Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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:

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 résistance de la Suisse aux cyberrisques.

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.

RS **126**
[1] RS **126** [FF **2020** 9665]

Art. 5, let. d à e

Dans la présente loi, on entend par:

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

e. *cyberattaque:* un cyberincident provoqué intentionnellement par un tiers non autorisé.

Titre précédant l'art. 73a

Chapitre 5 Mesures de la Confédération visant à protéger la Suisse contre les cyberrisques

Section 1 Dispositions générales

Art. 73a Principe

Afin de protéger la Suisse contre les cyberrisques, le Centre national pour la cybersécurité (NCSC) assume notamment les tâches suivantes:

a. sensibiliser le grand public aux cyberrisques;

b. mettre en garde contre les cyberrisques et les vulnérabilités des moyens informatiques;

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

d. effectuer des analyses techniques visant à évaluer et à écarter les cyberrisques;

e. réceptionner et traiter les signalements concernant les cyberincidents et les vulnérabilités des moyens informatiques;

f. soutenir les exploitants d'infrastructures critiques.

Art. 73b Traitement des signalements concernant les cyberincidents et les vulnérabilités

[1] Lorsque des cyberincidents ou des vulnérabilités de moyens informatiques sont signalés au NCSC, celui-ci les analyse afin de déterminer leur importance pour la protection de la Suisse contre les cyberrisques. Si la personne qui a effectué le signalement le souhaite, le NCSC émet une recommandation quant aux mesures à prendre pour autant que la situation ne nécessite pas d'analyses ou de clarifications supplémentaires.

[2] Le NCSC peut publier ou communiquer aux autorités et aux organisations intéressées des informations sur les cyberincidents si cela permet de prévenir ou de combattre les

cyberattaques. Ces informations peuvent contenir des données personnelles ou des données concernant des personnes morales, pour autant qu'il s'agisse de caractères d'identification et de ressources d'adressage usurpés et que la personne concernée ait donné son accord.

3 Le NCSC informe immédiatement le fabricant des vulnérabilités qui lui sont signalées et lui fixe un délai approprié pour y remédier. Si le fabricant n'y remédie pas dans le délai imparti, le NCSC publie la vulnérabilité en indiquant le logiciel ou le matériel concerné pour autant que cela contribue à la protection contre les cyberrisques.

Art. 73c Transmission d'informations

1 Si le signalement d'un cyberincident ou son analyse révèlent des informations pertinentes pour déceler à temps et prévenir des menaces contre la sécurité intérieure ou extérieure, pour évaluer le niveau de menace ou pour assurer un service d'alerte précoce dans le domaine du renseignement 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)[2], le NCSC transmet ces informations au SRC.

2 Les collaborateurs du NCSC ne sont pas soumis à l'obligation de dénoncer prévue à l'art. 22*a* de la loi du 24 mars 2000 sur le personnel de la Confédération[3] si, dans le cadre du signalement d'un cyberincident ou de son analyse, ils obtiennent des informations sur une infraction éventuelle. Le responsable du NCSC peut dénoncer l'infraction si cela semble indiqué au vu de sa gravité.

3 Les informations communiquées au NCSC par une personne dans le cadre d'un signalement ne peuvent être utilisées dans une procédure pénale contre cette personne qu'avec l'accord de celle-ci.

4 Le NCSC ne peut transmettre des informations qui révèlent des secrets pénalement protégés que conformément aux exigences prévues à l'art. 320 CP[4].

Art. 74 Soutien aux exploitants d'infrastructures critiques

1 Le NCSC aide les exploitants d'infrastructures critiques à se protéger contre les cyberrisques.

2 À cette fin, il met notamment à leur disposition les instruments suivants:

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

b. des informations techniques sur les cyberrisques et vulnérabilités connus ainsi que des recommandations sur les mesures de prévention;

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

3 Il les conseille et les aide dans la gestion des cyberincidents et la correction des vulnérabilités lorsqu'il existe un risque imminent de conséquences graves pour

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

l'infrastructure critique et que, pour autant qu'il s'agisse d'exploitants privés, il n'est pas possible d'obtenir un soutien équivalent sur le marché en temps utile.

4 Avec l'accord de l'exploitant concerné, il peut accéder aux informations et aux moyens informatiques de celui-ci pour analyser le cyberincident. L'exploitant peut donner son accord même s'il est tenu par des obligations de confidentialité.

Titre précédant l'art. 74a

Section 2 Obligation de signaler les cyberattaques contre des infrastructures critiques

Art. 74a Obligation de signalement

L'exploitant d'une infrastructure critique doit signaler les cyberattaques au NCSC le plus rapidement possible après leur découverte afin que celui-ci puisse identifier les modes opératoires à un stade précoce, avertir les victimes potentielles et leur recommander les mesures de prévention et de défense qui s'imposent.

Art. 74b Domaines

L'obligation de signalement 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[5];

b. aux autorités fédérales, cantonales ou communales ainsi qu'aux organisations intercantonales, cantonales et intercommunales;

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[6] ainsi que du commerce, de la mesure et de la gestion de l'énergie;

e. aux entreprises soumises à la loi du 8 novembre 1934 sur les banques[7], à la loi du 17 décembre 2004 sur la surveillance des assurances[8] ou à la loi du 19 juin 2015 sur l'infrastructure des marchés financiers[9];

f. aux fournisseurs de places de marché en ligne, d'informatique en nuage, de moteurs de recherche et à d'autres services numériques ainsi qu'aux registraires de noms de domaine et aux exploitants de centres de calcul, qui, en Suisse,

    1. sont sollicités par un grand nombre d'utilisateurs,

5 RS **414.20**
6 RS **730.0**
7 RS **952.0**
8 RS **961.01**
9 RS **958.1**

2. ont une grande importance pour l'économie numérique, ou
3. offrent des services de sécurité et de confiance;

g. aux hôpitaux figurant sur la liste hospitalière cantonale des hôpitaux conformément à l'art. 9, al. 1, let. e, de la loi fédérale du 18 mars 1994 sur l'assurance-maladie[10];

h. aux laboratoires médicaux titulaires d'une autorisation conformément à l'art. 16, al. 1, de la loi du 28 septembre 2012 sur les épidémies[11];

i. aux entreprises qui sont titulaires d'une autorisation de fabriquer, d'importer ou de faire le commerce de médicaments conformément à la loi du 15 décembre 2000 sur les produits thérapeutiques (LPTh)[12] ou qui fabriquent ou distribuent des dispositifs médicaux au sens de l'art. 4, al. 1, let. b, LPTh;

j. aux organisations qui fournissent des prestations d'assurance sociale pour 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;

k. aux fournisseurs de services de télécommunication au sens de l'art. 3, let. b, LTC;

l. à la Société suisse de radiodiffusion et télévision;

m. aux agences de presse d'importance nationale;

n. aux fournisseurs 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[13];

o. aux entreprises de transport soumises à la loi fédérale du 18 juin 2010 sur les organes de sécurité des entreprises de transports publics[14];

p. aux entreprises de l'aviation civile qui disposent d'une autorisation délivrée par l'Office fédéral de l'aviation civile;

q. 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[15] et aux entreprises qui effectuent l'enregistrement, le chargement ou le déchargement de marchandises dans le port de Bâle;

r. aux entreprises qui approvisionnent la population en biens d'usage quotidien indispensables;

s. aux fabricants de matériel et de logiciels informatiques 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:

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

1. technique de commande et surveillance des systèmes,
2. exploitation de dispositifs médicaux et d'installations de télécommunication,
3. garantie de la sécurité publique,
4. sécurité informatique, cryptage, identification, autorisation d'accès et d'entrée.

Art. 74c Exceptions à l'obligation de signalement

Le Conseil fédéral exempte certaines catégories d'exploitants d'infrastructures critiques de l'obligation de signalement si les défaillances ou les dysfonctionnements provoqués par des cyberattaques contre leurs infrastructures:

a. sont peu probables, notamment en raison d'une faible dépendance à l'égard des moyens informatiques, ou
b. n'ont qu'un impact limité sur le fonctionnement de l'économie ou sur le bien-être de la population, en particulier parce qu'ils:
    1. ne portent préjudice qu'à un petit nombre de personnes,
    2. sont suppléés par d'autres infrastructures critiques, ou
    3. ne présentent qu'un faible potentiel de dommages économiques.

Art. 74d Cyberattaques à signaler

[1] Une cyberattaque contre une infrastructure critique doit être signalée si des indices laissent présumer:

a. qu'elle met en péril le bon fonctionnement de l'infrastructure critique touchée ou une autre infrastructure critique;
b. qu'elle a été exécutée par un État étranger ou à son instigation;
c. qu'elle a entraîné ou pourrait entraîner une fuite ou la manipulation d'informations, ou
d. qu'elle est passée inaperçue pendant plus de 30 jours.

[2] Une cyberattaque contre une infrastructure critique doit toujours être signalée si elle s'accompagne d'actes de chantage, de menaces ou de contrainte à l'encontre de l'exploitant de l'infrastructure critique ou de ses collaborateurs.

Art. 74e Contenu du signalement

[1] Le signalement d'une cyberattaque contient des informations concernant l'infrastructure critique, le type de cyberattaque subie, son déroulement et ses conséquences ainsi que les mesures que compte prendre l'exploitant de l'infrastructure.

[2] Si, au moment du signalement, l'exploitant de l'infrastructure critique ne dispose pas de toutes les informations requises, il complète le signalement dès que celles-ci lui parviennent.

Art. 74f Communication du signalement

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

[2] Ce système doit permettre à l'exploitant d'une infrastructure critique de communiquer simultanément à d'autres services et autorités tout ou partie du signalement de la cyberattaque ou de ses conséquences.

[3] Si le service ou l'autorité concernés ont besoin d'informations qui dépassent le cadre de celles prévues à l'art. 74*e*, l'exploitant peut les leur communiquer directement via ce système.

Art. 74g Obligation de fournir des renseignements

L'exploitant de l'infrastructure critique fournit au NCSC les informations complémentaires sur le contenu du signalement visé à l'article 74*e* dont le NCSC a besoin pour remplir ses tâches en matière de prévention de toute nouvelle cyberattaque contre des infrastructures critiques.

Art. 74h Infraction à l'obligation de signalement ou à l'obligation de fournir des renseignements

[1] Si des indices laissent présumer une infraction aux obligations de signalement ou de fournir des renseignements, le NCSC en informe l'exploitant de l'infrastructure critique.

[2] Si, malgré cette information, l'exploitant ne remplit pas son obligation, le NCSC rend une décision concernant les obligations dont celui-ci est tenu de s'acquitter, lui fixe un délai et l'informe qu'il est menacé d'une amende en vertu de l'art. 74*i*.

Art. 74i Non-observation de décisions 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 signifiée sous la menace de la peine prévue par le présent article ou à une décision des instances de recours.

[2] Les infractions commises dans une entreprise sont soumises à l'art. 6 de la loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA)[16].

[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

16 RS **313.0**

renoncer à poursuivre ces personnes et condamner l'entreprise au paiement de l'amende.

4 En cas de non-observation d'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 Dans la mesure où il a en besoin 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[17] 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 celles-ci sont nécessaires 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 Il peut traiter les données personnelles à l'insu de la personne concernée si cela est nécessaire pour éviter de compromettre la finalité de ce traitement ou de devoir engager des efforts disproportionnés.

3 En cas de soupçon fondé d'usurpation d'identité ou d'utilisation abusive de ressources d'adressage, il en informe les personnes dont l'identité ou les ressources d'adressage sont usurpées; les art. 18*a*, al. 4, let. b, et 18*b* LPD[18] sont réservés.

Art. 76 Collaboration sur le plan national

1 Le NCSC peut communiquer aux exploitants d'infrastructures critiques des données personnelles dans la mesure où elles sont utiles à la protection des infrastructures critiques contre les cyberrisques.

2 Les exploitants d'infrastructures critiques peuvent communiquer au NCSC des données personnelles dans la mesure où elles sont utiles à la protection des infrastructures critiques contre les cyberrisques.

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 elles sont utiles à la protection des infrastructures critiques contre les cyberrisques.

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 elles sont utiles à la protection des infrastructures critiques contre les cyberrisques.

17 RS **784.10**
18 RS **235.1**

Art. 76a Assistance technique aux autorités

[1] Le NCSC apporte son appui au SRC dans la détection précoce et la prévention des menaces pour la sûreté intérieure ou extérieure, dans l'évaluation de la menace et dans le service d'alerte précoce en matière de renseignement pour la protection des infrastructures critiques conformément à l'art. 6, al. 1, let. a, 2 et 5, LRens[19] en procédant à des évaluations des cyberattaques quant à leur nombre, leur type et leur ampleur et à des analyses techniques des cyberrisques.

[2] Il octroie au SRC l'accès en ligne à des informations qui renseignent sur l'identité et le mode opératoire des auteurs de cyberattaques.

[3] Il octroie aux autorités de poursuite pénale l'accès en ligne à des informations qui renseignent sur l'identité et le mode opératoire des auteurs de cyberattaques.

[4] Il peut octroyer aux services cantonaux chargés de la cybersécurité l'accès en ligne à des informations nécessaires à la protection des autorités cantonales et des infrastructures critiques cantonales contre les cyberrisques.

Art. 77 Coopération internationale

[1] Le NCSC peut échanger des informations avec des services étrangers ou internationaux chargés de la cybersécurité si ceux-ci en ont besoin pour accomplir des tâches correspondant à celles du NCSC. Si l'échange d'informations comprend également des données personnelles au sens de l'art. 75, l'art. 6 LPD[20] est applicable.

[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.

[3] Si les informations sont nécessaires à l'exécution d'une procédure à l'étranger, les dispositions régissant l'assistance administrative et l'entraide judiciaire sont applicables.

Art. 78
Abrogé

Art. 79, al. 1

[1] Le NCSC conserve les données personnelles aussi longtemps que celles-ci sont utiles pour prévenir des dangers ou pour identifier des incidents, mais cinq ans au plus à compter de leur dernière utilisation; en ce qui concerne les données sensibles, la durée de conservation est limitée à deux ans.

Art. 80
Abrogé

19 RS **121**
20 RS **235.1**

II

Les lois mentionnées ci-après sont modifiées comme suit:

1. Loi du 23 mars 2007 sur l'approvisionnement en électricité[21]

Art. 8*a* Protection contre les cyberrisques

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

[2] Le Conseil fédéral peut étendre cette obligation à d'autres parties.

2. Loi du 25 septembre 2020 sur la protection des données[22]

Art. 24, al. 5bis

[5bis] Le PFPDT peut, avec l'accord du responsable tenu à l'obligation de signalement, transmettre le signalement au Centre national pour la cybersécurité à des fins d'analyse de l'incident. Le signalement peut contenir des données personnelles, y compris des données sensibles relatives à des poursuites ou à des sanctions pénales ou administratives visant le responsable tenu à l'obligation de signalement.

III

[1] La présente loi est sujette au référendum.

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

21 RS **734.7**
22 RS **235.1**, FF 2020 7397