Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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 23 novembre 2022[1],
decreta:

I

La legge del 18 dicembre 2020[2] sulla sicurezza delle informazioni è modificata come segue:

Titolo

Legge federale sulla sicurezza delle informazioni (Legge sulla sicurezza delle informazioni, LSIn)

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 della Svizzera alle ciberminacce.

1 FF **2022** …
2 RS **128**, RU **2022** 232

Art. 2 cpv. 5

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

Art. 4 cpv. 1 e 1bis

1 La legge del 17 dicembre 2004[3] sulla trasparenza (LTras) prevale sulla presente legge.

1bis Le informazioni di terzi di cui il Centro nazionale per la cibersicurezza (NCSC) viene a conoscenza tramite la ricezione e l'analisi di segnalazioni secondo il capitolo 5 non possono essere rese accessibili al pubblico secondo la LTras. Non sono considerati terzi le autorità, le organizzazioni e le persone menzionate all'articolo 2 capoverso 1 LTras.

Art. 5, frase introduttiva (concerne soltanto il testo francese) e lett. d–g

Ai sensi della presente legge s'intende per:

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

e. *ciberattacco:* un ciberincidente provocato intenzionalmente;

f. *ciberminaccia*: qualsiasi circostanza o evento che rende potenzialmente possibile un ciberincidente;

g. *vulnerabilità*: una ciberminaccia che è da ricondurre a punti deboli o errori nei mezzi informatici.

Inserire prima del titolo della sezione 2

Art. 10a Trattamento di dati personali

1 Le autorità e le organizzazioni assoggettate possono trattare i dati personali opportuni al fine di garantire la sicurezza delle informazioni, in particolare nei sistemi d'informazione previsti a tale scopo (applicazioni ISMS).

2 Possono scambiare i dati personali di cui al capoverso 1 reciprocamente nonché con organizzazioni di diritto pubblico nazionali, internazionali ed estere, sempre che:

a. ciò sia opportuno al fine di garantire la sicurezza delle informazioni;

b. non sia violato alcun obbligo legale o contrattuale di mantenere il segreto;

c. siano rispettate le disposizioni della legislazione sulla protezione dei dati; e

3 RS **152.3**

d. queste organizzazioni assumano compiti legali nell'ambito della sicurezza delle informazioni che corrispondono a quelli dell'autorità o dell'organizzazione che ha trasmesso la comunicazione.

3 Le autorità e le organizzazioni assoggettate possono collegare i propri sistemi d'informazione, in particolare le applicazioni ISMS, e scambiarsi dati automaticamente o su richiesta tramite interfacce.

4 Possono gestire i moduli digitali finalizzati all'inoltro e al trattamento di richieste e segnalazioni nell'ambito della sicurezza delle informazioni e collegarli alle proprie applicazioni ISMS o ad altri sistemi d'informazione.

5 Se ciò è necessario per contrastare violazioni della sicurezza delle informazioni o per eliminare vulnerabilità, le autorità e le organizzazioni assoggettate possono:

a. trattare;

b. scambiare reciprocamente nonché con organizzazioni nazionali, internazionali ed estere di diritto pubblico, sempre che le condizioni di cui al capoverso 2 lettera b siano soddisfatte

dati personali degni di particolare protezione secondo l'articolo 5 lettera c della legge del 25 settembre 2020[4] sulla protezione dei dati (LPD) di persone che sono o potrebbero essere coinvolte o interessate.

6 Le autorità e le organizzazioni assoggettate possono conservare i dati personali degni di particolare protezione fino a due anni dopo aver contrastato le violazioni della sicurezza delle informazioni o eliminato le vulnerabilità, ma non oltre dieci anni.

7 L'archiviazione dei dati è retta dalle prescrizioni della legislazione sull'archiviazione.

8 Il trattamento dei dati personali da parte dell'NCSC nel quadro dell'adempimento dei suoi compiti è retto dagli articoli 75–79.

Art. 23 cpv. 3
Concerne soltanto il testo francese.

Art. 44 cpv. 2

2 La restrizione del diritto d'accesso è retta dall'articolo 26 LPD[5].

4 RS **235.1**
5 RS **235.1**

Titolo dopo l'art. 73

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

Sezione 1: Disposizioni generali

Art. 73a Principio

[1] Ai fini della protezione della Svizzera contro le ciberminacce, l'NCSC effettua analisi tecniche per valutare e contrastare ciberincidenti e ciberminacce, nonché per identificare ed eliminare vulnerabilità.

[2] Sulla base delle analisi, l'NCSC svolge in particolare i seguenti compiti:

a. sensibilizzare e avvisare il pubblico riguardo alle ciberminacce;

b. avvisare le autorità, le organizzazioni e le persone interessate in caso di ciberminacce imminenti o di ciberattacchi in corso;

c. pubblicare informazioni sulla cibersicurezza e raccomandazioni per l'adozione di misure preventive e reattive contro i ciberincidenti;

d. ricevere e trattare le segnalazioni riguardanti ciberincidenti e ciberminacce;

e. sostenere i gestori di infrastrutture critiche.

Art. 73b Segnalazioni

[1] L'NCSC riceve le segnalazioni riguardanti ciberincidenti e ciberminacce. Le segnalazioni possono essere anonime.

[2] L'NCSC analizza le segnalazioni in relazione alla loro rilevanza per la protezione della Svizzera contro le ciberminacce. Su richiesta, l'NCSC emana una raccomandazione su come procedere, sempre che non siano necessari ulteriori analisi e chiarimenti.

[3] Se gli vengono segnalate vulnerabilità, l'NCSC informa immediatamente il produttore dell'hardware o del software interessato e gli fissa un congruo termine per eliminarle. Gli indica che la mancata osservanza può essere sanzionata secondo il diritto in materia di appalti pubblici (art. 44 cpv. 1 lett. f^{bis} della legge federale del 21 giugno 2019[6] sugli appalti pubblici) e che l'NCSC, allo scadere del termine, può pubblicare la vulnerabilità ai sensi dell'articolo 73*c* capoverso 2.

Art. 73c Pubblicazione di informazioni provenienti da segnalazioni

[1] L'NCSC può pubblicare informazioni relative a ciberincidenti, sempre che ciò serva alla protezione contro le ciberminacce. Queste informazioni possono permettere di risalire alla persona fisica o giuridica interessata soltanto se quest'ultima vi acconsente

6 RS **172.056.1**

e se le caratteristiche d'identificazione e gli elementi d'indirizzo sono stati utilizzati in modo abusivo.

2 L'NCSC può pubblicare informazioni relative a vulnerabilità indicando l'hardware o il software interessato, sempre che il produttore vi acconsenta o non abbia eliminato la vulnerabilità entro il termine di cui all'articolo 73*b* capoverso 3.

Art. 73d Inoltro di informazioni

1 L'NCSC può inoltrare informazioni provenienti da segnalazioni ad autorità e organizzazioni attive nel settore della cibersicurezza. Queste informazioni possono contenere dati personali soltanto se la persona interessata vi acconsente.

2 Se dalla segnalazione di un ciberincidente o dalla sua analisi emergono informazioni necessarie a individuare tempestivamente e sventare minacce per la sicurezza interna o esterna, a valutare la situazione di minaccia o ad assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche secondo l'articolo 6 capoversi 1 lettera a, 2 e 5 della legge federale del 25 settembre 2015[7] sulle attività informative (LAIn), l'NCSC inoltra queste informazioni al Servizio delle attività informative della Confederazione (SIC).

3 I collaboratori dell'NCSC che nell'ambito di una segnalazione o della sua analisi ottengono indizi di un possibile reato lo denunciano unicamente al direttore dell'NCSC, in deroga all'articolo 22*a* capoverso 1 della legge del 24 marzo 2000[8] sul personale federale (LPers). Quest'ultimo può sporgere denuncia presso le autorità di perseguimento penale, sempre che ciò appaia opportuno in considerazione della gravità del possibile reato.

4 L'NCSC può inoltrare informazioni che rivelano segreti protetti dal diritto penale unicamente secondo quanto disposto dall'articolo 320 del Codice penale[9].

Art. 74 Sostegno ai gestori di infrastrutture critiche

1 L'NCSC sostiene i gestori di infrastrutture critiche nella protezione contro le ciberminacce.

2 L'NCSC mette loro a disposizione gratuitamente per l'utilizzo su base volontaria in particolare i seguenti strumenti:

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

b. informazioni tecniche sulle ciberminacce attuali e raccomandazioni per l'adozione di misure preventive e reattive contro i ciberincidenti;

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

7 RS **121**
8 RS **172.220.1**
9 RS **311.0**

[3] L'NCSC può fornire loro consulenza e sostegno nel contrastare ciberincidenti ed eliminare vulnerabilità se il funzionamento dell'infrastruttura critica interessata rischia di essere compromesso e, nel caso si tratti di gestori privati, se non è possibile procurarsi per tempo un sostegno equivalente sul mercato.

[4] Previo consenso del gestore interessato, l'NCSC può accedere alle informazioni e ai mezzi informatici di quest'ultimo per analizzare un ciberincidente.

Titolo dopo l'art. 74

Sezione 2: Obbligo di segnalare ciberattacchi

Art. 74a Principi

[1] Le autorità e le organizzazioni di cui all'articolo 74*b* devono provvedere affinché i ciberattacchi verso i loro mezzi informatici siano segnalati all'NCSC.

[2] L'NCSC informa le autorità e le organizzazioni interessate sul loro eventuale assoggettamento ed emana su richiesta una decisione sull'assoggettamento all'obbligo di segnalare.

[3] Tramite la segnalazione di un ciberattacco, le autorità e le organizzazioni assoggettate all'obbligo di segnalare hanno diritto al sostegno dell'NCSC nel contrastare incidenti secondo l'articolo 74 capoverso 3.

[4] L'obbligo di segnalare è finalizzato soltanto a consentire all'NCSC di individuare per tempo modelli di attacco contro infrastrutture critiche e di avvisare così possibili interessati e raccomandare loro misure di prevenzione e di difesa adeguate.

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

[1] L'obbligo di segnalare si applica:

a. alle scuole universitarie secondo l'articolo 2 capoverso 2 della legge federale del 30 settembre 2011[10] sulla promozione e sul coordinamento del settore universitario svizzero;

b. alle autorità federali, cantonali e comunali nonché alle organizzazioni intercantonali, cantonali e intercomunali, ad eccezione dell'Aggruppamento Difesa, laddove l'esercito presti servizio d'appoggio secondo articolo 67 o servizio attivo secondo l'articolo 76 della legge militare del 3 febbraio 1995[11];

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[12]

10 RS **414.20**
11 RS **510.10**
12 RS **730.0**

sull'energia nonché nel commercio, nella misurazione e nella gestione dell'energia, ad eccezione dei titolari di licenze conformemente alla legge federale del 21 marzo 2003[13] sull'energia nucleare, sempre che venga effettuato un ciberattacco contro un impianto nucleare;

e. alle imprese che sottostanno alla legge dell'8 novembre 1934[14] sulle banche, alla legge del 17 dicembre 2004[15] sulla sorveglianza degli assicuratori o alla legge del 19 giugno 2015[16] sull'infrastruttura finanziaria;

f. alle strutture sanitarie che figurano nell'elenco compilato dal Cantone di cui all'articolo 39 capoverso 1 lettera e della legge federale del 18 marzo 1994[17] sull'assicurazione malattie;

g. ai laboratori medici che dispongono di un'autorizzazione secondo l'articolo 16 capoverso 1 della legge del 28 settembre 2012[18] sulle epidemie;

h. alle imprese che dispongono di un'autorizzazione secondo la legge del 15 dicembre 2000[19] sugli agenti terapeutici per la fabbricazione, l'immissione in commercio e l'importazione di medicamenti;

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

j. alla Società svizzera di radiotelevisione;

k. alle agenzie di stampa d'importanza nazionale;

l. ai fornitori di servizi postali registrati presso la Commissione delle poste secondo l'articolo 4 capoverso 1 della legge del 17 dicembre 2010[20] sulle poste;

m. alle imprese ferroviarie secondo l'articolo 5 o 8*c* della legge federale del 20 dicembre 1957[21] sulle ferrovie e alle imprese che gestiscono impianti di trasporto a fune, linee filoviarie, autobus e battelli e sono titolari di una concessione secondo l'articolo 6 della legge del 20 marzo 2009[22] sul trasporto di viaggiatori;

n. alle imprese dell'aviazione civile che dispongono di un'autorizzazione dell'Ufficio federale dell'aviazione civile e agli aeroporti nazionali conformemente al Piano settoriale dei trasporti, Parte Infrastruttura aeronautica;

13 RS **732.1**
14 RS **952.0**
15 RS **961.01**
16 RS **958.1**
17 RS **832.10**
18 RS **818.101**
19 RS **812.21**
20 RS **783.0**
21 RS **742.101**
22 RS **745.1**

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

p. alle imprese che riforniscono la popolazione di beni indispensabili di uso quotidiano, sempre che l'interruzione o il pregiudizio della loro attività comporti considerevoli difficoltà di approvvigionamento;

q. ai fornitori di servizi di telecomunicazione registrati presso l'Ufficio federale delle comunicazioni secondo l'articolo 4 capoverso 1 della legge del 30 aprile 1997[24] sulle telecomunicazioni (LTC);

r. ai gestori di registri e ai registri di domini Internet secondo l'articolo 28*b* LTC;

s. ai fornitori e ai gestori di servizi e infrastrutture che servono all'esercizio dei diritti politici;

t. ai fornitori e ai gestori di «cloud computing», motori di ricerca o servizi di sicurezza e fiduciari digitali nonché ai centri di calcolo, sempre che abbiano una sede in Svizzera;

u. ai produttori di hardware o software i cui prodotti sono utilizzati da infrastrutture critiche, sempre che tali hardware o software abbiano un accesso remoto per la manutenzione o siano impiegati per uno dei seguenti scopi:

1. la gestione e il monitoraggio di sistemi e processi tecnici,
2. la garanzia della sicurezza pubblica.

[2] Le autorità e le organizzazioni che esercitano anche attività non rientranti nel campo di applicazione del capoverso 1 non hanno l'obbligo di segnalare i ciberattacchi che hanno conseguenze unicamente su queste attività.

[3] L'obbligo di segnalare di cui al capoverso 1 si applica a ciberattacchi che hanno conseguenze in Svizzera anche se i mezzi informatici interessati si trovano all'estero.

Art. 74c Eccezioni all'obbligo di segnalare

Il Consiglio federale esenta le autorità e le organizzazioni di cui all'articolo 74*b* dall'obbligo di segnalare se i guasti funzionali causati da ciberattacchi hanno conseguenze minime sul funzionamento dell'economia o sul benessere della popolazione.

Art. 74d Ciberattacchi da segnalare

[1] Un ciberattacco deve essere segnalato se:

a. compromette il funzionamento dell'infrastruttura critica interessata;

b. ha comportato una manipolazione o una fuga di informazioni;

23 RS **747.30**
24 RS **784.10**

c. non è stato identificato per un periodo prolungato, in particolare se vi sono indizi secondo cui potrebbe essere stato effettuato per preparare altri ciberattacchi; oppure

d. è connesso al reato di estorsione, minaccia o coazione.

Art. 74e Termine e contenuto della segnalazione

[1] La segnalazione deve avvenire entro le 24 ore successive all'individuazione del ciberattacco.

[2] Deve contenere informazioni sull'autorità o sull'organizzazione assoggettata all'obbligo di segnalare, sul tipo di ciberattacco e sulla sua esecuzione, sulle sue conseguenze, sulle misure adottate e, se noto, sull'ulteriore modo di procedere previsto.

[3] Se al momento della segnalazione non sono ancora note tutte le informazioni necessarie, l'autorità o l'organizzazione assoggettata all'obbligo di segnalare completa la segnalazione non appena dispone di nuove informazioni.

[4] Chi deve adempiere l'obbligo di segnalare per conto di un'autorità o di un'organizzazione non è tenuto, nel quadro della segnalazione, a fornire indicazioni che lo rendono penalmente perseguibile.

[5] L'NCSC informa l'autorità o l'organizzazione assoggettata all'obbligo di segnalare non appena sono disponibili tutte le informazioni che consentono di adempiere tale obbligo.

Art. 74f Trasmissione della segnalazione

[1] Per la segnalazione elettronica di ciberattacchi, l'NCSC mette a disposizione un sistema sicuro con cui trasmettere la segnalazione allo stesso NCSC.

[2] Il sistema deve permettere alle autorità e alle organizzazioni assoggettate all'obbligo di segnalare di trasmettere ad altre autorità la segnalazione del ciberattacco o le sue conseguenze sia nella sua totalità sia in parte.

[3] Se per adempiere l'obbligo di segnalare nei confronti di altre autorità sono necessarie informazioni che vanno oltre quelle menzionate all'articolo 74*e*, il sistema deve permettere alle autorità e alle organizzazioni assoggettate all'obbligo di segnalare di trasmettere queste informazioni direttamente alle autorità interessate senza che l'NCSC vi acceda.

Art. 74g Violazione dell'obbligo di segnalare

[1] Se vi sono indizi di una violazione dell'obbligo di segnalare, l'NCSC ne informa l'autorità o l'organizzazione assoggettata a tale obbligo e fissa un congruo termine per provvedervi.

[2] Se l'autorità o l'organizzazione assoggettata all'obbligo di segnalare non adempie il proprio obbligo entro questo termine, l'NCSC emana una decisione fissando un nuovo termine e indicando la comminatoria della multa di cui all'articolo 74*h*.

Art. 74h Inosservanza di decisioni dell'NCSC

[1] Chi, intenzionalmente, non ottempera a una decisione dell'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] In caso di infrazioni di cui al capoverso 1 commesse nell'azienda è applicabile l'articolo 6 della legge federale del 22 marzo 1974[25] 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 dal perseguimento di dette persone e, in loro vece, condannare l'azienda al pagamento della multa.

[4] In caso di inosservanza di una decisione dell'NCSC, il perseguimento e il giudizio sono demandati ai Cantoni.

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, l'NCSC può trattare dati personali, ivi compresi elementi di indirizzo di cui all'articolo 3 lettera f LTC[26] e i relativi dati personali degni di particolare protezione, che contengono informazioni su:

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

b. perseguimenti e sanzioni di natura amministrativa o penale.

[2] In caso di trattamento di dati personali o di indizi concreti di usurpazione d'identità o di utilizzazione non autorizzata di elementi di indirizzo, l'NCSC informa le persone interessate sempre che ciò non comporti un onere sproporzionato e nessun interesse pubblico preponderante vi si opponga.

Art. 76 Cooperazione a livello nazionale

[1] L'NCSC può comunicare dati personali ai gestori di infrastrutture critiche, sempre che ciò sia necessario alla protezione contro le ciberminacce.

[2] I gestori di infrastrutture critiche possono comunicare dati personali all'NCSC, sempre che ciò sia necessario alla protezione contro le ciberminacce.

25 RS **313.0**
26 RS **784.10**

3 L'NCSC può comunicare ai fornitori di servizi di telecomunicazione elementi di indirizzo e i relativi dati personali, sempre che ciò sia necessario alla protezione contro le ciberminacce.

4 I fornitori di servizi di telecomunicazione possono comunicare all'NCSC elementi di indirizzo e i relativi dati personali, sempre che ciò sia necessario alla protezione contro le ciberminacce.

Art. 76a Sostegno alle autorità

1 L'NCSC sostiene il SIC con valutazioni periodiche sul numero, sul tipo e sulla portata dei ciberattacchi e, su richiesta, con analisi tecniche delle ciberminacce.

2 Concede al SIC l'accesso a informazioni che riguardano l'identità e il modo di operare degli autori di ciberattacchi al fine di individuare precocemente e prevenire minacce alla sicurezza interna o esterna, valutare la situazione di minaccia e assicurare un servizio di preallerta informativa per la protezione di infrastrutture critiche secondo l'articolo 6 capoversi 1 lettera a, 2 e 5 LAIn[27].

3 L'NCSC concede alle autorità di perseguimento penale l'accesso a informazioni che riguardano l'identità e il modo di operare degli autori di ciberattacchi.

4 Concede ai servizi cantonali competenti per la cibersicurezza l'accesso alle informazioni necessarie alla protezione contro le ciberminacce.

Art. 77 Cooperazione a livello internazionale

1 L'NCSC può scambiare informazioni che permettono di risalire all'identità e al modo di operare degli autori di ciberattacchi con servizi esteri e internazionali competenti per la cibersicurezza se questi ultimi necessitano di tali informazioni per l'adempimento di compiti corrispondenti a quelli dell'NCSC. Se lo scambio di informazioni concerne anche dati personali, vanno osservati gli articoli 16 e 17 LPD[28].

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

Art. 78
Abrogato

Art. 79 cpv. 1

1 L'NCSC conserva i dati personali soltanto finché ciò sia opportuno per individuare ciberminacce o contrastare ciberincidenti, ma al massimo per cinque anni dall'ultimo utilizzo a tale scopo; per i dati personali degni di particolare protezione il termine è di due anni.

27 RS **121**
28 RS **235.1**

Art. 80
Abrogato

II

Gli atti normativi qui appresso sono modificati come segue:

1. Legge federale del 21 giugno 2019[29] sugli appalti pubblici

Art. 44 cpv. 1 lett. f^bis

1 Il committente può escludere un offerente dalla procedura di aggiudicazione, radiarlo da un elenco o revocare l'aggiudicazione, se constata che l'offerente, un terzo coinvolto o i rispettivi organi realizzano una delle seguenti fattispecie:

f^bis non eliminano entro il termine fissato dal Centro nazionale per la cibersicurezza secondo l'articolo 73*b* capoverso 3 della legge del 18 dicembre 2020[30] sulla sicurezza delle informazioni una vulnerabilità nell'hardware o nel software da loro prodotto.

2. Legge federale del 25 settembre 2020[31] sulla protezione dei dati

Art. 24 cpv. 5^bis

5bis L'IFPDT, con il consenso del titolare del trattamento, può inoltrare la notifica al Centro nazionale per la cibersicurezza ai fini dell'analisi dell'incidente. La segnalazione può contenere dati personali, ivi compresi dati personali degni di particolare protezione su perseguimenti o sanzioni di natura amministrativa e penale concernenti il responsabile.

3. Legge federale del 21 marzo 2003[32] sull'energia nucleare

Art. 102 cpv. 2

2 Se riceve una segnalazione riguardante un ciberattacco a un impianto nucleare che adempie le condizioni di cui all'articolo 74*d* della legge del 18 dicembre 2020[33] sulla sicurezza delle informazioni, l'Ispettorato federale della sicurezza nucleare inoltra questa segnalazione al Centro nazionale per la cibersicurezza.

29 RS **172.056.1**
30 RS **128**, RU **2022** 232
31 RS **235.1**, RU **2022** 491
32 RS **732.1**
33 RS **128**, RU **2022** 232

4. Legge del 23 marzo 2007[34] sull'approvvigionamento elettrico

Art. 8a Protezione contro le ciberminacce

[1] I gestori di rete, i produttori e i gestori di impianti di stoccaggio devono adottare misure per proteggere adeguatamente i loro impianti contro le ciberminacce.

[2] Il Consiglio federale può prevedere eccezioni e, se ciò fosse necessario per garantire l'approvvigionamento, estendere l'obbligo di cui al capoverso 1 ad altri fornitori attivi nel settore dell'approvvigionamento elettrico.

5. Legge del 22 giugno 2007[35] sulla vigilanza dei mercati finanziari

Art. 39 cpv. 1

[1] La FINMA è autorizzata a trasmettere ad altre autorità svizzere di vigilanza, al Centro nazionale per la cibersicurezza e alla Banca nazionale svizzera le informazioni non accessibili al pubblico di cui esse necessitano per adempiere i loro compiti.

III

La presente legge sottostà a referendum facoltativo.

Il Consiglio federale ne determina l'entrata in vigore.

34 RS **734.7**
35 RS **956.1**