

Art. 6 Richieste sui titolari Per avvisare le autorità, le organizzazioni e le persone interessate in caso di ciberminacce imminenti o di ciberattacchi in corso, l'UFCS può richiedere i dati di contatto dei titolari dei nomi di dominio ai gestori dei registri dei nomi di dominio che rientrano nella competenza della Confederazione o sono subordinati a tali nomi di dominio.

Tre partecipanti si sono espressi a favore di questo articolo e chiedono soltanto alcune modifiche formali:

- *GE* propone una riformulazione per chiarire meglio l'intento e la finalità della richiesta dei dati di contatto dei titolari dei nomi di dominio: «L'OFCS peut, afin d'avertir les autorités, les organisations ou les personnes visées par une cybermenace, imminente ou en cours, requérir les coordonnées des titulaires de noms de domaine auprès du registre des noms de domaine relevant de la compétence de la Confédération».

- *SH* è favorevole al potere attribuito all'UFCS all'articolo 6 di formulare richieste relative ai titolari di domini. Si propone tuttavia di estendere tale potere al blocco di domini criminali anziché soltanto alla diramazione di avvisi.

- *ISSS* segnala che all'UFCS manca la competenza di avanzare richieste sui titolari a valle di un attacco e di richiedere informazioni storiche sui medesimi.

3.3.2.7 Articolo 7 (Analisi tecnica di ciberincidenti e ciberminacce)

Art. 7 Analisi tecnica di ciberincidenti e ciberminacce [1] L'UFCS gestisce il team nazionale di risposta alle emergenze informatiche (Computer Emergency Response Team [CERT]), che svolge in particolare i seguenti compiti: a. gestione tecnica degli incidenti; b. analisi di questioni tecniche; c. identificazione e valutazione di ciberminacce. [2] Per l'analisi dei ciberincidenti e delle ciberminacce l'UFCS gestisce un'infrastruttura resiliente che deve funzionare indipendentemente dal resto dell'informatica della Confederazione.

16 partecipanti alla procedura di consultazione si sono espressi in merito a questa disposizione dell'ordinanza. La maggior parte delle proposte riguarda modifiche testuali o chiarimenti.

❖ **Articolo 7 capoverso 1: analisi tecnica e CERT**

- Per quanto riguarda la *definizione e i compiti del CERT*, *CH++* segnala che, anziché «CERT», si debba utilizzare l'acronimo «CSIRT», trattandosi nel primo caso di un marchio protetto. *UFDC* sollecita a precisare la composizione del CERT nel rapporto esplicativo e propone di sostituire, all'articolo 7 capoverso 1 lettere a e b, l'aggettivo «tecnico» con l'espressione «in materia di cibersicurezza». *ISSS* critica il fatto che l'articolo non stabilisca di chi sia a disposizione il CERT e segnala come le lettere a e b abbiano un focus di tipo tecnico, ma non la lettera c. *ISSS* chiede che venga rivisto l'articolo, integrando la disposizione, e che di norma si pubblichino le analisi effettuate. Infine *Pour Demain* propone di estendere l'articolo 7 capoverso 1 lettera a alla «gestione tecnica degli incidenti, inclusi gli eventi senza coinvolgimento di terzi» e di creare un nuovo articolo 7 capoverso 1 lettera d in cui prevedere il monitoraggio di incidenti correlati all'intelligenza artificiale, ampliando in tal modo l'elenco.

- Per quanto riguarda la *collaborazione e il coordinamento*, *economiesuisse* e *scienceindustries* invocano una precisazione collettiva delle prestazioni e della collaborazione tra UFCS, CERT privati e in-

frastrutture critiche. *Swiss Banking* e *Swiss FC-CSC* ritengono che sia importante garantire una gestione tecnica degli incidenti anche su richiesta di altre autorità e organizzazioni, per cui propongono di integrare l'articolo 7 capoverso 1 lettera a con la seguente proposizione secondaria: «se necessario anche su richiesta di altre autorità e organizzazioni». *CCS* riscontra che non viene esplicitamente citata la collaborazione con le autorità di perseguimento penale e propone di istituzionalizzare i contatti con le medesime all'interno dell'ordinanza. *Switch* chiede di sancire nell'ordinanza lo scambio tra il CERT e i centri di competenza nazionali e internazionali. *swissuniversities* raccomanda di disciplinare nell'ordinanza la collaborazione tra il CERT dell'UFCS, il CERT di Switch e le organizzazioni di cibersicurezza delle scuole universitarie. Da ultimo, *AES* invoca una precisazione collettiva delle prestazioni e della collaborazione tra UFCS, CERT privati e infrastrutture critiche.

- Per quanto riguarda *le risorse e le infrastrutture*, *VS* raccomanda un uso congiunto delle infrastrutture o delle risorse con altre organizzazioni federali.

❖ **Articolo 7 capoverso 2: infrastruttura**

- *CH++* segnala, rispetto all'articolo 7 capoverso 2, che «resiliente» non è un concetto sufficientemente preciso. L'organizzazione propone di fare più chiarezza con una formulazione come «L'esercizio di tale infrastruttura deve poter essere garantita in qualsiasi momento e indipendentemente da terzi». *CH++* solleva inoltre la questione dell'infrastruttura tecnica per le analisi e suggerisce una precisazione relativa all'utilizzo di servizi cloud.

- *L'aeroporto di ZH* approva il fatto che l'infrastruttura dell'UFCS sia indipendente dal resto dell'informatica della Confederazione e propone un livello di protezione elevato.

❖ **Altre osservazioni**

- *eAVS/AI* chiede che nel rapporto esplicativo vi sia una descrizione più comprensibile dell'intervento immediato da parte dell'UFCS.

- *GE* propone di sostituire, nella versione francese dell'articolo 7 capoverso 1, «qui» con «laquelle», onde evitare ambiguità.

- *CCS* suggerisce anche di definire l'oggetto, gli obiettivi d'efficacia e l'entità delle «contromisure», specificando le competenze del CERT necessarie a tal fine.

3.3.2.8 Articolo 8 (Priorizzazione della consulenza e del sostegno in caso di ciberattacchi)

Art. 8 Priorizzazione della consulenza e del sostegno in caso di ciberattacchi
[1] Se la richiesta di consulenza e sostegno in caso di ciberattacco supera le capacità dell'UFCS, questo può stabilire delle priorità per quanto riguarda i tempi e l'entità della consulenza e del sostegno forniti.
[2] A tale riguardo tiene conto della sicurezza e dell'ordine pubblici, del benessere della popolazione e del funzionamento dell'economia.

12 partecipanti alla procedura di consultazione si sono espressi in merito a questa disposizione dell'ordinanza.

❖ **Osservazioni generali in merito all'articolo 8**

- Rispetto *alla collaborazione e alle competenze* disciplinate in questa disposizione, *UFDC* chiede se, in caso di grave crisi, si debba prevedere l'intervento di operatori privati. Eventualmente si potreb-

bero definire i criteri con cui individuare e selezionare a priori tali operatori. *ZH* suggerisce di formalizzare la collaborazione con il Ministero pubblico e la polizia e di coinvolgere le autorità cantonali. In tale contesto *Switch* raccomanda di concretizzare la sussidiarietà dell'UFCS e di sancire la responsabilità personale degli operatori privati. *swissuniversities* propone infine che, in caso di ciberattacco, *Switch* coadiuvi l'UFCS occupandosi delle scuole universitarie.

- Per quanto riguarda *le competenze e le misure* previste da questa disposizione, *ISSS* propone di consentire un supporto esterno al CERT in caso di ciberattacchi, mentre *ZH* suggerisce di definire l'oggetto, gli obiettivi d'efficacia e l'entità delle «contromisure», specificando le competenze del CERT nel testo dell'ordinanza.

- In merito al ruolo dell'UFCS, *eAVS/AI* precisa che l'articolo 8 si applica in materia di priorizzazione quando si tratta di raccogliere ulteriori informazioni in caso di incidente legato alla sicurezza. Le *FFS* sollecitano un chiarimento del rapporto tra segnalazione e richiesta di sostegno. *Swico* approva la consulenza e il sostegno dell'UFCS, ma mette in guardia da una possibile concorrenza statale nei confronti di offerte private in caso di attacchi a bassa priorità.

❖ **Articolo 8 capoverso 1: priorizzazione e criteri**

- Per quanto riguarda la *definizione dei criteri di priorizzazione, digitalswitzerland* chiede un elenco di criteri specifici e una graduatoria degli scenari di danno concreti ai fini della priorizzazione. *GE* propone di integrare i criteri per la gestione delle priorità. Da parte di *UR* si suggerisce di definire le priorità per le imprese e le organizzazioni soggette all'obbligo di segnalazione in base alle loro funzioni, mentre le *FFS* chiedono una chiara priorizzazione in caso di carenze di capacità. *AES*, infine, sollecita una definizione trasparente dei criteri di priorizzazione, basata sull'elenco di infrastrutture critiche dell'Ufficio federale della protezione della popolazione (UFPP).

- Per quanto concerne la *comunicazione delle priorità, GE* propone di formulare un nuovo capoverso 3 che preveda quanto segue: «Il communique alors aux parties concernées les priorités définies».

❖ **Articolo 8 capoverso 2: considerazione degli interessi pubblici**

- In merito all'articolo 8 capoverso 2 *digitalswitzerland* fa notare che un elenco di criteri specifici o una graduatoria degli scenari di danno concreti in base a cui definire le priorità sarebbe un ausilio importante per l'economia digitale.

3.3.2.9 Articolo 9 (Divulgazione coordinata delle vulnerabilità)

Art. 9 Divulgazione coordinata delle vulnerabilità
[1] L'UFCS assicura la divulgazione coordinata delle vulnerabilità secondo gli standard riconosciuti a livello internazionale.
[2] Fissa al produttore dell'hardware o del software interessato un termine di 90 giorni per eliminare le vulnerabilità.
[3] Può accorciare questo termine se una vulnerabilità:

a. mette a rischio il corretto funzionamento di infrastrutture critiche;
b. può essere sfruttata in modo particolarmente semplice per un ciberattacco; o
c. riguarda sistemi molto diffusi.

[4] Può prolungare il termine fissato se eliminare la vulnerabilità si rivela particolarmente complesso.
[5] Può già informare i gestori di infrastrutture critiche prima che le vulnerabilità vengano eliminate o divulgate.
[6] I capoversi da 1 a 4 non si applicano alle vulnerabilità riscontrate dall'Ufficio federale della comunicazione (UFCOM) nell'ambito dei propri controlli di vigilanza (art. 36 segg. dell'ordinanza del 25 novembre 2015 sugli impianti di telecomunicazione). In questi casi l'UFCOM provvede a informare l'UFCS.
[7] L'UFCS informa tempestivamente l'UFCOM in merito alle vulnerabilità riscontrate sugli impianti di telecomunicazione di cui all'articolo 3 lettera d della legge del 30 aprile 1997 sulle telecomunicazioni.

Questo articolo ha dato adito a numerose reazioni. 25 partecipanti alla procedura di consultazione si sono espressi in merito alla divulgazione coordinata delle vulnerabilità.

❖ **Osservazioni generali in merito all'articolo 9**

- Per quanto riguarda *la definizione e la gestione delle vulnerabilità, SH* segnala a titolo generale la necessità di lasciare ai produttori un periodo di tempo sufficiente per eliminare le vulnerabilità prima che esse vengano divulgate. *Swiss Banking*, *Swiss FS-CSC* e le *FFS* chiedono una definizione del termine «vulnerabilità». Le *FFS* chiedono inoltre chiarimenti in merito ai termini per l'eliminazione delle vulnerabilità, alla comunicazione tra l'UFCS e l'Ufficio federale dei trasporti (UFT), alla delimitazione tra l'obbligo di segnalazione dei produttori e quello dei gestori e all'interconnessione tra produttori e gestori.

- Per quanto riguarda *il ruolo e i compiti dell'UFCS, Il Centro* li ritiene adeguati e necessari.

- *PNR 77 ETHZ UNIL* raccomanda di concretizzare nell'ordinanza le conseguenze in caso di mancata eliminazione.

- *SwissICT* esprime *preoccupazioni* in merito all'ulteriore onere per i produttori e ai rischi legati alla riservatezza.

❖ **Articolo 9 capoverso 1: principio della divulgazione coordinata**

- *SP* approva espressamente la regolamentazione, intravedendo un chiaro miglioramento rispetto alla situazione odierna.

- *asut, Salt, digitalswitzerland* e *ZG* propongono di tenere conto, nel testo dell'ordinanza, delle «best practice», oltre che degli standard internazionali. *asut, Salt* e *digitalswitzerland* suggeriscono per l'articolo 9 capoverso 1 la seguente formulazione: «[1] L'UFCS assicura la divulgazione coordinata delle vulnerabilità, successivamente alla loro eliminazione, secondo gli standard riconosciuti a livello internazionale e le best practice». *ZG* chiede inoltre di estendere il campo d'applicazione a gestori e servizi.

- *BE* propone di formulare il capoverso come segue: «[1] L'UFCS assicura la divulgazione coordinata delle vulnerabilità.»

- Con riferimento alle tempistiche di divulgazione, *economiesuisse* e *scienceindustries* propongono che le vulnerabilità vengano divulgate soltanto una volta eliminate.

❖ **Articolo 9 capoverso 2: termine per l'eliminazione delle vulnerabilità**

- Da parte di *digitalswitzerland, asut, Salt, economiesuisse, scienceindustries e Swico* si richiede una *flessibilizzazione del termine*. Nello specifico, *economiesuisse, scienceindustries* e *Swico* chiedono di utilizzare nel testo dell'ordinanza l'espressione «termine adeguato» anziché un termine fisso di 90 giorni; *asut* e *Salt* ritengono tuttavia utile precisare che il termine adeguato dev'essere di almeno 90 giorni.

- Per quanto riguarda la *specifica dei destinatari*, *H+* propone di precisare i produttori dell'hardware o del software di infrastrutture critiche, mentre *SwissICT* chiede di aggiungere i gestori quali soggetti potenzialmente tenuti all'eliminazione delle vulnerabilità.

❖ **Articolo 9 capoverso 3: informazione in caso di ciberminaccia acuta**

- Ai fini di una migliore comprensibilità, *BE* consiglia di formulare l'articolo 9 capoverso 3 come segue: «[3] Qualora sia a conoscenza di una vulnerabilità tale da costituire una ciberminaccia acuta per alcune singole infrastrutture critiche, l'UFCS informa prontamente i relativi gestori, prima che detta vulnerabilità venga pubblicata o eliminata».

❖ **Articolo 9 capoverso4: accorciamento o prolungamento del termine**

- *CH++* propone di formulare l'articolo 9 capoverso 4 in maniera più rigorosa, onde evitare che in troppi casi vi sia un prolungamento dei termini.

- *Swico* suggerisce di consultare il produttore prima di un eventuale accorciamento del termine e chiede di formulare l'articolo 9 capoverso 4 come segue: «Previa consultazione del produttore, [l'UFCS] può accorciare il termine se una vulnerabilità: …».

- *UFDC* fa notare una possibile contraddizione tra «accorciare il termine se la vulnerabilità può essere sfruttata in modo particolarmente semplice» e «prolungare il termine se eliminare la vulnerabilità si rivela particolarmente complesso».

❖ **Articolo 9 capoverso 5: informazione ai gestori di infrastrutture critiche**

- *CH++* sollecita a inasprire la formulazione, così da non suscitare l'impressione che, in situazioni di rischio, il DDPS possa trattenere informazioni sulle lacune in materia di sicurezza per poterle eventualmente sfruttare da sé più a lungo in maniera offensiva. *CH++* propone di modificare la formulazione potestativa dell'articolo 9 capoverso 5: «In linea di principio, informa i gestori di infrastrutture critiche ancor prima che le vulnerabilità vengano eliminate o divulgate».

- Sia *Migros* (informazione immediata) che *l'aeroporto di ZH* (informazione obbligatoria entro 72 ore) richiedono un'informazione più rapida.

- *NEDIK* suggerisce che l'UFCS debba fondamentalmente informare i gestori prima che la vulnerabilità sia eliminata o divulgata, con la possibilità di attendere in determinati casi.

- *UFDC* chiede come ci si comporti in presenza di una vulnerabilità critica, complessa da eliminare, e propone di citare la possibilità di implementare misure di mitigazione transitorie finché la vulnerabilità non sarà stata eliminata.

❖ **Articolo 9 capoversi 6 e 7: coordinamento con l'UFCOM**

- *Sunrise* approva le norme sul coordinamento tra UFCS e UFCOM, ritenendole il giusto approccio per armonizzare e coordinare tra loro le diverse procedure di segnalazione.

- *FER* segnala che armonizzare le procedure dell'UFCOM e dell'UFCS potrebbe risultare complesso (ad es. l'UFCOM deve informare l'UFCS in merito alle vulnerabilità, affinché quest'ultimo possa eventualmente procedere a una loro divulgazione coordinata).

- Il *Partito Pirata Svizzero* propone di stralciare il capoverso 6 o di modificarlo in maniera tale che la divulgazione continui sostanzialmente ad avvenire ai sensi dei capoversi 1-4, ma tenendo conto delle specificità del controllo a cura dell'UFCOM. Il partito lamenta il fatto che non sia sufficiente avere una gestione indefinita delle informazioni relative alle vulnerabilità nelle infrastrutture critiche, per cui chiede una regolamentazione più chiara all'interno dell'ordinanza.

3.3.2.10 Articolo 10 (Sostegno alle autorità)

Art. 10 Sostegno alle autorità L'UFCS fornisce sostegno alle autorità della Confederazione e dei Cantoni nello sviluppo, nell'attuazione e nella verifica degli standard e delle regolamentazioni in materia di cibersicurezza.

Soltanto due partecipanti alla procedura di consultazione si sono espressi in merito a questo articolo, senza respingerlo:

- *UR* solleva la questione del coinvolgimento dei Comuni nel processo globale.

- *swissuniversities* invita a verificare se anche le scuole universitarie non debbano beneficiare di questo sostegno.

3.3.2.11 Articolo 11 (Sistema di comunicazione per lo scambio sicuro delle informazioni)

Art. 11 Sistema di comunicazione per lo scambio sicuro delle informazioni [1] Hanno accesso al sistema di comunicazione dell'UFCS per lo scambio sicuro delle informazioni (art. 74 cpv. 2 lett. a) le organizzazioni e le autorità con sede in Svizzera. [2] L'UFCS è responsabile della sicurezza del sistema di comunicazione e della liceità del trattamento dei dati.

In tutto 13 partecipanti si sono espressi in merito a questa disposizione e ai seguenti tre ambiti tematici.

❖ **Accesso al sistema di comunicazione**

- *PNR 77 ETHZ UNIL* fa notare che non è chiaro se tutte le autorità e le organizzazioni con sede in Svizzera abbiano accesso al sistema di comunicazione dell'UFCS o se siano solo le infrastrutture critiche ad averlo. Consiglia una precisazione nell'ordinanza.

- *Swiss Banking*, S*wiss FS-CSC*, *digitalswitzerland*, *economiesuisse* e *scienceindustries* propongono di estendere l'accesso a tutte le organizzazioni e le autorità soggette all'obbligo di segnalazione, a prescindere dal fatto che abbiano o meno sede in Svizzera. Sostengono che ciò è necessario per

rafforzare la ciberresilienza sulla piazza economica svizzera e che faciliti alle imprese globali lo scambio a livello transfrontaliero.

❖ **Funzionalità e implementazione del sistema di comunicazione**

- *Swico* approva il sistema di comunicazione centrale per lo scambio sicuro delle informazioni, ma segnala la necessità di un elevato standard di sicurezza.

- *BE* chiede che si chiarisca la distinzione tra i sistemi di cui all'articolo 11 e quelli dell'articolo 12, precisando che né dalle norme né dal rapporto esplicativo si evincono chiaramente la delimitazione tra i due sistemi, i differenti criteri di utilizzo e gli scopi.

- *SGV* sottolinea l'importanza di una registrazione semplice e non burocratica per partecipare allo scambio di informazioni e di un accesso non complicato a livello pratico. L'associazione chiede all'UFCS di assicurare la facilità d'accesso nell'attuazione pratica dell'ordinanza.

- Le *FFS* lamentano una mancanza di chiarezza in merito alle responsabilità per il monitoraggio di nuove minacce sulla piattaforma di comunicazione dell'UFCS e in merito ai diritti d'accesso. Chiedono di chiarire tali punti.

❖ **Proposte di ampliamento e precisazione**

- *BE* suggerisce di introdurre un obbligo di registrazione per le organizzazioni e le autorità soggette all'obbligo di segnalazione e per i gestori di infrastrutture critiche sul sistema di comunicazione per lo scambio sicuro delle informazioni e sui sistemi d'informazione per lo scambio automatico.

- *ASA* sottolinea l'importanza di un resoconto dettagliato (anonimizzato) periodico da parte dell'UFCS in merito alle segnalazioni pervenute. Tale rapporto viene ritenuto decisivo per il settore assicurativo al fine di contribuire a incrementare la ciberresilienza dell'economia svizzera e contemporaneamente aumentare la penetrazione del prodotto assicurativo.

- *eAVS/AI* vede la possibilità, con l'introduzione dell'obbligo di segnalazione, che l'UFCS assuma una funzione di interfaccia nell'ottica del principio once-only.

- *Switch* suggerisce di concretizzare in determinati casi la sussidiarietà dell'UFCS e di introdurre un ulteriore capoverso che sancisca il principio della responsabilità personale dei gestori privati in materia di cibersicurezza.

3.3.2.12 Articolo 12 (Sistemi d'informazione per lo scambio automatico)

Art. 12 Sistemi d'informazione per lo scambio automatico
[1] L'UFCS mette a disposizione dei gestori di infrastrutture critiche sistemi d'informazione per lo scambio automatico di informazioni tecniche su ciberminacce e ciberincidenti.
[2] L'UFCS è responsabile della sicurezza dei sistemi d'informazione e della liceità del trattamento dei dati.

Cinque partecipanti alla procedura di consultazione si sono espressi in merito a questa disposizione. Le proposte relative al testo dell'ordinanza riguardano gli aspetti della chiarezza e della precisione, gli standard di sicurezza e la protezione dei dati, l'accesso e l'utilizzo del sistema d'informazione.

❖ **Chiarezza e precisione del testo dell'ordinanza**

- *GL* segnala un'incoerenza terminologica tra il testo dell'ordinanza e le spiegazioni. Mentre nel testo dell'ordinanza si parla solo di «informazioni tecniche», secondo il rapporto esplicativo vengono trattati anche dati personali.

- *SH* nota che rimane poco chiaro come debba avvenire lo scambio di informazioni tra tutti i soggetti interessati. Chiede più precisione nel disciplinare la modalità di scambio delle segnalazioni e delle informazioni.

❖ **Standard di sicurezza e protezione dei dati**

- *L'aeroporto di ZH* propone che l'UFCS miri ai massimi standard di sicurezza e raccomanda di sancirlo esplicitamente nel testo dell'ordinanza.

- Le *FFS* chiedono di fare chiarezza in merito alle modalità consentite per la gestione delle informazioni in ambienti cloud. In particolare le *FFS* domandano quali siano le condizioni che autorizzino al salvataggio delle informazioni in ambienti cloud al di fuori della Svizzera.

❖ **Accesso e utilizzo del sistema d'informazione**

- *swissuniversities* sottolinea che alle scuole universitarie sarebbe molto utile ricevere dall'UFCS o tramite *Switch* informazioni dirette sulle attuali minacce (Threat Intelligence), per cui sottolinea l'importanza dello scambio di informazioni per il settore universitario.

3.3.2.13 Articolo 13 (Registrazione)

Art. 13 Registrazione
[1] Per utilizzare il sistema di comunicazione le organizzazioni e le autorità devono registrarsi. Devono comunicare immediatamente qualsiasi cambiamento nei dati registrati.
[2] La registrazione deve contenere almeno le seguenti informazioni:
a. ragione sociale, nome o designazione nonché indirizzo;
b. dati di contatto della persona registrata.

Otto partecipanti alla procedura di consultazione si sono espressi in merito a questo articolo, che nessuno ha respinto nella forma proposta.

❖ **Articolo 13 capoverso 1: terminologia e processo di registrazione**

- *GE* raccomanda di sostituire, nella versione francese dell'articolo 13 capoerso 1, il termine «enregistrement» con «enrôlement», onde evitare ambiguità. Tale modifica mira a descrivere il processo di registrazione con maggiore precisione.

- *L'aeroporto di ZH* chiede una registrazione obbligatoria per le infrastrutture critiche entro 90 giorni dall'entrata in vigore della legge, ma sottolinea che la partecipazione allo scambio di informazioni deve rimanere facoltativa.

- *swissuniversities* spiega che le scuole universitarie hanno interesse a registrarsi il prima possibile e a rendersi disponibili per un'eventuale pre-registrazione. Propone anche di verificare la possibilità di un coordinamento da parte di *Switch*.

❖ **Articolo 13 capoverso 2: informazioni per la registrazione e dati di contatto**

- *GE* propone di aggiungere, nella versione francese dell'articolo 13, una nuova lettera c al capoverso 2 che specifichi i dati di contatto dell'unità competente in materia di cibersicurezza all'interno dell'organizzazione o autorità.

- *SH* propone che, in caso di segnalazioni critiche, le informazioni non vengano indirizzate a un'unica persona. Per garantire la continuità della catena d'informazione, suggerisce di consentire la registrazione a più persone. Anche *l'aeroporto di ZH, digitalswitzerland* e *Swico* sono del medesimo avviso e propongono di utilizzare, all'articolo 13 capoverso 2 lettera b, anziché «dati di contatto della persona registrata» la frase «dati di una o più persone di contatto».

- *economiesuisse* e *scienceindustries* chiedono che venga cancellato l'articolo 13 capoverso. 2 o quanto meno adattato l'articolo 13 capoverso 2 lettera b, ritenendo che i dati richiesti siano troppo dettagliati e formalistici.

3.3.2.14 Articolo 14 (Fornitori di servizi)

Art. 14 Fornitori di servizi
[1] I gestori di infrastrutture critiche possono notificare all'UFCS eventuali fornitori di servizi che vogliono partecipare allo scambio di informazioni.
[2] I fornitori di servizi devono registrarsi indicando la ragione sociale o il nome come pure i dati di contatto della persona registrata.

Sei partecipanti alla procedura di consultazione si sono espressi in merito a questo articolo. Dai pareri emerge un consenso di fondo nei confronti dell'articolo, unito a richieste di precisazioni e suggerimenti di integrazioni.

❖ **Articolo 14 capoverso 1: definizione e ambito d'azione dei fornitori di servizi**

- *FR* suggerisce di utilizzare nella versione francese l'espressione «fournisseurs de prestations de cybersécurité» (fornitori di servizi di cibersicurezza), onde evitare confusioni. Questa proposta mira a definire più chiaramente l'ambito d'azione dei fornitori di servizi in questione.

- *GE* propone di precisare, nel testo dell'ordinanza, che l'UFCS verifichi l'adesione dei fornitori di servizi. Questa proposta tiene conto della sensibilità dei dati oggetto di scambio e mira a incrementare la sicurezza dello scambio di informazioni.

- *VS* chiede di precisare se l'articolo si riferisca a tutti i fornitori di servizi informatici o soltanto a quelli legati alla cibersicurezza.

- *Swiss Banking* e *Swiss FS-CSC* propongono di precisare l'articolo, specificando che i gestori di infrastrutture critiche possono notificare all'UFCS eventuali fornitori che erogano loro servizi nell'ambito della propria attività e che pertanto vogliono partecipare allo scambio di informazioni. Propongono di precisare l'articolo 14 capoverso 1 come segue: «I gestori di infrastrutture critiche possono notificare all'UFCS eventuali fornitori che erogano loro servizi nell'ambito della propria attività (ad es. nell'ambito di un outsourcing) e che pertanto vogliono partecipare insieme a loro allo scambio di informazioni.», motivando tale precisazione con la prassi corrente per cui tali fornitori di servizi sono già autorizzati a partecipare allo scambio di informazioni se soddisfano i requisiti dell'UFCS.

- *Swico* accoglie favorevolmente il fatto che i fornitori di servizi dei gestori di infrastrutture critiche possano avere accesso, su base volontaria, ai suddetti sistemi d'informazione. L'associazione ritiene

che la notifica prevista da parte dei gestori e la successiva iscrizione a cura del fornitore di servizi sia una procedura sensata.

❖ **Articolo 14 capoverso 2: registrazione dei fornitori di servizi**

- *Swico* propone di sostituire, all'articolo 14 capoverso 2, la formulazione «dati di contatto della persona registrata» con ««dati di una o più persone di contatto»: «[2] I fornitori di servizi devono registrarsi indicando la ragione sociale o il nome come pure i ~~dati di contatto della persona registrata~~ dati di una o più persone di contatto.» L'associazione sostiene che l'attuale formulazione potrebbe implicare una responsabilità in capo alla persona notificante, cosa che si dovrebbe evitare.

3.3.2.15 Articolo 15 (Trasmissione e utilizzo delle informazioni)

Art. 15 Trasmissione e utilizzo delle informazioni
[1] Le aziende e le autorità registrate trasmettono informazioni all'UFCS e stabiliscono se e a chi l'UFCS può a sua volta trasmettere le informazioni, qualora la trasmissione delle informazioni non fosse contemplata dalla legge.
[2] L'UFCS decide in merito alla pubblicazione delle informazioni autorizzate alla trasmissione sul sistema di comunicazione come pure sui sistemi d'informazione per lo scambio automatico.
[3] I destinatari delle informazioni devono garantire la protezione delle informazioni.
[4] I fornitori di servizi di gestori di infrastrutture critiche possono utilizzare le informazioni che ricevono esclusivamente per la protezione delle infrastrutture critiche.

In tutto 12 partecipanti alla procedura di consultazione hanno commentato l'aspetto della trasmissione e dell'utilizzo delle informazioni. Nessuno ha respinto l'articolo 15. I pareri contengono prevalentemente proposte di precisazione, ampliamento o adeguamento dell'articolo.

❖ **Osservazioni generali in merito all'articolo 15**

- *SH* si aspetta che le segnalazioni non vengano solo filtrate, ma anche categorizzate da parte di un team di supporto specializzato. Si propone di istituire un'autorità federale centrale che possieda conoscenze tecniche esplicite in materia e presti consulenza a livello nazionale.

- *Swissgrid* chiede quali siano le conseguenze in caso di mancato rispetto della classificazione TLP e come ci si debba comportare se il fornitore delle informazioni non definisce la cerchia dei destinatari. Sollecita le opportune integrazioni all'ordinanza o alle spiegazioni.

- *PNR 77 ETHZ UNIL* propone di precisare la disposizione, specificando che in fase di trasmissione delle informazioni le aziende e le autorità debbano indicare se e a quali delle categorie di destinatari previste dal protocollo TLP le si debba inoltrare. Indica un potenziale conflitto tra il capoverso 1 e il capoverso 2 dell'articolo 15 e suggerisce di apportare un chiarimento nell'ordinanza. Andrebbe inoltre stabilito che l'UFCS può pubblicare informazioni soltanto se necessario al fine di proteggere le infrastrutture critiche o la Svizzera dalle ciberminacce.

❖ **Articolo 15 capoverso 1: trasmissione di informazioni**

- *L'aeroporto di ZH* propone di consentire alle aziende e alle autorità registrate di stabilire quali informazioni trasmettere e a chi.

- *GR* suggerisce di prevedere la possibilità, in fase di trasmissione, di stabilire quali informazioni poter diffondere, dal momento che alcune devono essere condivise rapidamente, mentre altre – per motivi tattici – solo più tardi.

- *NEDIK* fa notare che la segnalazione può essere gestita dallo stesso segnalante e che vi sono varie classificazioni possibili. Sottolinea l'importanza di una corretta classificazione e del fatto che i segnalanti devono poter limitare o estendere la trasmissione di informazioni a determinati dati.

- *Swico* sottolinea l'importanza del fatto che sia l'organizzazione o l'autorità mittente a determinare se e a chi trasmettere le informazioni segnalate, tenendo conto della sensibilità delle informazioni e del rapporto di fiducia necessario.

❖ **Articolo 15 capoverso 2: pubblicazione e trasmissione di informazioni**

- *BA* propone di citare esplicitamente il salvataggio delle informazioni da parte dell'UFCS al fine di consentire una loro eventuale successiva trasmissione alle autorità di perseguimento penale.

- *Swiss Banking* e *Swiss FS-CSC* chiedono una concretizzazione delle modalità di trasmissione delle segnalazioni all'UFCS. Propongono che, in caso di segnalazioni collettive a più autorità, ciascuna di esse possa leggere soltanto la parte a lei destinata. Per garantirlo, si propone di integrare due capoversi nell'articolo 15 del progetto di ordinanza sulla cibersicurezza. Il primo capoverso dovrebbe recitare come segue: «^{1bis} Il sistema messo a disposizione dall'UFCS per la trasmissione delle segnalazioni è configurato in maniera tale che tutte le autorità aderenti possano leggere ed elaborare soltanto i contenuti destinati loro dall'organizzazione segnalante.», mentre il secondo nuovo capoverso proposto dovrebbe contenere il seguente testo: «^{1ter} Per quanto riguarda i contenuti delle segnalazioni condivisi con l'UFCS attraverso questo canale, spetta all'UFCS decidere in merito alla pubblicazione... [continuazione secondo art. 15 cpv. 2]».

- *CCS* sollecita a circoscrivere la competenza dell'UFCS in materia di trasmissione delle informazioni in maniera tale che sia garantito un inoltro completo delle informazioni alle autorità di perseguimento penale.

- *ZH* suggerisce di imporre all'UFCS l'obbligo di inoltrare eventuali segnalazioni di ciberattacchi alle autorità di perseguimento penale competenti ai fini di una valutazione penale. Si propone di definire con maggiore precisione nell'ordinanza come gestire eventuali informazioni di rilevanza penale.

❖ **Articolo 15 capoversi 3 e 4: protezione e utilizzo delle informazioni**

- *VS* ritiene che l'articolo 15 capoverso 4 sia troppo restrittivo e propone di consentire ai fornitori di servizi l'utilizzo delle informazioni relative alle vulnerabilità, così da tutelare meglio altri clienti.

- *NEDIK* segnala che le autorità di perseguimento penale sono tenute per legge ad avviare un'inchiesta, se a conoscenza di reati perseguibili d'ufficio. Chiede che l'UFCS assicuri che, nelle informazioni pubblicate, il gestore delle infrastrutture critiche in questione non sia identificabile.

- *Swico* approva l'obbligo di protezione delle informazioni da parte del destinatario e il loro esclusivo utilizzo ai fini della tutela delle infrastrutture critiche, in maniera tale da scongiurare vantaggi competitivi sleali.

3.3.2.16 Articolo 16 (Eccezioni all'obbligo di segnalazione)

Art. 16 Eccezioni all'obbligo di segnalazione

[1] Le seguenti autorità e organizzazioni sono esentate dall'obbligo di segnalazione alle seguenti condizioni:

a. gli organi di cui all'articolo 74*b* capoverso 1 lettere b e c LSIn: se sono responsabili di meno di 1000 abitanti; è determinante la popolazione stabilmente risiedente;

b. le imprese di cui all'articolo 74*b* capoverso 1 lettera d LSIn, a condizione che:

   1. in qualità di gestori di rete, produttori di energia elettrica, gestori di impianti elettrici di stoccaggio o di fornitori di servizi nell'ambito dell'elettricità secondo l'articolo 5*a* capoverso 1 e l'allegato 1*a* dell'ordinanza del 14 marzo 2008 sull'approvvigionamento elettrico (OAEl) non siano tenute a rispettare né il livello di protezione A né il livello di protezione B,

   2. in qualità di esercenti di gasdotti secondo l'articolo 2 capoverso 3 dell'ordinanza del 4 giugno 2021 sulla sicurezza degli impianti di trasporto in condotta (OSITC) presentino negli ultimi cinque anni una media di energia trasportata inferiore a 400 GWh all'anno;

c. le imprese di cui all'articolo 74*b* capoverso 1 lettera n LSIn, a condizione che:

   1. non debbano realizzare alcun sistema di gestione della sicurezza delle informazioni secondo gli articoli 2 e 4 e l'allegato II del regolamento (UE) 2023/203 oppure secondo l'articolo 2 e l'allegato del regolamento (UE) 2022/1645,

   2. non debbano applicare le direttive di cui al punto 1.7 dell'allegato del regolamento di esecuzione (UE) 2015/1998 nel loro programma di sicurezza secondo gli articoli 2, 12, 13 o 14 del regolamento (CE) 300/2008;

d. le imprese ferroviarie come pure le imprese che gestiscono impianti di trasporto a fune, linee filoviarie, autobus e battelli di cui all'articolo 74*b* capoverso 1 lettera m LSIn, a condizione che:

   1. non siano incaricate di assumere compiti sistemici (art. 37 della legge federale del 20 dicembre 1957 sulle ferrovie [Lferr]),

   2. siano titolari di una concessione per il trasporto di viaggiatori secondo l'articolo 6 legge del 20 marzo 2009 sul trasporto di viaggiatori (LTV), ma non forniscono alcuna offerta di trasporto ordinata congiuntamente dalla Confederazione e dai Cantoni (art. 28–31*c* LTV),

   3. dispongano di una concessione d'infrastruttura di cui all'articolo 5 Lferr che però non è stata rilasciata poiché sussiste un interesse pubblico alla costruzione e all'esercizio dell'infrastruttura (art. 6 cpv. 1 lett. a Lferr);

e. i fornitori e i gestori di servizi di cui all'articolo 74*b* capoverso 1 lettera t LSIn, a condizione che abbiano sede in Svizzera e che non forniscano le loro prestazioni in parte o interamente dietro compenso a favore di terzi.

[2] Le imprese di cui all'articolo 74*b* capoverso 1 lettere f, g, h, l e p LSIn, alle quali il capoverso 1 non è applicabile, sono esentate dall'obbligo di segnalazione se nel settore interessato occupano meno di 50 persone e se la loro cifra d'affari annua o il loro totale di bilancio annuo non supera i 10 milioni di franchi.

In tutto 24 partecipanti alla procedura di consultazione si sono espressi in merito a questa disposizione. Nessuno di essi l'ha respinta, ma sono state comunque avanzate critiche e proposte di modifica o integrazione.

❖ **Articolo 16 capoverso 1: eccezioni generali all'obbligo di segnalazione**

– *AG, SZ, VD e SwissICT* criticano l'*eccezione per i Comuni* con meno di 1000 abitanti, dal momento che questi ultimi potrebbero essere più esposti ai ciberattacchi a causa delle minori risorse a disposizione, sono connessi alla rete cantonale e i ciberattacchi potrebbero avere ripercussioni negative sulla relativa infrastruttura, sono in genere i più vulnerabili e la loro esenzione trasmetterebbe un segnale sbagliato, ma anche perché le istituzioni minori rivestono un ruolo importante per l'individuazione tempestiva dei ciberattacchi. Di diverso parere è *SGV*, che approva l'eccezione per i Comuni con meno di 1000 abitanti, ma sottolinea l'importanza delle segnalazioni volontarie e dell'assistenza tecnica per tutti i Comuni.

- Per quanto riguarda le *eccezioni per le scuole universitarie e altre istituzioni, Switch* propone di esentare, in determinati casi, scuole universitarie e registrar dall'obbligo di segnalazione, essendo un obbligo di segnalazione completo sproporzionato per tali categorie. *swissuniversities* suggerisce per le scuole universitarie l'introduzione di valori soglia basati su diversi criteri, quali dimensioni, infrastrutture e sistemi di ricerca.

- *Swiss Banking e Swiss FS-CSC* propongono di esentare dall'obbligo di segnalazione i ciberattacchi aventi effetti soltanto minimi sull'attività degli istituti finanziari. Lo si potrebbe formulare come capoverso 1 lettera d^{bis} nella maniera seguente: «d^{bis} le imprese di cui all'articolo 74*b* capoverso 1 lettera e LSIn, a condizione che i ciberattacchi abbiano effetti soltanto minimi sull'attività dell'impresa, in particolare che non siano attacchi andati interamente o parzialmente a buon fine ai danni di funzioni critiche che, se bloccate o perturbate, comprometterebbero fortemente la protezione dei clienti o il funzionamento dei mercati. Questa disposizione può essere concretizzata con un'ordinanza della FINMA o un'autoregolamentazione delle associazioni di competenza».

- Le *FFS* chiedono di rivedere le eccezioni previste per le imprese ferroviarie minori, gli esercenti di gasdotti e le centrali elettriche, essendo anch'essi potenzialmente esposti ad attacchi rilevanti per la sicurezza.

- *CH++* e *H+* sostengono che gli ospedali dovrebbero essere soggetti all'obbligo di segnalazione a prescindere dalle loro dimensioni.

- *ASIP* chiede di estendere l'esenzione dall'obbligo di segnalazione a tutti gli istituti di previdenza registrati e non registrati (con e senza prestazioni regolamentari) aventi fino a 30 000 assicurati. *ASIP* sostiene che la responsabilità in materia di cibersicurezza deve essere di competenza dell'organo supremo dell'istituto di previdenza e che non debba essere inutilmente limitata da disposizioni di legge.

- *Swissgrid* chiede di includere anche i fornitori di servizi che si occupano dei sistemi di misurazione e gestione intelligenti, purché soddisfino determinati valori limite.

❖ **Articolo 16 capoverso 2: eccezioni per piccole strutture**

- *UFDC* mette in dubbio l'adeguatezza dell'espressione «piccole strutture» per l'esonero dall'obbligo di segnalazione e invita a considerare altri criteri, come le dimensioni dei clienti interessanti.

- *economiesuisse, scienceindustries* e *Swico* propongono di esentare dall'obbligo di segnalazione le imprese e altre organizzazioni di diritto privato aventi meno di 250 collaboratori. Per l'articolo 16 capoverso 2 dell'ordinanza viene proposto il seguente testo: «[2] Le imprese di cui all'articolo 74*b* capoverso 1 lettere f, g, h, l e p LSIn ~~alle quali il capoverso 1 non è applicabile~~ sono esentate dall'obbligo di segnalazione se ~~nel settore interessato occupano meno di 50 persone e se la loro cifra d'affari annua o il loro totale di bilancio annuo non supera i 10 milioni di franchi~~ al 1° gennaio dell'anno impiegano meno di 250 collaboratori.»

- *SwissICT* suggerisce di eliminare le eccezioni basate sul numero di collaboratori e sulla cifra d'affari di un'impresa, dal momento che potrebbero pregiudicare il senso e lo scopo dell'obbligo di segnalazione.

❖ **Altre proposte e osservazioni**

- *UCS* chiede se sia prevista un'integrazione delle «condizioni generali per le prestazioni TIC» e fa notare che il rapporto esplicativo non è molto chiaro relativamente a questo articolo.

- *BE* propone una precisazione della frase introduttiva, così da distinguere tra gestori di infrastrutture critiche, da un lato, e autorità e organizzazioni, dall'altro: «Alle condizioni sotto indicate, sono esclusi dall'obbligo di segnalazione le autorità, le organizzazioni e i gestori di infrastrutture critiche seguenti: ...»

- *GE* fa notare che all'articolo 16 capoverso 1 lettera b non è chiaro se le due condizioni siano cumulative o alternative.

- *GR* raccomanda di tenere conto, nel definire la dimensione delle istituzioni, del rischio di diffusione a cascata di un eventuale incidente relativo ai dati.

- *SO* ritiene che le eccezioni previste all'obbligo di segnalazione siano coerenti e comprensibili.

- *VS* propone di invertire la sequenza delle lettere c e d all'articolo 16 capoverso 1, in maniera tale da seguire lo stesso ordine della LSIn.

- *Swiss Banking e Swiss FS-CSC* propongono di evitare rimandi diretti a legislazioni UE (cfr. in merito art. 16 cpv. 1 lett. c n. 1 e 2 della bozza di ordinanza sulla cibersicurezza) che, essendo spesso oggetto di emendamenti, renderebbero inutili tali riferimenti, con conseguente incertezza giuridica.

- *CH++* lamenta l'assenza di una regolamentazione sulla gestione dei rischi cumulativi.

3.3.2.17 Articolo 17 (Obbligo di documentazione delle richieste di informazioni sull'assoggettamento all'obbligo di segnalazione)

Art. 17 Obbligo di documentazione delle richieste di informazioni sull'assoggettamento all'obbligo di segnalazione
Le autorità e le organizzazioni interessate devono mettere a disposizione dell'UFCS tutti i documenti necessari per fornire informazioni in merito all'assoggettamento all'obbligo di segnalazione.

Un partecipante alla procedura di consultazione si è espresso in merito a questa disposizione, criticando la poca precisione con cui è formulato l'articolo 17.

- *PNR 77 ETHZ UNIL* critica la formulazione poco chiara del titolo della disposizione, quanto meno nella versione francese. Propone di utilizzare espressioni alternative, quali «Obligation de mettre à disposition des informations», «Obligation de collaborer» o «Obligation d'information».

3.3.2.18 Articolo 18 (Ciberattacchi da segnalare)

Art. 18 Ciberattacchi da segnalare

[1] Il funzionamento di un'infrastruttura critica è considerato compromesso se:

a. i collaboratori o i terzi sono interessati da interruzioni del sistema; o

b. l'organizzazione o l'autorità interessata può mantenere le proprie attività soltanto con l'aiuto di piani d'emergenza.

[2] Vi è una manipolazione o una fuga di informazioni se:

a. informazioni rilevanti per le attività aziendali vengono modificate o divulgate da persone non autorizzate; o

b. si è verificata una violazione della sicurezza dei dati secondo l'articolo 24 della legge federale del 25 settembre 2020 sulla protezione dei dati (LPD).

[3] Un ciberattacco è considerato non identificato per un periodo prolungato se l'incidente si è verificato più di 90 giorni prima.

[4] Un ciberattacco è considerato connesso ai reati di estorsione, minaccia o coazione se suddetti reati sono rivolti contro le autorità o le organizzazioni assoggettate all'obbligo di segnalazione, o contro i loro responsabili o i loro collaboratori, compresi gli ex responsabili o gli ex collaboratori, oppure contro persone che lavorano per le autorità o le organizzazioni assoggettate all'obbligo di segnalazione.

33 partecipanti alla procedura di consultazione si sono espressi in merito ai ciberattacchi da segnalare. Nessuno ha respinto l'articolo 18, i pareri contengono prevalentemente proposte di precisazione, ampliamento o adeguamento dell'articolo.

❖ **Articolo 18 capoverso 1: definizione di attacchi soggetti ad obbligo di segnalazione**

- Numerosi partecipanti hanno chiesto di *precisare l'obbligo di segnalazione*:
  - *asut e Salt* propongono di limitare l'obbligo di segnalazione agli incidenti che hanno ripercussioni dirette sull'esercizio dell'infrastruttura critica.
  - *L'aeroporto di ZH* chiede che si debbano segnalare soltanto i ciberattacchi con conseguenze funzionali andati a buon fine.
  - *economiesuisse e scienceindustries* sottolineano che si dovrebbero segnalare soltanto gli attacchi con conseguenze funzionali andati a buon fine.
  - In merito all'articolo 18 capoverso 1 lettera a *BL* fa notare la necessità di precisare «interruzioni del sistema», visto che un'interruzione al sistema di contabilità dovuta all'utilizzo dell'IA, ad esempio, non ha praticamente alcuna ripercussione sulla competenza chiave del sistema.
  - *H+* sostiene che la formulazione è troppo generica e dovrebbe essere meglio specificata.
  - *GR* chiede di definire con maggiore precisione l'istante di inizio di un ciberattacco e di citare espressamente i principali segnali di un attacco preparatorio.
  - *SGV* chiede precisazioni in merito alla definizione di ciberattacchi soggetti a obbligo di segnalazione.
  - Le *FFS* criticano le formulazioni troppo ampie e generiche e chiedono di precisare e circoscrivere i concetti.
  - *ASA* sostiene che devono essere segnalate soltanto le interruzioni del sistema provocate intenzionalmente.
  - *Swico* propone alcune precisazioni per chiarire che si deve trattare di eventi che compromettano direttamente l'esercizio dell'infrastruttura.
  - *SwissICT* critica la definizione di compromissione della funzionalità perché troppo articolata e suggerisce una ponderazione.
  - *Migros* sostiene che non tutte le interruzioni di sistema compromettono la funzionalità di un'infrastruttura critica e propone di considerare come soggette a obbligo di segnalazione soltanto le interruzioni di un «sistema critico per l'operatività aziendale».

- Alcuni partecipanti alla procedura di consultazione chiedono che *si tenga conto della gravità*. *digitalswitzerland*, *SUVA* e *La Posta Svizzera SA*, ad esempio, suggeriscono di considerare nell'obbligo di segnalazione la gravità di un ciberattacco, così da evitare inutili incombenze amministrative.

- Da alcuni partecipanti viene chiesto anche di *specificare vari concetti:*

  - *NEDIK* sostiene che l'ordinanza dovrebbe definire e circoscrivere con maggiore precisione cosa si intenda per «guasto al sistema».

  - *GE* propone di precisare nel rapporto esplicativo cosa si intenda per «part importante».

  - *GL* raccomanda di indicare più chiaramente nel rapporto esplicativo che all'UFCS vanno segnalate soltanto le interruzioni del sistema correlate a un ciberattacco.

❖ **Articolo 18 capoverso 2: manipolazione o fuga di informazioni**

- *UFDC* segnala che una fuga di informazioni può essere individuata prima che queste ultime vengano pubblicate da persone non autorizzate.

- *PNR 77 ETHZ UNIL* critica il fatto che il rimando alla LPD non sia ideale, dal momento che tale legge prevede obblighi di segnalazione anche per violazioni non intenzionali della protezione dei dati.

- In merito all'articolo 18 capoverso 1 lettera a *ASA* sostiene che si devono segnalare soltanto le interruzioni di sistema provocate intenzionalmente e che all'articolo 18 capoverso 2 va aggiunto quanto segue: vi è una manipolazione o una fuga d'informazioni se informazioni rilevanti per le attività aziendali vengono modificate o divulgate da persone non autorizzate e quindi «sottratte, distrutte, disattivate o trattate in altro modo da ripercuotersi a medio o lungo termine su applicazioni o sistemi fondamentali». L'articolo 18 capoverso 2 lettera c, inoltre, dev'essere integrato con l'aggiunta di un'ultima porzione di frase: «che si presume comporti un rischio elevato per la personalità o i diritti fondamentali della persona interessata».

- Per coerenza, *Swiss Banking* e *Swiss FS-CSC* propongono di precisare le formulazioni al fine di restringere il campo d'interesse ai ciberattacchi e tralasciare altri aspetti come la protezione dei dati.

❖ **Articolo 18 capoverso 3: termine di 90 giorni**

- *ZH* suggerisce che sarebbe auspicabile una regolamentazione di base che specifichi quali dati di log possono essere conservati e per quanto tempo.

❖ **Articolo 18 capoverso 4: obbligo di segnalazione in caso di estorsione, minaccia o coazione**

- *BE* propone di ampliare l'obbligo di segnalazione in caso di estorsione, minaccia o coazione direttamente agli ex responsabili o collaboratori dell'ente assoggettato all'obbligo di segnalazione oppure di omettere del tutto questo gruppo di persone.

- Le *FFS* chiedono di limitare la portata dell'articolo 18 capoverso 4 sancendo l'obbligo di segnalazione soltanto per i ciberattacchi credibili e penalmente rilevanti.

❖ **Altre osservazioni sull'articolo 18**

- *BA* è favorevole al fatto che l'UFCS segnali automaticamente alle autorità di perseguimento penale i ciberattacchi che potrebbero rappresentare un reato.

- *ISSS* critica il fatto che i vari capoversi non contengano espressioni quali «in particolare» o formulazioni analoghe indicanti che si tratta di un elenco non esaustivo.

- *Il Centro* riscontra come la cerchia di destinatari debba essere sufficientemente ampia affinché l'obbligo di segnalazione possa avere piena efficacia.

- *SH* critica il fatto che l'art. 18 sia troppo breve e che l'obbligo di segnalazione stesso non venga citato esplicitamente.

- *UR* sostiene che i Comuni più piccoli per numero di abitanti, accorpati in uno dei due raggruppamenti dei centri di calcolo, non dovrebbero essere sollevati dall'obbligo di segnalazione.

- *CCS* propone di aggiungere un nuovo capoverso 5 che imponga all'UFCS l'obbligo di denunciare alle autorità di perseguimento penale competenti almeno i casi di cui al capoverso 4.

- *swissuniversities* precisa che le segnalazioni delle scuole universitarie all'attenzione dell'UFCS devono essere coordinate con il CERT di Switch.

3.3.2.19 Articolo 19 (Contenuto della segnalazione)

Art. 19 Contenuto della segnalazione

[1] La segnalazione deve contenere le seguenti informazioni sul ciberattacco:

a. data e ora in cui è stato rilevato l'attacco;
b. data e ora in cui è stato compiuto l'attacco;
c. tipo di attacco;
d. metodo di attacco; e
e. indicazioni sull'autore.

[2] Deve inoltre contenere informazioni che indichino se l'attacco era connesso ai reati di estorsione, minaccia o coazione e se è stata sporta una denuncia penale.

[3] Deve contenere le seguenti informazioni sulle ripercussioni del ciberattacco:

a. unità dell'organizzazione o dell'autorità interessate;
b. grado di compromissione della disponibilità, dell'integrità e della confidenzialità delle proprie informazioni e delle informazioni di terzi; e
c. ripercussioni del ciberattacco sul funzionamento delle unità dell'organizzazione o dell'autorità interessate.

[4] Se la segnalazione non viene effettuata tramite il sistema di comunicazione dell'UFCS, deve contenere anche le seguenti informazioni sull'autorità o sull'organizzazione assoggettata all'obbligo di segnalazione:

a. ragione sociale, nome o designazione nonché indirizzo; e
b. dati di contatto della persona che effettua la segnalazione.

30 partecipanti alla consultazione si sono espressi sul contenuto della segnalazione e nessuno ha respinto completamente questa disposizione.

❖ **Articolo 19 capoverso 1: contenuto della segnalazione**

- Numerosi partecipanti alla consultazione hanno chiesto di introdurre nell'ordinanza precisazioni in merito *all'entità e al tipo delle informazioni da segnalare*:

  - *BE* e *PNR 77, PFZ* e *UNIL* propongono di sostituire «indicazioni sull'autore» con «indicazioni sull'aggressore»;

  - *GE* raccomanda di aggiungere nell'articolo 19 capoverso 1 lettera e, «lorsqu'elles sont disponibles» (qualora disponibili) alla fine del capoverso;

  - *ZH* raccomanda di integrare il contenuto della segnalazione con «involvierte Dienstleister oder andere Dritte» (fornitori di servizi coinvolti o altri terzi) per tenere conto degli attacchi alla catena di fornitura e consentire all'UFCS di valutare in modo adeguato la situazione di minaccia nazionale;

  - *Migros* propone di unire le lettere «tipo di attacco» e «metodo di attacco»;

  - *AES* propone di aggiungere «angegriffene Systeme» (sistemi attaccati) all'elenco delle informazioni da segnalare;

  - il *PLR* critica l'elenco dettagliato delle informazioni, ritenendolo troppo ampio e difficile da comprendere;

  - *Swiss Banking* e *Swiss FS-CSC* raccomandano di integrare l'articolo per rendere più flessibili i requisiti relativi al contenuto della segnalazione e basarli sulle conoscenze che, ragionevolmente, possono essere disponibili;

  - *La Posta Svizzera SA* e *digitalswitzerland* considerano problematiche le indicazioni sull'autore del ciberattacco e propongono di richiederle solo se possono essere determinate senza onerose procedure forensi;

  - *NEDIK* sottolinea che nella segnalazione manca la classificazione per la trasmissione dell'informazione e raccomanda di stabilirla in modo chiaro sin dall'inizio;

  - *Primeo* propone di aggiungere come ulteriore punto relativo all'obbligo di segnalazione l'indicazione dell'ambito OT (tecnologia operativa) colpito dall'attacco;

  - *Swissgrid* propone che le indicazioni sull'autore vengano richieste solo se note («sofern bekannt») e che nella segnalazione siano incluse anche informazioni sui sistemi attaccati.

- In merito agli aspetti della *protezione dei dati* e dei *dati personali,* l'*asut, Salt, Switch* e *Sunrise* osservano che la segnalazione può includere anche dati personali e raccomandano di definire le procedure in modo tale che sia obbligatorio trasmettere i dati personali solo in caso di incidenti accertati.

❖ **Articolo 19 capoverso 2: ulteriori informazioni**

- *GE* propone una nuova formulazione per facilitare la comprensione: «…des informations sur l'éventualité ou la réalité d'un chantage, ainsi que d'une dénonciation pénale» (informazioni sull'eventualità o sull'effettiva esistenza di un'estorsione, nonché di una denuncia penale).

- *NEDIK* afferma che la segnalazione dovrebbe contenere anche l'indicazione dell'autorità presso cui è stata sporta una denuncia penale.

- SwissICT raccomanda di stralciare senza sostituzione l'articolo 19 capoverso 2 OCS, o di richiedere su base facoltativa tali informazioni nel modulo di segnalazione.

❖ **Articolo 19 capoverso 3: ripercussioni del ciberattacco**

- *UCS* chiede quale sia la differenza tra «elevata» e «grave» nel rapporto esplicativo e propone formulazioni alternative.

- L'*aeroporto di Zurigo* propone di includere nel contenuto della segnalazione la funzione dele unità interessate.

- *Swiss Banking* e *Swiss FS-CSC* propongono di definire il grado di gravità dell'attacco in modo generico come leggero, medio o grave.

- *economiesuisse* e *scienceindustries* chiedono di stralciare l'articolo 19 capoverso 3 poiché ritengono che vada oltre le disposizioni legali e sia troppo rigido.

- *AES* afferma, in merito all'articolo 19 capoverso 3, che quest'ultimo si riferisce alle «unità dell'organizzazione o dell'autorità interessate» e che, pertanto, la segnalazione di cui all'articolo 19 capoverso deve contenere anche l'indicazione dei sistemi attaccati («angegriffene Systeme»).

- *Migros* raccomanda a sua volta di stralciare questo capoverso, poiché in caso di evento reale le informazioni rilevanti dipendono fortemente dal contesto.

❖ **Articolo 19 capoverso 4: canale di segnalazione**

- L'*aeroporto di Zurigo* propone che, per le organizzazioni assoggettate all'obbligo di segnalazione, quest'ultima debba avvenire esclusivamente tramite il sistema di comunicazione dell'UFCS e che anche le imprese non assoggettate all'obbligo di segnalazione possano segnalare un ciberattacco all'UFCS.

- *GE* raccomanda di aggiungere nel capoverso 4 una lettera c relativa all'indicazione dei dati di contatto dell'unità competente per la cibersicurezza in seno all'organizzazione o all'autorità.

❖ **Osservazioni generali sull'articolo 19**

- *LU* raccomanda di introdurre categorie di segnalazione in base alle ripercussioni dell'evento: incidente minore (nessuna segnalazione o segnalazione facoltativa), incidente medio (segnalazione obbligatoria entro una settimana) e incidente grave (segnalazione obbligatoria entro 24 ore). L'obiettivo è garantire che vengano segnalati all'UFCS solo gli incidenti rilevanti.

- *VS* propone di centralizzare le segnalazioni di ciberattacchi indirizzate all'UFCS per evitare segnalazioni multiple a diversi servizi federali.

- *FER* osserva che la valutazione delle conseguenze dei ciberattacchi può essere soggettiva e variare da organizzazione a organizzazione.

- *ISSS* propone di distinguere tra il contenuto della prima segnalazione e, a seconda della classificazione dell'incidente, altri contenuti.

- Le *FFS* ritengono che le informazioni richieste siano parzialmente impraticabili e irrealistiche e chiedono che l'articolo venga modificato in modo da permettere la segnalazione anche se non sono disponibili tutti i dati richiesti.

- *ASA* raccomanda di armonizzare la soglia per le segnalazioni basate sulla LSIn con quella per le segnalazioni basate sulla LPD.

- L'*aeroporto di Zurigo* chiede il divieto per l'UFCS di trasmettere informazioni alle autorità di perseguimento penale e ad altre autorità senza il consenso dell'autorità o dell'organizzazione assoggettata all'obbligo di segnalazione.

- *Switch* propone di concretizzare la disposizione sotto vari aspetti, in particolare stabilendo un limite temporale e un limite relativo al numero di persone interessate.

3.3.2.20 Articolo 20 (Trasmissione della segnalazione)

Art. 20 Trasmissione della segnalazione
Se la segnalazione non viene effettuata tramite il sistema di comunicazione dell'UFCS, questo informa la persona di contatto di cui all'articolo 13 capoverso 2 lettera b di aver ricevuto la segnalazione e del suo contenuto.

Cinque partecipanti alla consultazione si sono espressi in merito alla trasmissione della segnalazione. Nessuno dei partecipanti alla consultazione ha respinto l'articolo 20. I pareri contengono proposte di integrazione e precisazione dell'articolo.

❖ **Segnalazione tramite organizzazioni terze**

- *Switch* propone che una o più imprese possano decidere congiuntamente di trasmettere le segnalazioni tramite un'organizzazione terza specializzata che supporti anche la risposta agli incidenti («incident response»).

- *swissuniversities* raccomanda di integrare l'articolo 20 OCS con un ulteriore capoverso che consenta a una o più imprese di decidere congiuntamente di segnalare gli incidenti tramite un'organizzazione terza specializzata. Propone inoltre una formulazione concreta per tale aggiunta, ossia: «[2] Eine oder mehrere meldepflichtige Behörden oder Organisationen können beschliessen, den Meldeprozess einzeln oder gemeinsam an eine spezialisierte Drittorganisation auszulagern» ([2] Una o più autorità o organizzazioni assoggettate all'obbligo di segnalazione possono decidere di esternalizzare il processo di segnalazione, singolarmente o congiuntamente, a un'organizzazione terza specializzata).

❖ **Anonimato nelle segnalazioni**

- *economiesuisse, scienceindustries* e *digitalswitzerland* propongono di adeguare la formulazione per garantire l'anonimato nelle segnalazioni da parte di terzi. Inoltre, raccomandano una formulazione che permetta la trasmissione dei dati di contatto solo nei casi in cui ciò sia necessario per la protezione della cibersicurezza: «Falls ~~die~~ eine Meldung nicht über das Kommunikationssystem des BACS erfolgt, informiert dieses die Kontaktperson nach Artikel 13 Absatz 2 Buchstabe b einer registrierten und von der Meldung betroffenen Organisation über den Eingang und den Inhalt der Meldung, indes ohne die Kontaktangaben der meldenden Organisation oder Person, es sei denn, auch die Kontaktangaben sind zum Schutz der Cybersicherheit erforderlich» (se ~~la~~ una segnalazione non viene effettuata tramite il sistema di comunicazione dell'UFCS, questo informa la persona di contatto

di cui all'articolo 13 capoverso 2 lettera b di un'organizzazione registrata e interessata dalla segnalazione di aver ricevuto la segnalazione e del suo contenuto, tuttavia senza indicare i dati di contatto dell'organizzazione o della persona che ha effettuato la segnalazione, a meno che anche i dati di contatto non siano necessari per la protezione della cibersicurezza).

3.3.2.21 Articolo 21 (Termine per registrare la segnalazione)

Art. 21 Termine per registrare la segnalazione
[1] Se entro il termine di segnalazione di 24 ore non sono note tutte le informazioni necessarie, l'UFCS concede all'autorità o all'organizzazione interessata un termine di 14 giorni per completare la segnalazione.
[2] Se entro la scadenza del termine non sono disponibili tutte le informazioni necessarie, l'UFCS chiede all'autorità o all'organizzazione interessata di completarle immediatamente o di confermare che le informazioni non sono disponibili.

Dieci partecipanti alla consultazione si sono espressi in merito al termine e alla registrazione della segnalazione. Nessuno dei partecipanti alla consultazione ha respinto l'articolo 21. I pareri contengono proposte di integrazione e precisazione dell'articolo.

❖ **Termine di 24 ore per la prima segnalazione**

- *PNR 77, PFZ* e *UNIL* raccomandano di utilizzare la formulazione più precisa «innerhalb von 24 Stunden nach der Entdeckung des Cyberangriffs» (entro le 24 ore successive all'individuazione del ciberattacco) per facilitare la comprensione da parte delle autorità e delle organizzazioni soggette all'obbligo di segnalazione.

- *Switch* ritiene che il termine di 24 ore costituisca un onere sproporzionato soprattutto per le organizzazioni più piccole. Propone quindi che il termine di 24 ore venga riferito alle settimane lavorative e agli orari d'ufficio.

- *Swissgrid* suggerisce di precisare nell'ordinanza che la segnalazione deve avvenire entro le 24 ore successive all'individuazione del ciberattacco oppure di inserire un rimando diretto all'articolo 74*e* capoverso 1 LSIn.

- *swissuniversities* sottolinea che i requisiti relativi al termine di segnalazione di 24 ore rappresentano una notevole sfida per le piccole scuole universitarie, sia in termini di maturità dei processi esistenti che di personale impiegato o richiesto.

❖ **Termine di 14 giorni per le segnalazioni successive**

- *LU* suggerisce di precisare se il termine di 14 giorni indicato per il completamento della segnalazione si riferisce a giorni lavorativi o a giorni della settimana in generale.

- *SwissICT* suggerisce di fissare un termine inferiore a 14 giorni per le segnalazioni successive e di specificare cosa fa l'UFCS con le informazioni ricevute.

❖ **Adeguamento dei termini agli standard internazionali**

- *economiesuisse* e *scienceindustries* sono favorevoli all'allineamento degli obblighi di segnalazione agli standard internazionali e, di conseguenza, all'adeguamento dei termini a quelli della direttiva NIS2 dell'UE (24 ore per la pre-notifica e 72 ore per la notifica di un incidente).

❖ **Ruolo dell'UFCS e supporto nella raccolta delle informazioni**

- *eAVS/AI* propone che nell'articolo 21 OCS si stabilisca che la raccolta di eventuali ulteriori informazioni che non possono essere acquisite direttamente avvenga nell'ambito di uno scambio con l'UFCS e con il supporto di quest'ultimo.

❖ **Sanzioni in caso di inadempimento**

- *UR* chiede quali sanzioni sono previste se un'autorità interessata non fornisce le informazioni richieste e non adempie all'obbligo di segnalazione all'UFCS.

3.3.2.22 Articolo 22

Art. 22 Modifica di altri atti normativi La modifica di altri atti normativi è disciplinata nell'allegato.

Nessuno dei partecipanti alla consultazione si è espresso in merito all'articolo 22.

3.3.2.23 Articolo 23

Art. 23 Entrata in vigore La presente ordinanza entra in vigore il 1° gennaio 2025.

Dieci partecipanti alla consultazione si sono espressi in merito all'entrata in vigore. Nessuno dei partecipanti alla consultazione ha respinto l'articolo 23. Nei pareri si chiede che l'obbligo di segnalazione previsto entri in vigore successivamente.

❖ **Richiesta di un periodo transitorio di almeno sei mesi**

- *asut, Salt* e *Sunrise* propongono un periodo di introduzione di almeno sei mesi al fine di dare alle imprese il tempo necessario per adattare i loro processi e sistemi tecnici.

❖ **Richiesta di un periodo transitorio di almeno nove mesi**

- *SUISSEDIGITAL* chiede un periodo transitorio di almeno nove mesi tra la pubblicazione del testo ufficiale dell'OCS e l'inizio effettivo dell'obbligo di segnalazione.

❖ **Richiesta di un periodo transitorio di almeno 12 mesi**

- Il *PLR, Swiss Banking* e *Swiss FS-CSC* chiedono un periodo transitorio di almeno un anno, preferibilmente due, tra il momento a partire dal quale il testo finale dell'ordinanza è disponibile e la sua entrata in vigore.

- *ASA, La Posta Svizzera SA, economiesuisse* e *scienceindustries* sostengono che l'entrata in vigore il 1° gennaio 2025 sia prematura e chiedono un periodo di attuazione di almeno un anno dopo la pubblicazione ufficiale dell'ordinanza.

3.3.2.24 Ordinanza del 7 marzo 2003 sull'organizzazione del Dipartimento federale della difesa, della protezione della popolazione e dello sport (OOrg-DDPS)

Art. 15*a* cpv. 2 frase introduttiva nonché lett. f e h [2] Assume in particolare le seguenti funzioni: f. gestisce il team nazionale di risposta alle emergenze informatiche *(Computer Emergency Response Team [CERT])*; h. rappresenta la Svizzera in organi internazionali per l'analisi tecnica di ciberminacce e per la gestione di ciberincidenti.

Tre partecipanti alla consultazione si sono espressi sulle modifiche all'OOrg-DDPS). Nessuno dei partecipanti alla consultazione le ha respinte. I pareri contengono proposte di precisazione e adeguamento dell'articolo.

❖ **Entità e limitazione della partecipazione dell'UFCS agli organi internazionali**

- *ZH* suggerisce di indicare con maggiore precisione l'entità della partecipazione dell'UFCS agli organi internazionali e di limitare tale partecipazione al settore della cibersicurezza. A tale proposito sottolinea tuttavia che lo scambio nazionale e internazionale tra le autorità di perseguimento penale per la protezione preventiva contro le ciberminacce e per la gestione repressiva dei ciberincidenti non deve essere limitato.

- *CMP* chiede di prevedere, nell'articolo 15*a* capoverso 2 lettera h OOrg-DDPS, una definizione più precisa dell'entità del lavoro dell'UFCS in seno agli organi internazionali e una limitazione di tale lavoro al settore della cibersicurezza. Inoltre, sottolinea che questa disposizione non deve limitare lo scambio nazionale e internazionale tra le autorità di perseguimento penale per la protezione – a scopo preventivo – contro le ciberminacce e per la gestione – a scopo repressivo – dei ciberincidenti.

❖ **Spostamento e uniformazione dell'elenco dei compiti**

- *VS* suggerisce di spostare nell'OCS l'elenco dei compiti di cui all'articolo 15*a* OOrg-DDPS e di utilizzare in modo uniforme sia l'acronimo francese «OFCS» (ossia UFCS in italiano) sia la versione inglese NCSC («National Cyber Security Centre [NCSC]») in tutte le basi legali esistenti (LSIn, OSIn e OCS).

3.3.2.25 Ordinanza del 31 agosto 2022 sulla protezione dei dati (OPDa)

Art. 41 cpv. 1 *Abrogato*

Nessuno dei partecipanti alla consultazione si è espresso in merito all'articolo 41 capoverso 1 OPDa.

3.3.2.26 Altre osservazioni

Nove partecipanti alla consultazione hanno formulato nei loro pareri, senza fare riferimento diretto al testo dell'ordinanza, ulteriori osservazioni.

❖ **Coordinamento centrale da parte dell'UFCS**

- L'*aeroporto di Zurigo* propone un nuovo articolo che preveda che una segnalazione all'UFCS annulli automaticamente tutti gli altri obblighi di segnalazione in caso di ciberattacco. L'UFCS dovrebbe fungere da servizio di coordinamento centrale e coordinare le richieste delle autorità.

- *La Posta Svizzera SA*suggerisce che l'UFCS riceva tutte le segnalazioni degli incidenti soggetti all'obbligo di segnalazione e le coordini poi con le altre autorità competenti. In alternativa, propone che le autorità a cui deve essere effettuata la segnalazione si coordinino tra di loro.

- *digitalswitzerland* suggerisce che, per quanto concerne l'obbligo di segnalazione, l'UFCS assuma un ruolo centrale e di coordinamento al fine di evitare oneri supplementari e doppioni.

- *economiesuisse* e *scienceindustries* lamentano la mancanza di coordinamento o armonizzazione tra le molteplici procedure di segnalazione in caso di ciberattacchi e chiedono soluzioni per armonizzare e coordinare le singole procedure.

- *Migros* sottolinea l'importanza di un approccio cooperativo nell'attuazione di procedure armonizzate per quanto concerne l'obbligo di segnalazione e propone di concentrarsi meno sul formalismo e più sul rafforzamento di un dialogo basato sul partenariato tra le autorità e i rappresentanti delle infrastrutture critiche.

- *Swico* accoglie con favore il rafforzamento del ruolo dell'UFCS come servizio di coordinamento centrale, ma ritiene che sia necessario armonizzare le molteplici procedure di segnalazione.

❖ **Altri temi**

- *LU* chiede una definizione più chiara del concetto di «potenziale di danno elevato» nel contesto della cibercriminalità come elemento della ciberstrategia nazionale.

- *digitalswitzerland* propone di introdurre incentivi per favorire un comportamento proattivo nella segnalazione delle vulnerabilità a livello di cibersicurezza e di creare un elenco di criteri specifici per la definizione delle priorità tra le segnalazioni.

- Poiché *Beat Lehmann* non ha formulato commenti specifici su singoli articoli e capoversi dell'ordinanza, le sue proposte e raccomandazioni sono riassunte qui di seguito per temi:

    - *obblighi di segnalazione*: raccomanda di prendere in considerazione diverse situazioni, come l'insorgenza di perturbazioni su larga scala nonché l'obbligo di segnalazione nell'elaborazione degli incarichi e quello relativo alle imprese collegate. Inoltre, propone di armonizzare i vari obblighi di segnalazione previsti dalle diverse leggi e raccomanda di coordinare gli obblighi di segnalazione in caso di ciberattacchi transfrontalieri. Infine, propone di attribuire all'UFCS la competenza di pubblicare promemoria o linee guida per gruppi di casi tipici;

    - *minacce dinamiche*: fa notare le possibili perturbazioni nell'infrastruttura informatica causate da Stati esteri o dai loro agenti. In questo contesto, pone l'accento sul rischio di ciberattacchi come parte della guerra ibrida nonché della disinformazione mirata e sottolinea che non solo l'elaborazione tradizionale dei dati, ma anche la tecnologia operativa (OT) e i sistemi SCADA possono diventare obiettivi di ciberattacchi. Infine, evidenzia il ruolo chiave dell'intelligenza artificiale nello sviluppo di strumenti e metodi per i ciberattachi e la difesa da questi ultimi;

    - *cooperazione internazionale*: raccomanda di evidenziare la possibilità di cooperazione internazionale tra l'UFCS e l'OCSE, l'UE / ENISA e la NATO;

    - *partenariato pubblico-privato*: propone che la LSIn ampliata e l'OCS fungano da base per un ampio partenariato pubblico-privato tra le autorità statali di tutti i livelli, l'economia e il mondo scientifico.

4 Allegato

4.1 Cantoni

AG	Cancelleria dello Stato del Cantone di Argovia	Edificio governativo 5001 Aarau
AI	Cancelleria del Consiglio del Cantone di Appenzello Interno	Marktgasse 2 9050 Appenzello
BE	Cancelleria dello Stato del Cantone di Berna	Postgasse 68 3000 Berna 8
BL	Cancelleria dello Stato del Cantone di Basilea Campagna	Edificio governativo Rathausstrasse 2 4410 Liestal
BS	Cancelleria dello Stato del Cantone di Basilea Città	Marktplatz 9 4001 Basilea
FR	Cancelleria dello Stato del Cantone di Friburgo	Rue des Chanoines 17 1701 Friburgo
GE	Cancelleria dello Stato del Cantone di Ginevra	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Ginevra 3
GL	Cancelleria dello Stato del Cantone di Glarona	Municipio 8750 Glarona
GR	Cancelleria dello Stato del Cantone dei Grigioni	Reichsgasse 35 7001 Coira
LU	Cancelleria dello Stato del Cantone di Lucerna	Bahnhofstrasse 15 6002 Lucerna
NW	Cancelleria dello Stato del Cantone di Nidvaldo	Dorfplatz 2 Casella postale 1246 6371 Stans
OW	Cancelleria dello Stato del Cantone di Obvaldo	Municipio 6061 Sarnen
SG	Cancelleria dello Stato del Cantone di San Gallo	Edificio governativo 9001 San Gallo
SH	Cancelleria dello Stato del Cantone di Sciaffusa	Beckenstube 7 8200 Sciaffusa
SO	Cancelleria dello Stato del Cantone di Soletta	Municipio Barfüssergasse 24 4509 Soletta
SZ	Cancelleria dello Stato del Cantone di Svitto	Edificio governativo Bahnhofstrasse 9 Casella postale 1260 6431 Svitto
TG	Cancelleria dello Stato del Cantone di Turgovia	Edificio governativo Zürcherstrasse 188 8510 Frauenfeld
TI	Cancelleria dello Stato del Cantone Ticino	Piazza Governo 6 6501 Bellinzona
UR	Cancelleria dello Stato del Cantone di Uri	Rathausplatz 1 6460 Altdorf
VD	Cancelleria dello Stato del Cantone di Vaud	Place du Château 4 1014 Losanna

VS	Cancelleria dello Stato del Cantone del Vallese	Planta 3 1950 Sion
ZG	Cancelleria dello Stato del Cantone di Zugo	Seestrasse 2 Edificio governativo Postplatz 6300 Zugo
ZH	Cancelleria dello Stato del Cantone di Zurigo	Neumühlequai 10 Casella postale 8090 Zurigo

4.2 Conferenze cantonali e commissioni federali

CDDGP	Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia	Casa dei Cantoni Speichergasse 6 Casella postale 3001 Berna
CMP	Conferenza svizzera dei Ministeri pubblici	Casa dei Cantoni Speichergasse 6 Casella postale 3001 Berna
UFDC	Ufficio federale del consumo	Ufficio federale del consumo (UFDC) Palazzo federale Est 3003 Berna

4.3 Partiti politici rappresentati in seno all'Assemblea federale

Il Centro		Segreteria generale Hirschengraben 9 Casella postale 3001 Berna
PLR	PLR.I Liberali Radicali	Segreteria generale Neuengasse 20 Casella postale 3001 Berna
PS	Partito socialista svizzero	Segretariato centrale Theaterplatz 4 Casella postale 3001 Berna

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

ACS	Associazione dei Comuni Svizzeri	Holzikofenweg 8 Casella postale 3001 Berna
UCS	Unione delle città svizzere	Monbijoustrasse 8 Casella postale 3001 Berna

4.5 Associazioni mantello nazionali dell'economia

economie-suisse	Federazione delle imprese svizzere	Hegibachstrasse 47 Casella postale 8032 Zurigo
Swiss Banking	Associazione svizzera dei banchieri	Aeschenplatz 7 Casella postale 4182 4002 Basilea
USAM	Unione svizzera delle arti e mestieri	Schwarztorstrasse 26 Casella postale 3001 Berna
USS	Unione sindacale svizzera	Monbijoustrasse 61 3007 Berna

4.6 Altre cerchie interessate

Aeroporto di Ginevra		Aéroport international de Genève CP100 CH 1215 Ginevra
Aeroporto di Zurigo		Flughafen Zurich AG 8058 Zurigo Aeroporto
AES	Associazione delle aziende elettriche svizzere	Hintere Bahnhofstrasse 10 5000 Aarau
ASA	Associazione Svizzera d'Assicurazioni	Conrad-Ferdinand-Meyer-Strasse 14 Casella postale CH-8022 Zurigo
ASIP	Associazione svizzera degli istituti di previdenza	Kreuzstrasse 26 8008 Zurigo
asut	Associazione svizzera delle telecomunicazioni	Hirschengraben 8 3011 Berna
Beat Lehmann		Acting Counsel RioTinto / Alcan Holdings Switzerland AG Kongoweg 9 (Home Office) 5034 Suhr
CH++	Associazione CH++	Sattelgasse 4 4051 Basilea
digital-switzerland	digitalswitzerland	Waisenhausplatz 14 3011 Berna
eAVS/AI		p.a. mundi consulting ag Marktgasse 55 Casella postale 3001 Berna
FAMH	Associazione dei laboratori medici della Svizzera	Altenbergstrasse 29 Casella postale 686 3000 Berna 8
FER	Federazione delle imprese romande	98 rue de Saint-Jean 1211 Ginevra 11
FFS		FFS SA Public Affairs e regolamentazione Hilfikerstrasse 1

		3000 Berna 65
H+	H+ Gli Ospedali Svizzeri	Segretariato centrale Lorrainestrasse 4A 3013 Berna
ISSS	Information Security Society Switzerland	Kochergasse 6 3011 Berna
Migros	Migros	Migros Direzione Politica economica Limmatstrasse 152 Casella postale 1766 8031 Zurigo
MPC	Ministero pubblico della Confederazione	Guisanplatz 1 3003 Berna
NEDIK	Rete di supporto digitale alle indagini sulla criminalità informatica, gestita dalla CCPCS e dalla CDDGP	c/o Segreteria generale CDDGP Casa dei Cantoni Speichergasse 6 Casella postale 3001 Berna
Partito Pirata Svizzero	Partito Pirata Svizzero	Partito Pirata Berna 3000 Berna
PNR 77, PFZ e UNIL	Parere congiunto	
Posta CH SA	La Posta Svizzera SA	Wankdorfallee 4 Casella postale 3030 Berna
Pour Demain	Pour Demain	Marktgasse 46 3011 Berna
Primeo		Weidenstrasse 27 4142 Münchenstein
RAILplus SA	RAILplus SA	Bahnhofstrasse 85 5001 Aarau
Salt		Salt Mobile SA Rue du Caudray 4 CH-1020 Renens 1
science-industries	Associazione economica dell'industria chimica, farmaceutica e life science svizzera	Nordstrasse 15 Casella postale 8021 Zurigo
Suissedigital	Associazione delle reti di comunicazione	Bollwerk 15 CH-3011 Berna
Sunrise		Sunrise GmbH Thurgauerstrasse 101B 8152 Glattpark (Opfikon)
SUVA		Fluhmattstrasse 1 Casella postale 4358 6004 Lucerna
Swico	Swico	Lagerstrasse 33 8004 Zurigo
Swiss FS-CSC	Swiss Financial Sector Cyber Security Centre	Aeschenplatz 7 Casella postale 4182 4002 Basilea

Swiss-ICT	SwissICT	Vulkanstr. 120 8048 Zurigo
swiss-universities	Organizzazione mantello delle università svizzere	swissuniversities Effingerstrasse 15 Casella Postale 3001 Berna
Swissgrid		Bleichemattstrasse 31 Casella postale 5001 Aarau
Switch		Werdstrasse 2 Casella postale 8021 Zurigo
Transitgas	Transitgas AG	Franklinstrasse 27 8050 Zurigo