Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ce texte est une version provisoire. La version définitive qui sera publiée sous www.fedlex.admin.ch fait foi.

«$$QrCode»

Loi fédérale sur la sécurité de l'information au sein de la Confédération

(Loi sur la sécurité de l'information, LSI)

Modification du ...

L'Assemblée fédérale de la Confédération suisse,
vu le message du Conseil fédéral du …
arrête:

I

La loi du 18 décembre 2020 sur la sécurité de l'information[1] est modifiée comme suit:

Titre

Loi fédérale sur la sécurité de l'information (loi sur la sécurité de l'information, LSI)

Art. 1, al. 1

[1] La présente loi vise:

a. à garantir la sécurité du traitement des informations relevant de la compétence de la Confédération et la sécurité de ses moyens informatiques;

b. à accroître la capacité de résilience de la Suisse face aux cybermenaces.

Art. 2, al. 5

[5] Les organisations de droit public ou de droit privé qui exploitent des infrastructures critiques sans être visées par les al. 1 à 3 sont soumises aux art. 73*a* à 79. La législation spéciale peut prévoir que d'autres dispositions de la présente loi leur sont applicables.

1 RS **128**; RO **2022** 232

Art. 4, al. 1 et 1bis

1 La loi du 17 décembre 2004 sur la transparence (LTrans)[2] prime la présente loi.

1bis Les informations relatives à des tiers dont le Centre national pour la cybersécurité (NCSC) prend connaissance dans son activité de réception et d'analyse des signalements conformément au chap. 5 ne peuvent être rendues accessibles en vertu de la LTrans. Les autorités, les organisations et les personnes visées à l'art. 2, al. 1, LTrans ne sont pas considérées comme des tiers.

Art. 5, phrase introductive et let. d à g

Au sens de la présente loi, on entend par:

d. *cyberincident:* un événement survenant lors de l'utilisation de moyens informatiques et ayant pour conséquence une atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'informations ou à la traçabilité de leur traitement;

e. *cyberattaque:* un cyberincident provoqué intentionnellement;

f. *cybermenace*: toute circonstance ou tout événement pouvant entraîner un cyberincident;

g. *vulnérabilité*: une cybermenace due à des failles ou à des erreurs dans les moyens informatiques.

Insérer avant le titre de la section 2

Art. 10a Traitement des données personnelles

1 Les autorités et organisations soumises à la présente loi peuvent traiter les données personnelles utiles à la sécurité de l'information, notamment dans les systèmes de gestion de la sécurité des informations prévus à cet effet (applications SGSI).

2 Elles peuvent échanger des données personnelles au sens de l'al. 1 entre elles et avec des organisations nationales, internationales ou étrangères de droit public, dans la mesure où:

a. cela est utile à la sécurité de l'information;

b. cela n'enfreint aucune obligation légale ou contractuelle de garder le secret;

c. les dispositions de la législation fédérale sur la protection des données sont respectées, et

d. l'organisation qui reçoit les données assume des tâches légales dans le domaine de la sécurité de l'information qui correspondent à celles de l'autorité ou de l'organisation qui fait la communication.

3 Elles peuvent relier entre eux leurs systèmes d'information, notamment les applications SGSI, et échanger des données automatiquement ou sur demande par l'intermédiaire d'interfaces.

2 RS **152.3**

4 Elles peuvent administrer des formulaires électroniques servant à soumettre ou à traiter des demandes et des signalements dans le domaine de la sécurité de l'information et les relier à leurs applications SGSI ou à d'autres systèmes d'information.

5 Dans la mesure où cela est nécessaire pour gérer des violations de la sécurité de l'information ou pour éliminer des vulnérabilités, elles peuvent effectuer les actions suivantes avec des données sensibles au sens de l'art. 5, let. c, de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[3] relatives à des personnes qui sont impliquées dans ces violations ou ces vulnérabilités ou qui sont ou pourraient être concernées par elles:

a. les traiter;

b. les échanger entre elles et avec des organisations nationales, internationales ou étrangères de droit public, pour autant que les conditions visées à l'al. 2, let. b, soient remplies.

6 Elles peuvent conserver les données sensibles jusqu'à deux ans après la gestion des violations de la sécurité de l'information ou l'élimination des vulnérabilités, mais dix ans au plus.

7 L'archivage des données est régi par les dispositions de la législation relative à l'archivage.

8 Le traitement de données personnelles par le NCSC dans le cadre de l'accomplissement de ses tâches est régi par les articles 75–79.

Art. 23, al. 3

3 Elles peuvent exploiter, conformément à l'art. 34, al. 1ter, de la loi du 30 avril 1997 sur les télécommunications (LTC)[4], une installation perturbatrice dans les zones de sécurité où des informations classifiées «secret» sont fréquemment traitées ou des moyens informatiques de la catégorie de sécurité «protection très élevée» sont exploités.

Art. 44, al. 2

2 Les restrictions à la communication de renseignements sont régies par l'art. 26 LPD[5].

Titre suivant l'art. 73

3 RS **235.1**
4 RS **784.10**
5 RS **235.1**

Chapitre 5 Mesures de la Confédération afin de protéger la Suisse contre les cybermenaces

Section 1 Dispositions générales

Art. 73a Principe

[1] Afin de protéger la Suisse contre les cybermenaces, le NCSC réalise des analyses techniques pour évaluer et contrer les cyberincidents et les cybermenaces, ainsi que pour identifier et éliminer les vulnérabilités.

[2] Sur la base de ces analyses, le NCSC assume notamment les tâches suivantes:

a. sensibiliser le grand public aux cybermenaces et l'alerter sur de telles menaces;

b. alerter les autorités, les organisations et les personnes concernées en cas de cybermenace immédiate ou de cyberattaque en cours;

c. publier des informations sur la cybersécurité et des recommandations sur les mesures préventives et réactives à prendre contre les cyberincidents;

d. réceptionner et traiter les signalements concernant les cyberincidents et les cybermenaces;

e. soutenir les exploitants d'infrastructures critiques.

Art. 73b Signalements

[1] Le NCSC reçoit des signalements concernant des cyberincidents et des cybermenaces. Les signalements peuvent être anonymes.

[2] Le NCSC analyse les signalements au regard de leur importance pour la protection de la Suisse contre les cybermenaces. Sur demande, il émet une recommandation quant aux mesures à prendre, pour autant qu'aucune analyse ou clarification supplémentaire ne soit nécessaire à cet effet.

[3] Si le NCSC prend connaissance d'une vulnérabilité, il en informe immédiatement le fabricant du matériel informatique ou du logiciel concerné et lui fixe un délai approprié pour l'éliminer. Il lui indique que tout manquement pourra être sanctionné en vertu du droit des marchés publics (art. 44, al. 1, let. f[bis], de la loi fédérale du 21 juin 2019 sur les marchés publics[6]) et qu'à l'expiration du délai, il pourra rendre publique la vulnérabilité en vertu de l'art. 73*c*, al. 2.

Art. 73c Publication d'informations provenant de signalements

[1] Le NCSC peut publier des informations relatives à des cyberincidents, pour autant que cela serve à la protection contre les cybermenaces. Ces informations ne peuvent contenir de données relatives aux personnes physiques ou morales concernées que si ces dernières y consentent et que ces données sont des caractères d'identification et des ressources d'adressage utilisés de manière abusive.

6 RS **172.056.1**

[2] Le NCSC peut publier des informations relatives à des vulnérabilités en indiquant le matériel informatique ou le logiciel concerné, à condition que le fabricant y consente ou qu'il n'ait pas éliminé la vulnérabilité dans le délai visé à l'art. 73*b*, al. 3.

Art. 73d Transmission d'informations

[1] Le NCSC peut transmettre des informations provenant de signalements aux autorités et aux organisations actives dans le domaine de la cybersécurité. Ces informations ne peuvent contenir de données personnelles que si la personne concernée y consent.

[2] Si le signalement d'un cyberincident ou son analyse révèle des informations nécessaires pour déceler à temps et prévenir des menaces pour la sûreté intérieure ou extérieure, pour apprécier la menace ou pour assurer un service d'alerte précoce en vue de protéger les infrastructures critiques conformément à l'art. 6, al. 1, let. a, 2 et 5, de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)[7], le NCSC transmet ces informations au SRC.

[3] En dérogation à l'art. 22*a*, al. 1, de la loi du 24 mars 2000 sur le personnel de la Confédération[8], les collaborateurs du NCSC qui, dans le cadre d'un signalement ou de son analyse, obtiennent des informations sur une possible infraction la rapportent exclusivement au directeur du NCSC. Celui-ci peut dénoncer cette possible infraction aux autorités de poursuite pénale si la gravité de cette dernière le justifie.

[4] La transmission par le NCSC de secrets protégés par le droit pénal doit obéir aux exigences prévues à l'art. 320 du code pénal[9].

Art. 74 Soutien aux exploitants d'infrastructures critiques

[1] Le NCSC aide les exploitants d'infrastructures critiques à se protéger contre les cybermenaces.

[2] Il met notamment à leur disposition, à titre gratuit et pour une utilisation sur une base volontaire, les outils suivants:

a. un système de communication permettant l'échange sécurisé d'informations;

b. des informations techniques sur les cybermenaces en cours et des recommandations sur les mesures préventives et réactives à prendre contre les cyberincidents;

c. des instruments techniques et des instructions de détection des cyberincidents visant à répondre aux besoins accrus de protection des infrastructures critiques.

[3] Il peut les conseiller et les soutenir dans la gestion des cyberincidents et l'élimination des vulnérabilités lorsque le fonctionnement de l'infrastructure critique concernée est mis en péril et, s'il s'agit d'exploitants privés, qu'il n'est pas possible d'obtenir en temps voulu un soutien équivalent sur le marché.

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

[4] Avec l'accord de l'exploitant concerné, il peut accéder aux informations et aux moyens informatiques de celui-ci pour analyser un cyberincident.

Titre suivant l'art. 74

Section 2 Obligation de signaler les cyberattaques

Art. 74a Principes

[1] Les autorités et les organisations énumérées à l'art. 74*b* veillent à ce que les cyberattaques visant leurs moyens informatiques soient signalées au NCSC.

[2] Le NCSC renseigne les autorités et les organisations intéressées sur leur éventuel assujettissement à l'obligation de signaler et rend sur demande une décision concernant leur assujettissement à cette obligation.

[3] Lorsqu'elles signalent une cyberattaque, les autorités et les organisations assujetties à l'obligation de signaler ont droit, dans la gestion de l'incident, au soutien du NCSC prévu à l'art. 74, al. 3.

[4] L'obligation de signaler vise uniquement à permettre au NCSC de détecter à un stade précoce les modes opératoires utilisés lors des attaques visant les infrastructures critiques et, ainsi, d'avertir les victimes potentielles et de leur recommander les mesures préventives et réactives qui s'imposent.

Art. 74b Autorités et organisations assujetties à l'obligation de signaler

[1] L'obligation de signaler s'applique:

a. aux hautes écoles au sens de l'art. 2, al. 2, de la loi du 30 septembre 2011 sur l'encouragement et la coordination des hautes écoles[10];

b. aux autorités fédérales, cantonales et communales ainsi qu'aux organisations intercantonales, cantonales et intercommunales, à l'exception du Groupement Défense lorsque l'armée accomplit un service d'appui ou un service actif au sens respectivement des art. 67 et 76 de la loi du 3 février 1995 sur l'armée[11];

c. aux organisations chargées de tâches de droit public dans les domaines de la sécurité et du sauvetage, de l'approvisionnement en eau potable, du traitement des eaux usées et de l'élimination des déchets;

d. aux entreprises œuvrant dans les domaines de l'approvisionnement énergétique au sens de l'art. 6, al. 1, de la loi du 30 septembre 2016 sur l'énergie[12] ainsi que du commerce, de la mesure et de la gestion de l'énergie, à l'exception des détenteurs d'une autorisation au sens de la loi du 21 mars 2003 sur l'énergie nucléaire[13] si une cyberattaque est lancée contre une installation nucléaire;

10 RS **414.20**
11 RS **510.10**
12 RS **730.0**
13 RS **732.1**

e. aux entreprises soumises à la loi du 8 novembre 1934 sur les banques[14], à la loi du 17 décembre 2004 sur la surveillance des assurances[15] ou à la loi du 19 juin 2015 sur l'infrastructure des marchés financiers[16];

f. aux établissements de santé figurant sur la liste hospitalière cantonale conformément à l'art. 39, al. 1, let. e, de la loi fédérale du 18 mars 1994 sur l'assurance-maladie[17];

g. aux laboratoires médicaux titulaires d'une autorisation conformément à l'art. 16, al. 1, de la loi du 28 septembre 2012 sur les épidémies[18];

h. aux entreprises titulaires d'une autorisation de fabriquer, de mettre sur le marché ou d'importer des médicaments conformément à la loi du 15 décembre 2000 sur les produits thérapeutiques[19];

i. aux organisations qui fournissent des prestations destinées à couvrir les conséquences de la maladie, des accidents, de l'incapacité de travail et de gain, de la vieillesse, de l'invalidité et de l'impotence;

j. à la Société suisse de radiodiffusion et télévision;

k. aux agences de presse d'importance nationale;

l. aux prestataires de services postaux enregistrés auprès de la Commission de la poste conformément à l'art. 4, al. 1, de la loi du 17 décembre 2010 sur la poste[20];

m. aux entreprises ferroviaires visées à l'art. 5 ou 8*c* de la loi fédérale du 20 décembre 1957 sur les chemins de fer[21] ainsi qu'aux entreprises d'installations à câbles, de trolleybus, d'autobus et de navigation concessionnaires au sens de l'art. 6 de la loi du 20 mars 2009 sur le transport de voyageurs[22];

n. aux entreprises de l'aviation civile disposant d'une autorisation délivrée par l'Office fédéral de l'aviation civile et aux aéroports nationaux figurant dans le Plan sectoriel de l'infrastructure aéronautique;

o. aux entreprises qui transportent des marchandises sur le Rhin conformément à la loi fédérale du 23 septembre 1953 sur la navigation maritime sous pavillon suisse[23] et aux entreprises qui effectuent l'enregistrement, le chargement ou le déchargement de marchandises dans le port de Bâle;

p. aux entreprises qui approvisionnent la population en biens d'usage quotidien indispensables et dont la défaillance partielle ou complète entraînerait de graves difficultés d'approvisionnement;

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**
23 RS **747.30**

q. aux fournisseurs de services de télécommunication enregistrés auprès de l'Office fédéral de la communication (OFCOM) conformément à l'art. 4, al. 1, LTC[24];

r. aux registres et aux registraires de domaines Internet au sens de l'art. 28*b* LTC;

s. aux fournisseurs et aux exploitants de services et d'infrastructures servant à l'exercice des droits politiques;

t. aux fournisseurs et aux exploitants d'informatique en nuage, de moteurs de recherche, de services numériques de sécurité ou de confiance ainsi que de centres de calcul, pour autant qu'ils aient un siège en Suisse;

u. aux fabricants de matériel informatique ou de logiciels dont les produits sont utilisés par des infrastructures critiques, si le matériel ou les logiciels concernés disposent d'un accès de télémaintenance ou sont utilisés à l'une des fins suivantes:

1. commande et surveillance de systèmes et de processus techniques,
2. garantie de la sécurité publique.

[2] Les autorités et les organisations qui exercent également des activités ne relevant pas de l'al. 1 n'ont pas l'obligation de signaler les cyberattaques qui ont un effet uniquement sur ces activités.

[3] L'obligation de signaler visée à l'al. 1 s'applique aux cyberattaques qui ont un effet en Suisse, même si les moyens informatiques concernés se trouvent à l'étranger.

Art. 74c Exceptions à l'obligation de signaler

Le Conseil fédéral exempte les organisations et les autorités de l'obligation de signaler visée à l'art. 74*b* lorsque les perturbations provoquées par les cyberattaques n'ont qu'un effet limité sur le fonctionnement de l'économie ou sur le bien-être de la population.

Art. 74d Cyberattaques à signaler

Une cyberattaque doit être signalée lorsqu'elle:

a. met en péril le fonctionnement de l'infrastructure critique concernée;

b. a entraîné une manipulation ou une fuite d'informations;

c. n'a pas été détectée pendant une période prolongée, en particulier si des indices laissent penser qu'elle a été exécutée en vue de préparer d'autres cyberattaques, ou

d. s'accompagne d'actes de chantage, de menaces ou de contrainte.

Art. 74e *Délai et contenu du signalement*

[1] Le signalement doit être fait dans les 24 heures suivant la détection de la cyberattaque.

[2] Il doit contenir des informations sur l'autorité ou l'organisation assujetties à l'obligation de signaler, sur le type et l'exécution de la cyberattaque, sur ses effets, sur les mesures prises et, si elles sont connues, sur les mesures prévues.

[3] Si toutes les informations requises ne sont pas connues au moment du signalement, l'autorité ou l'organisation assujettie à l'obligation de signaler complète le signalement dès qu'elle dispose de nouvelles informations.

[4] Celui qui assume l'obligation de signaler pour une autorité ou une organisation n'est pas tenu, dans le cadre du signalement, de fournir des informations qui l'exposent à des poursuites pénales.

[5] Le NCSC informe l'autorité ou l'organisation assujettie à l'obligation de signaler dès que toutes les données permettant de satisfaire à l'obligation de signaler sont disponibles.

Art. 74f *Communication du signalement*

[1] Le NCSC met à disposition un système sécurisé qui permet de lui communiquer le signalement des cyberattaques par voie électronique.

[2] Le système doit permettre aux autorités ou aux organisations assujetties à l'obligation de signaler de communiquer simultanément à d'autres autorités tout ou partie du signalement de la cyberattaque ou de ses effets.

[3] Si des informations dépassant le cadre de celles prévues à l'art. 74*e* sont nécessaires à l'exécution d'une obligation de signaler vis-à-vis d'autres autorités, le système doit permettre aux autorités ou aux organisations assujetties à l'obligation de signaler de les communiquer directement aux autorités concernées, sans que le NCSC y ait accès.

Art. 74g *Violation de l'obligation de signaler*

[1] Si des indices laissent présumer une violation de l'obligation de signaler, le NCSC en informe l'autorité ou l'organisation assujettie à l'obligation de signaler et lui fixe un délai approprié pour s'acquitter de cette obligation.

[2] Si l'autorité ou l'organisation concernée ne s'acquitte pas de son obligation dans ce délai, le NCSC rend une décision concernant cette obligation, dans laquelle il lui fixe un nouveau délai et l'informe qu'elle est menacée d'une amende conformément à l'art. 74*h*.

Art. 74h *Insoumission à une décision du NCSC*

[1] Est puni d'une amende de 100 000 francs au plus quiconque, intentionnellement, ne se conforme pas à une décision entrée en force que le NCSC lui a notifiée sous la menace de l'amende prévue par le présent article ou à une décision des instances de recours.

2 L'insoumission aux décisions visées à l'al. 1 au sein d'une entreprise est soumise à l'art. 6 de la loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA)[25].

3 Si le montant prévisible de l'amende ne dépasse pas 20 000 francs et que l'enquête portant sur des personnes punissables en vertu de l'art. 6 DPA implique des mesures d'instruction hors de proportion par rapport à la peine encourue, l'autorité peut renoncer à poursuivre ces personnes et condamner l'entreprise au paiement de l'amende.

4 En cas d'insoumission à une décision du NCSC, la poursuite et le jugement sont du ressort des cantons.

Titre précédant l'art. 75

Section 3 Protection des données et échange d'informations

Art. 75 *Traitement des données personnelles*

1 Pour accomplir ses tâches, le NCSC peut traiter des données personnelles, y compris les ressources d'adressage au sens de l'art. 3, let. f, LTC[26] et les données sensibles qui s'y rapportent, qui contiennent des informations relatives:

a. à des opinions religieuses, philosophiques ou politiques; le traitement des données n'est admissible que dans la mesure où il est nécessaire à l'évaluation de menaces et de dangers concrets en matière de cybersécurité;

b. à des poursuites ou à des sanctions pénales ou administratives.

2 Lors du traitement de données personnelles ou en cas de soupçon fondé d'usurpation d'identité ou d'utilisation abusive de ressources d'adressage, le NCSC en informe les personnes concernées si cela n'entraîne pas des efforts disproportionnés et qu'aucun intérêt public prépondérant ne s'y oppose.

Art. 76 *Collaboration* sur le plan national

1 Le NCSC peut communiquer aux exploitants d'infrastructures critiques des données personnelles dans la mesure où cela est nécessaire à la protection contre des cybermenaces.

2 Les exploitants d'infrastructures critiques peuvent communiquer au NCSC des données personnelles dans la mesure où cela est nécessaire à la protection contre des cybermenaces.

3 Le NCSC peut communiquer aux fournisseurs de services de télécommunication des ressources d'adressage et les données personnelles qui s'y rapportent dans la mesure où cela est nécessaire à la protection contre des cybermenaces.

4 Les fournisseurs de services de télécommunication peuvent communiquer au NCSC des ressources d'adressage et les données personnelles qui s'y rapportent dans la mesure où cela est nécessaire à la protection contre les cybermenaces.

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

Art. 76a Soutien aux autorités

[1] Le NCSC apporte son soutien au SRC en lui fournissant des évaluations périodiques du nombre, du type et de l'ampleur des cyberattaques ainsi que, sur demande, des analyses techniques des cybermenaces.

[2] Il octroie au SRC l'accès à des informations concernant l'identité ou le mode opératoire des auteurs de cyberattaques dans le but de déceler à temps et de prévenir les menaces pour la sûreté intérieure ou extérieure, d'apprécier la menace ou d'assurer un service d'alerte précoce en vue de protéger les infrastructures critiques au sens de l'art. 6, al. 1, let. a, 2 et 5, LRens[27]. Il octroie aux autorités de poursuite pénale l'accès à des informations concernant l'identité et le mode opératoire des auteurs de cyberattaques.

[4] Il octroie aux services cantonaux chargés de la cybersécurité l'accès aux informations nécessaires à la protection contre les cybermenaces.

Art. 77 Coopération internationale

[1] Le NCSC peut échanger avec des services étrangers ou internationaux chargés de la cybersécurité des informations permettant de connaître l'identité ou le mode opératoire des auteurs de cyberattaques s'ils en ont besoin pour accomplir des tâches qui correspondent à celles du NCSC. Si l'échange d'informations comprend également des données personnelles, les art. 16 et 17 LPD[28] sont applicables.

[2] L'échange d'informations au sens de l'al. 1 n'est autorisé que si les services étrangers ou internationaux garantissent que les données seront utilisées conformément aux fins prévues.

Art. 78

Abrogé

Art. 79, al. 1

[1] Le NCSC conserve les données personnelles aussi longtemps que celles-ci sont utiles pour détecter des cybermenaces ou gérer des cyberincidents, mais cinq ans au plus à compter de leur dernière utilisation à cette fin. Pour les données sensibles, le délai est de deux ans.

Art. 80

Abrogé

II

Les actes mentionnés ci-après sont modifiés comme suit:

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

1. Loi fédérale du 21 juin 2019 sur les marchés publics[29]

Art. 44, al. 1, let. f^bis

[1] L'adjudicateur peut exclure un soumissionnaire de la procédure d'adjudication, le radier d'une liste ou révoquer une adjudication s'il est constaté que le soumissionnaire, un de ses organes, un tiers auquel il fait appel ou un organe de ce dernier:

f^bis. n'élimine pas une vulnérabilité du matériel informatique ou du logiciel qu'il a fabriqué dans le délai fixé par le Centre national pour la cybersécurité conformément à l'art. 73b, al. 3, de la loi du 18 décembre 2020 sur la sécurité de l'information[30] ;

2. Loi fédérale du 25 septembre 2020 sur la protection des données[31]

Art. 24, al. 5^bis

[5bis] Le PFPDT peut, avec l'accord du responsable du traitement, transmettre l'annonce au Centre national pour la cybersécurité pour que celui-ci analyse l'incident. La communication peut contenir des données personnelles, y compris des données sensibles relatives à des poursuites ou à des sanctions pénales ou administratives visant le responsable du traitement.

3. Loi du 21 mars 2003 sur l'énergie nucléaire[32]

Art. 102, al. 2

[2] Si l'IFSN reçoit un signalement concernant une cyberattaque lancée contre une installation nucléaire et remplissant les conditions visées à l'art. 74*d* de la loi du 18 décembre 2020 sur la sécurité de l'information[33], elle transmet ce signalement au Centre national pour la cybersécurité.

4. Loi du 23 mars 2007 sur l'approvisionnement en électricité[34]

Art. 8a Protection contre les cybermenaces

[1] Les gestionnaires de réseau, les producteurs et les agents de stockage prennent des mesures pour protéger adéquatement leurs installations contre les cybermenaces.

29 RS **172.056.1**
30 RS **128**, RO **2022** 232
31 RS **235.1**; RO **2022** 491
32 RS **732.1**
33 RS **128**, RO **2022** 232
34 RS **734.7**

2 Le Conseil fédéral peut prévoir des exceptions et, si cela est nécessaire pour garantir l'approvisionnement, étendre l'obligation visée à l'al. 1 à d'autres prestataires de l'approvisionnement en électricité.

5. Loi du 22 juin 2007 sur la surveillance des marchés financiers[35]

Art. 39, al. 1

1 La FINMA est habilitée à communiquer à d'autres autorités suisses exerçant des tâches de surveillance, au Centre national pour la cybersécurité ainsi qu'à la Banque nationale suisse les informations non accessibles au public dont elles ont besoin pour s'acquitter de leurs tâches.

III

La présente loi est sujette au référendum.

Le Conseil fédéral fixe la date de l'entrée en vigueur.

35 RS **956.1**