Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

«$$QrCode»

Legge federale sulla sicurezza delle informazioni in seno alla Confederazione

(Legge sulla sicurezza delle informazioni, LSIn)

Modifica del …

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

I

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

Art. 1 cpv. 1

[1] La presente legge ha lo scopo di:

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

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

Art. 2 cpv. 5

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

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

Art. 5 lett. d ed e

Ai sensi della presente legge s'intende per:

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

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

Titoli prima dell'art. 73a

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

Sezione 1: Disposizioni generali

Art. 73a Principio

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

a. sensibilizzare il pubblico sui ciber-rischi;

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

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

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

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

f. sostenere i gestori di infrastrutture critiche.

Art. 73b Trattamento delle notifiche di ciberincidenti e vulnerabilità

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

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

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

Art. 73c Inoltro di informazioni

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

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

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

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

Art. 74 Sostegno ai gestori di infrastrutture critiche

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

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

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

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

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

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

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

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

Titolo prima dell'art. 74a

Sezione 2: Obbligo di notifica di ciberattacchi a infrastrutture critiche

Art. 74a Obbligo di notifica

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

Art. 74b Settori

L'obbligo di notifica si applica:

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

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

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

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

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

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

    1. sono utilizzati da un gran numero di utenti,

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

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

3. offrono servizi di sicurezza e fiduciari;

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

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

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

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

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

l. alla Società svizzera di radiotelevisione;

m. alle agenzie di stampa d'importanza nazionale;

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

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

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

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

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

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

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

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

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

Art. 74c Eccezioni all'obbligo di notifica

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

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

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

1. riguardano unicamente un numero esiguo di persone,

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

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

Art. 74d Ciberattacchi da notificare

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

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

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

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

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

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

Art. 74e Contenuto della notifica

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

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

Art. 74f Trasmissione della notifica

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

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

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

Art. 74g Obbligo d'informazione

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

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

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

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

Art. 74i Infrazioni contro le decisioni del NCSC

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

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

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

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

16 RS **313.0**

Titolo prima dell'art. 75

Sezione 3: Protezione dei dati e scambio di informazioni

Art. 75 Trattamento di dati personali

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

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

b. procedimenti e sanzioni di carattere amministrativo o penale.

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

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

Art. 76 Cooperazione a livello nazionale

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

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

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

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

Art. 76a Sostegno alle autorità

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

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

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

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

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

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

Art. 77 Cooperazione a livello internazionale

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

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

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

Art. 78
Abrogato

Art. 79 cpv. 1

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

Art. 80
Abrogato

20 RS **235.1**

II

Gli atti normativi qui appresso sono modificati come segue:

1. Legge del 23 marzo 200721 sull'approvvigionamento elettrico

Art. 8a Protezione contro i ciber-rischi

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

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

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

Art. 24 cpv. 5[bis]

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

III

[1] La presente legge sottostà a referendum facoltativo.

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

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