www.jusletter.ch

Pauline Meyer / Sylvain Métille

Loi fédérale sur la sécurité de l'information : version 2.0

La Loi fédérale sur la sécurité de l'information (LSI) servira de cadre légal pour assurer des traitements (informatisés ou non) sécurisés de l'information, principalement au sein de l'administration fédérale. Elle servira également de base légale pour l'activité du Centre national pour la cybersécurité (NCSC) et prévoira une obligation de signaler les cyberattaques visant les infrastructures critiques. Nous allons examiner en quoi consiste exactement cette loi et, plus particulièrement, les conséquences de l'obligation de signaler les cyberattaques pour les organisations qui y seront soumises.

Catégories d'articles : Contributions
Domaines juridiques : Protection des données ; Informatique et droit

Proposition de citation : Pauline Meyer / Sylvain Métille, Loi fédérale sur la sécurité de l'information : version 2.0, in : Jusletter 5 septembre 2022

ISSN 1424-7410, jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

EDITIONS WEBLAW

Table des matières

I. Introduction

[1] La législation sur la sécurité de l'information au sein de la Confédération est aujourd'hui encore fragmentée avec une Ordonnance concernant la protection des informations de la Confédération (OPrI),[1] plusieurs ordonnances sur les contrôles de personnes,[2] une Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (OPCy)[3] ou encore des directives internes à l'administration. Aujourd'hui, le législateur a admis qu'une législation unifiée et harmonisée, prévoyant la protection des informations contre les (cyber)risques les menaçant, était

1 RS 510.411.

2 Ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes (OCSP, RS 120.4), Ordonnance de la Chancellerie fédérale du 30 novembre 2011 sur les contrôles de sécurité relatifs aux personnes (OCSP-ChF, RS 120.421), Ordonnance du DEFR du 2 novembre 2011 sur les contrôles de sécurité relatifs aux personnes (OCSP-DEFR, RS 120.422), Ordonnance du DDPS du 12 mars 2012 concernant les contrôles de sécurité relatifs aux personnes (OCSP-DDPS, RS 120.423), Ordonnance du DFAE du 14 août 2012 sur les contrôles de sécurité relatifs aux personnes (OCSP-DFAE, RS 120.424), Ordonnance du DETEC du 15 février 2013 sur les contrôles de sécurité relatifs aux personnes (OCSP-DETEC, RS 120.425), Ordonnance du DFJP du 26 juin 2013 sur les contrôles de sécurité relatifs aux personnes (OCSP-DFJP, RS 120.426), Ordonnance du DFI du 12 août 2013 sur les contrôles de sécurité relatifs aux personnes (OCSP-DFI, RS 120.427).

3 RS 120.73. L'OPCy était le résultat de la mesure 15 (M15) de la Stratégie nationale pour la protection de la Suisse contre les cyberrisques pour la période 2018–2022 (SNPC 2018–2022). La LSI, reprenant cette Ordonnance, permet donc de prendre en compte la protection de la Suisse contre les cyberrisques en considération.

nécessaire.[4] C'est dans cette vision qu'a été adoptée la LSI, qui a vocation à reprendre la majorité de ces réglementations. Elle pose les principes et mesures générales de protection de l'information, de protection des moyens informatiques permettant le traitement de l'information ainsi que du contrôle des personnes traitant l'information.

[2] La Loi sur la sécurité de l'information (LSI)[5] a pourtant failli ne jamais voir le jour, le Conseil national ayant initialement refusé d'entrer en matière sur le projet.[6] Cette loi est pourtant bien nécessaire pour assurer la protection de plusieurs éléments d'importance nationale : la protection des informations traitées par les autorités de la Confédération, la protection de la Suisse contre les (cyber)risques et la protection des infrastructures critiques. En tant que loi principale pour la sécurité de l'information au sein de la Confédération, elle visera à garantir la sécurité du traitement (informatisé ou non) des informations relevant de la Confédération, ainsi qu'à augmenter la capacité de résistance de cette dernière face aux cyberrisques (art. 1 al. 1 AP-LSI2).[7] Les menaces visant la Suisse sont aujourd'hui nombreuses et pèsent toujours plus sur les informations traitées par la Confédération. La Confédération traite, dans l'accomplissement de ses tâches, des volumes importants d'informations revêtant un intérêt notamment pour la sécurité intérieure ou extérieure ou les relations internationales de la Suisse. Elle traite également des informations devant être classifiées, soumises à des secrets ou contenant des données personnelles. Les informations traitées par la Confédération doivent être protégées contre les vols, l'espionnage et les autres perturbations. La majorité des traitements effectués par l'administration sont aujourd'hui informatisés, raison pour laquelle il faut, en accord avec la mise en œuvre de la Stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC),[8] protéger les informations traitées par ce biais. Néanmoins, il ne faut pas oublier les autres traitements d'informations effectués par les autorités de la Confédération.

[3] Alors que la LSI n'est pas encore entrée en vigueur, elle est déjà en voie d'être modifiée (LSI2). Cette modification est nécessaire afin d'avoir une base légale pour les fonctions du Centre national pour la cybersécurité (NCSC), ainsi que pour obliger le signalement des cyberattaques visant les infrastructures critiques.[9] Vulnérables aux cyberattaques et délivrant des prestations essentielles au bien-être de la population ou au fonctionnement de l'État, les infrastructures critiques sont au cœur de la protection de la Suisse contre les cyberrisques.[10] C'est dans ce cadre qu'une obligation

4 FF 2017 2766, 2776–2778.

5 L'abréviation « LSI » est utilisée ici pour désigner la Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération, déjà adoptée et publiée au RO 2022 232, https://www.fedlex.admin.ch/eli/oc/2022/232/fr (consulté le 18 août 2022).

6 Conseil national, 13 mars 2018, https ://www.parlament.ch/fr/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen ?SubjectId=42833 (consulté le 18 août 2022). Une séance de conciliation a même été nécessaire entre les deux Conseils.

7 L'abréviation « AP-LSI2 » est utilisée pour désigner l'avant-projet de la loi révisée, disponible à https ://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2021/70/cons_1/doc_1/fr/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2021-70-cons_1-doc_1-fr-pdf-a.pdf (consulté le 18 août 2022).

8 Au sujet de la dernière SNPC, en voie de renouvellement, voir Conseil fédéral, Plan de mise en oeuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022, mai 2019 ; Conseil fédéral, Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022, avril 2018.

9 Centre national pour la cybersécurité (NCSC), Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques, Modification de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information, LSI), Rapport explicatif relatif à l'ouverture de la procédure de consultation, 12 janvier 2022, p. 10.

10 Centre national pour la cybersécurité (NCSC), Évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques pour les années 2018 à 2022, rapport final, 28 mars 2022, p. 15.

de signaler d'abord les cyberincidents puis uniquement les cyberattaques a été conçue. Cette obligation doit permettre de mieux protéger les infrastructures critiques et de dresser un tableau plus précis de la situation relative aux cyberattaques en Suisse.

[4] L'avant-projet de modification de la LSI (AP-LSI2) a été mis en consultation et l'entrée en vigueur de la loi est prévue pour 2023.[11] La LSI n'est pas encore bien connue et ses contours, comme sa portée, peuvent paraître encore flous. La présente contribution cherche à exposer brièvement la systématique de la loi et sa portée en soulevant quelques questions qu'elle pose. Nous approfondirons ensuite les nouveautés introduites par la révision de ce projet de loi, dont l'élément principal est la nouvelle obligation de signaler les cyberattaques touchant les infrastructures critiques. La procédure de consultation s'est achevée il y a peu et il est déjà possible de dessiner les principales obligations pour les différentes entités soumises à cette obligation.

II. Champ d'application institutionnel

1. Principe : administration fédérale

[5] L'Assemblée fédérale, le Conseil fédéral, les tribunaux de la Confédération, le Ministère public de la Confédération et son autorité de surveillance, ainsi que la Banque nationale suisse, seront soumises à la LSI (art. 2 al. 1 LSI).[12] Il est important que le champ d'application institutionnel de la loi s'étende à toutes les autorités fédérales, y compris les autorités législatives et judiciaires. Cette décision se justifie du fait que ces pouvoirs traitent des informations classifiées et participent à des échanges d'informations. La LSI doit renforcer les échanges, notamment électroniques, entre autorités, démontrant dans un contexte de développement de la cyberadministration un souhait de comblement de lacunes transversales et d'harmonisation des systèmes informatiques utilisés par différentes autorités.[13]

[6] Dans la mesure où les autorités susmentionnées délèguent de nombreuses tâches à des organisations, ces dernières seront également soumises à la LSI. Sont compris à ce titre les Services du Parlement, l'administration fédérale, les services administratifs des tribunaux de la Confédération, l'armée et les organisations et personnes de droit public ou privé extérieures à l'administration fédérale à qui la législation fédérale confie des tâches (renvoi à l'art. 2 al. 4 de la loi sur l'organisation du gouvernement et de l'administration, LOGA).[14] Ces organisations mentionnées à l'art. 2 al. 2 LSI ne sont pas soumises à toutes les dispositions de la loi, contrairement aux autorités susmentionnées. La loi limite déjà en son sein la portée de certaines dispositions à certaines autorités. Il en va de la sorte pour l'obligation d'assurer la responsabilité en matière de sécurité de l'information dans son domaine de compétence (art. 7 LSI) ou de l'établissement

11 Communiqué du Conseil fédéral, du Département fédéral de la défense, de la protection de la population et des sports, du Groupement de la Défense et d'Armasuisse, Entrée en vigueur partielle de la loi sur la sécurité de l'information décidée par le Conseil fédéral, Berne 6 avril 2022, https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-87907.html (consulté le 16 août 2022).

12 FF 2017 282 3 s. Elles sont assimilées dans la LSI aux « autorités soumises à la présente loi ».

13 FF 2017 2787, 2810.

14 RS 172.010.

d'un plan d'action et d'exercices dans l'éventualité de graves incidents susceptibles de menacer l'accomplissement des tâches indispensables de la Confédération (art. 10 al. 2 LSI).[15]

[7] Lorsqu'il en va plus précisément de l'administration décentralisée ou des organisations de l'art. 2 al. 4 LOGA pour leurs tâches administratives, le Conseil fédéral pourra restreindre (dans une ordonnance relative à la LSI ou dans les ordonnances relatives aux lois spéciales) le champ d'application de la LSI aux entités exerçant des activités sensibles ou accédant à des moyens informatiques de la Confédération dans l'accomplissement de leurs tâches (art. 2 al. 3 LSI). Il pourra également limiter le champ d'application de la loi à certaines dispositions pour ces personnes (art. 2 al. 4 LSI).[16]

2. Champ d'application limité

a. Aux cantons

[8] Les cantons ne seront soumis aux obligations prévues par la LSI que de façon limitée (art. 3 LSI). Il semble de prime abord difficilement possible, pour des raisons constitutionnelles, que la Confédération impose aux cantons une utilisation sûre de leurs propres moyens informatiques et des informations qu'ils traitent indépendamment de la Confédération.[17]

[9] D'une part, les dispositions sur la classification des informations (art. 11 à 15 LSI) ne s'appliqueront à ces derniers que lorsqu'ils traitent des informations classifiées de la Confédération (art. 3 al. 1 lit. a LSI). D'autre part, les dispositions relatives à la sécurité des moyens informatiques (art. 16 à 19 LSI) leur seront applicables uniquement lorsqu'ils accèdent à des moyens informatiques de la Confédération (art. 3 al. 1 lit. b LSI). La loi prévoit une exception pour les cantons garantissant une sécurité au moins équivalente de l'information (art. 3 al. 2 LSI).

b. Aux exploitants d'infrastructures critiques

[10] L'infrastructure critique est définie à l'art. 5 lit. c LSI comme « l'approvisionnement en eau potable et en énergie, les infrastructures d'information, de communication et de transports, ainsi que d'autres installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population ». L'art. 74b AP-LSI2 contient actuellement une liste d'organisations soumises à l'obligation de signaler les cyberattaques. La coordination entre ces deux dispositions n'est pas claire et pose la question de savoir si l'art. 74b AP-LSI2 prévoit d'illustrer la définition de l'art. 5 lit. c LSI ou s'il se limitera à lister certaines entités considérées comme infrastructures (critiques ou non) devant être soumises à l'obligation de signaler les cyberattaques. Il serait en tout cas regrettable que les organisations soumises à l'obligation de signaler les cyberattaques ne puissent pas bénéficier du soutien du NCSC comme les autres infrastructures entrant dans la définition de l'art. 5 de la LSI. Les infrastructures critiques devraient pouvoir compter sur le soutien du NCSC et de son service technique GovCERT, dans la mesure de leurs ressources.

15 FF 2017 2824. L'art. 10 al. 2 LSI ne mentionne que « les autorités soumises à la présente loi », contrairement à l'art. 10 al. 1 LSI qui prévoit « les autorités et organisations soumises à la présente loi ». Les « autorités » sont celles énumérées à l'art. 2 al. 1 alors que les « organisations » le sont à l'art. 2 al. 2 LSI.

16 FF 2017 2824 s.

17 FF 2017 2787.

[11] La LSI prévoyait que les organisations de droit public ou privé exploitant des infrastructures critiques sans être visées par l'art. 2 al. 1 à 3 LSI n'étaient soumises qu'aux art. 74 à 80 LSI, contenant des dispositions spécifiques aux infrastructures critiques, sous réserve évidemment de législation spéciale. L'AP-LSI2 modifie sensiblement ces dispositions et propose de soumettre ces exploitants aux art. 73a à 79 AP-LSI2. Les art. 73 a à 73c et 75 à 79 AP-LSI2 concernant davantage les compétences du NCSC, ce sont donc surtout les art. 74a ss AP-LSI2 concernant l'obligation de signalement qui seront pertinents.

[12] Il n'est pas prévu aujourd'hui de les soumettre à d'autres dispositions de la LSI. Il peut être étonnant que ces organisations soient considérées comme suffisamment critiques pour être soumises à une obligation de signalement, mais pas pour être soumises aux mesures de protection des art. 6 ss LSI. Bien que plusieurs secteurs critiques disposent, de manière disparate, d'exigences minimales de cybersécurité, ces exigences ne sont aujourd'hui pas applicables à tous les exploitants d'infrastructure critique. Une base légale *ad hoc* est prévue pour le secteur de l'approvisionnement en électricité dans le cadre de la révision de la LSI,[18] mais un tel besoin existe vraisemblablement aussi pour d'autres secteurs et sous-secteurs critiques ne bénéficiant pas du même niveau d'exigences réglementaires. À notre avis, la LSI pourrait servir de fondement pour harmoniser les exigences minimales de cybersécurité pour les secteurs critiques, par exemple en prévoyant qu'elle s'applique plus largement à ceux-ci (au moins les art. 6 à 10 LSI), à condition encore que la conformité des exploitants d'infrastructures critiques à ces mesures puisse être contrôlée périodiquement à l'aune de l'état des connaissances scientifiques et techniques. Cela n'empêcherait par ailleurs pas les secteurs et sous-secteurs critiques de développer des mesures précises selon leurs besoins et spécificités.[19]

III. Contenu

1. Cadre en matière de protection contre les cyberrisques

[13] La LSI comprend les aspects réglementaires les plus importants en termes de sécurité de l'information et, partant, de cybersécurité en Suisse. Elle pose les définitions principales du domaine (reprises de l'OPCy[20] et partiellement revues), à l'instar des notions de moyen informatique, de cyberincident et cyberattaque ou encore d'infrastructure critique (art. 5 LSI, art. 5 AP-LSI2). La LSI pose ensuite les exigences minimales en matière de protection de l'information (art. 6 à 26 LSI), applicables aux autorités et organisations soumises à la loi devant prendre des mesures de protection de différents niveaux (au niveau informatique, physique et informationnel). Ayant une portée relativement large en ce qu'il en va de la protection de l'information, la loi règle les contrôles de sécurité relatifs aux personnes et les procédures de sécurité relatives aux entreprises avec ses art. 27 à 72.

18 Art. 8a LApEl ; NCSC (n. 8), p. 26 s.

19 Dans la mesure où les autorités cantonales et communales sont considérées comme des infrastructures critiques, le fait que la Confédération puisse leur confier des obligations soulève des questions constitutionnelles, FF 2017 2787. Néanmoins, l'art. 74b lit. b AP-LSI2 leur imposant déjà l'obligation de signaler les cyberattaques, nous ne verrions pas d'inconvénient à les soumettre aux principes des art. 6 à 10 LSI.

20 L'OPCy devrait être abrogée avec l'entrée en vigueur de la LSI et de ses ordonnances.

2. Mesures générales de sécurité

a. Remarque introductive

[14] Les autorités et organisations soumises à la LSI devront, dans une mesure variable, prendre les mesures permettant d'assurer la sécurité des informations qu'elles traitent. Par sa fonction de base en matière de cybersécurité et de sécurité de l'information, il semble cohérent que la LSI impose aux entités auxquelles elle s'applique les mesures générales à prendre pour assurer la sécurité de l'information. Les dispositions relatives à ces mesures se divisent entre les principes les gouvernant (art. 6 à 10 LSI), la classification des informations (art. 11 à 15 LSI), les mesures de sécurité des moyens informatiques (art. 16 à 19 LSI), les mesures relatives aux personnes (art. 20 s. LSI), les mesures de protection physique (art. 22 s. LSI) et les dispositions relatives aux systèmes de gestion de données d'identification (art. 24 à 26 LSI).

b. Les principes

[15] La sécurité de l'information se compose de quatre éléments : la *confidentialité*, la *disponibilité*, l'*intégrité* et la *traçabilité* des informations (art. 6 al. 2 LSI).[21] Les autorités et organisations soumises à la loi devront, pour assurer ces éléments, évaluer leur besoin de protection (art. 6 al. 1 LSI) et veiller à la protection de leurs moyens informatiques contre des utilisations abusives et perturbations (art. 6 al. 3 LSI).

[16] Les autorités, responsables de la sécurité des informations qu'elles traitent et des systèmes informatiques qu'elles exploitent, devront fixer leurs objectifs, les principes de gestion de risques ainsi que les conséquences d'une violation des prescriptions en veillant à ce que la sécurité de l'information soit, dans leur domaine de compétence, organisée, mise en œuvre et contrôlée conformément à l'état des connaissances scientifiques et techniques (art. 7 LSI).[22]

[17] La gestion des risques est centrale à l'établissement de la responsabilité propre à chaque autorité et organisation (art. 8 LSI). Avec l'entrée en vigueur de la LSI, elle impliquera tout d'abord l'évaluation des risques, dans leur domaine de compétence, en matière de sécurité de l'information. Ensuite, la gestion de risques impliquera pour les autorités et organisations la mise en place des mesures nécessaires pour éliminer les risques ou les ramener à un niveau acceptable. Finalement, les risques acceptables devront être formellement acceptés et supportés.[23]

[18] Lorsqu'une entité soumise à la LSI contracte ou collabore avec des tiers, les exigences et mesures prévues par la LSI devront être reprises dans les accords liant les parties et contrôlées de manière adéquate (art. 9 LSI).[24]

[19] Parallèlement, les autorités et organisations devront, sur la base de l'art. 10 al. 1 LSI, veiller à détecter rapidement les violations de la sécurité de l'information, clarifier leurs causes et réduire autant que possible leurs conséquences. L'art. 10 al. 2 LSI prévoit que les autorités doivent réagir à un incident sur la base d'un plan d'action établi préalablement dans l'éventualité de graves violations de la sécurité de l'information susceptibles de menacer l'accomplissement de tâches

21 Pour plus d'informations sur les mesures générales de sécurité, voir FF 2017 2827 ss.

22 En s'inspirant notamment des standards internationaux, FF 2017 2829.

23 FF 2017 2830.

24 Ce qui se justifie particulièrement pour les autorités fédérales qui ont souvent besoin de déléguer certaines tâches, FF 2017 2831.

indispensables de la Confédération. Elles devront organiser des exercices afin de préparer au mieux l'application de ces plans d'action.[25]

[20] À noter qu'en parallèle de l'obligation de respecter ces principes, les exploitants d'infrastructures critiques considérées comme autorités et organisations au sens de la LSI demeureront soumis à leurs obligations parallèles de se conformer aux autres lois leur étant spécifiquement applicables, à l'instar pour les fournisseurs de services de télécommunication des exigences de cybersécurité contenues par exemple à l'art. 48a de la Loi sur les télécommunications (LTC)[26], pour les gestionnaires de réseau, producteurs et agents de stockage dans l'approvisionnement électrique du pays de l'art. 8a de la Loi sur l'approvisionnement en électricité (LApEl)[27], ou encore, pour le secteur financier, des circulaires et autres normes édictées par l'Autorité fédérale de surveillance des marchés financiers (finma).

c. Classification des informations

[21] Parmi les mesures à prendre afin d'assurer la sécurité de l'information, il convient déjà pour les autorités et organisations soumises à la loi de veiller à classifier les informations susceptibles de nuire aux intérêts publics de l'art. 1 al. 2 LSI. La classification de la LSI se base sur le système de classification mis préalablement en place par l'OPrI (art. 4 ss), prévoyant les échelons « secret », « confidentiel » et « interne » selon la possible mise en danger des intérêts poursuivis par la LSI (art. 1 LSI).[28] Les conséquences de cette classification ne ressortent malheureusement pas clairement de la LSI, bien qu'il semblerait principalement s'agir de conséquences sur le niveau de protection des moyens informatiques exploités pour le traitement de ces informations. Les autorités devront désigner les personnes et services compétents pour classifier lesdites informations (auteurs de la classification) selon l'art. 12 LSI. Seules pourront accéder à ces informations les personnes offrant les garanties d'un traitement correct qui en ont besoin pour accomplir une tâche légale ou qui disposent d'une autorisation d'accès conférée contractuellement et nécessitent ces informations pour accomplir une tâche confiée (art. 14 LSI). À noter que le droit de procédure applicable prime lors d'accès à des informations classifiées auprès de l'Assemblée fédérale, des Services du Parlement, des tribunaux et des ministères publics (art. 15 LSI).[29]

[22] D'autres schémas sont régulièrement utilisés sur le plan international, comme le *Traffic Light Protocol* (*TLP*)[30], qui indique avec qui les informations peuvent être transmises.[31] Bien que ces

25 FF 2017 2831.

26 RS 784.10.

27 RS 734.7.

28 Conseil fédéral, Rapport « Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense » en réponse aux postulats Dobler 19.3135 « Acquisitions de l'armée. Avons-nous la maîtrise de la cybersécurité ? » et 19.3136 « Infrastructures critiques. Avons-nous la maîtrise des composants matériels et logiciels ? » du 18 mars 2019, 24 novembre 2021, p. 14.

29 Pour plus d'informations sur la classification des informations, FF 2017 2832 ss.

30 Forum of Incident Response and Security Teams FIRST, Traffic Light Protocol (TLP), FIRST Standards Definitions and Usage Guidance, version 2.0, https://www.first.org/tlp/ (consulté le 18 août 2022).

31 FF 2017 2873. Rouge (TLP RED) pour les informations exclusivement destinées à ses destinataires directs, Orange (TLP AMBER) pour les informations destinées aux membres de l'organisation mais qui peuvent être partagées avec des clients ou des usagers qui ont besoin de connaître ces informations pour se protéger ou prévenir d'autres dommages, Vert (TLP GREEN) pour les informations destinées à une communauté, mais non vouées à être diffusées largement et Blanc (TLP WHITE) pour les informations libres de diffusion (sous réserve d'autres limitations comme le droit d'auteur).

schémas ne semblent pas poursuivre les mêmes objectifs, la LSI aurait pu prendre le *TLP* en compte, afin d'éviter d'avoir deux systèmes qui cohabitent en pratique sans être légalement harmonisés.

d. Sécurité des moyens informatiques

[23] L'utilisation des systèmes informatiques devra également être sécurisée par les autorités soumises à la LSI (art. 16 à 19 LSI). Ces exigences de sécurité sont aujourd'hui déjà partiellement exigées par les directives internes de l'administration fédérale, par exemple les directives informatiques du NCSC relatives aux procédures de sécurité dans l'administration fédérale.[32] Les dispositions se basent sur les catégories de sécurité « protection de base », « protection élevée » et « protection très élevée » pour établir les besoins de moyens informatiques et élaborer les procédures de sécurité (art. 17 LSI).[33] Celles-ci définissent en particulier les critères permettant d'évaluer le besoin de protection des informations avant la mise en service des moyens informatiques, les modalités de mise en œuvre et le contrôle des mesures de sécurité, la compétence d'autoriser les moyens informatiques et la procédure à suivre lorsqu'un risque est modifié (art. 16 al. 2 LSI).

[24] En outre, les autorités devront fixer les exigences applicables aux catégories de sécurité de l'art. 17 en respectant dans tous les cas la « protection de base » (art. 18 al. 1 et 2 LSI) et en contrôlant périodiquement les moyens informatiques de la catégorie « protection très élevée » en vertu de l'art. 18 al. 3 LSI.[34]

[25] Finalement, les autorités et organisations devront naturellement garantir la sécurité des moyens informatiques exploités (art. 19 al. 1 LSI). L'art. 19 al. 2 LSI renvoie pour le surplus aux art. 57i ss LOGA lorsqu'il en va du traitement de données personnelles.[35]

e. Accès aux informations

[26] Les personnes pouvant accéder aux informations, moyens informatiques, locaux et autres infrastructures de la Confédération devront être choisies soigneusement par les autorités et organisations soumises à la loi, identifiées en fonction de la sensibilité de l'activité concernée, soumises si nécessaire au secret et elles devront suivre des formations adaptées à leurs responsabilités (art. 20 al. 1 LSI). De surcroît, seules les personnes nécessitant des informations pour accomplir leurs tâches pourront recevoir des autorisations d'accès, qui devront être retirées lorsqu'elles ne sont plus nécessaires ou que des indices concrets laissent à penser que la sécurité est menacée (art. 21 LSI).[36]

[27] Les autorités sont autorisées à exploiter des systèmes de gestion de données d'identification afin d'identifier les personnes ayant accès aux informations, aux moyens informatiques, aux locaux et autres infrastructures. Elles devront désigner un service responsable pour chaque système (art. 24 al. 1 et 3 LSI). Ces systèmes permettent l'échange de données et leur harmonisation avec

---

32 Voir notamment Centre national pour la cybersécurité (NCSC), Si001 – Protection informatique de base dans l'administration fédérale, version 5.0, 1er mars 2022.

33 FF 2017 2838 s.

34 FF 2017 2840.

35 FF 2017 2840 s.

36 FF 2017 2841 s.

les systèmes d'information raccordés, les répertoires de personnes et d'utilisateurs ainsi qu'avec d'autres systèmes de gestion de données d'identification exploités par des autorités soumises à la LSI (art. 25 LSI).

[28] Outre les personnes susceptibles de chercher l'accès à ces informations dans le cadre de leurs fonctions, le public a droit de requérir l'accès à ces informations sur la base du principe de transparence de l'État et en vertu de la Loi sur la transparence (LTrans)[37], loi primant par ailleurs la LSI (art. 4 al. 1 LSI). La classification d'une information n'impliquera pas que cette dernière échappe au devoir de transparence de l'État, mais sa classification est un indice sur l'intérêt de l'État à ne pas la publier.[38]

[29] Les autorités seront compétentes pour édicter des dispositions d'exécution lorsqu'il en va de la protection et de la sécurité des données, des données personnelles traitées, de l'échange et de l'harmonisation des données avec d'autres systèmes, de la journalisation et de la transmission des données de journalisation aux systèmes d'information raccordés pour vérifier les autorisations ainsi que du contrôle périodique externe du traitement de données personnelles (art. 26 LSI).

f. Protection physique

[30] Les informations et moyens informatiques respectivement traités et exploités par les autorités et organisations soumises à la LSI devront être protégés physiquement contre les utilisations et les perturbations comme le vandalisme, le vol ou encore les dommages naturels comme certaines inondations ou certains incendies (art. 22 LSI).[39] Pour ce faire, celles-ci devront instituer des zones de sécurité dans les locaux et espaces où sont fréquemment traitées des informations confidentielles et secrètes ou exploités des moyens informatiques de catégories « protection élevée » ou « protection très élevée » (art. 23 al. 1 LSI). Les autorités et organisations pourront prendre des mesures telles que la surveillance de secteurs sensibles ou la réalisation de contrôles inopinés dans ces locaux. À noter que ces mesures sont déjà partiellement appliquées au sein de la Confédération.[40]

3. Contrôles relatifs aux personnes et procédures de sécurité au sein des entreprises

[31] Les art. 27 à 73 LSI fournissent la base légale formelle pour les contrôles et procédures de sécurité, les art. 27 à 48 prévoyant le contrôle de sécurité relatif aux personnes et les art. 49 à 73 concernant les procédures de sécurité relatives aux entreprises.[41]

[32] Le contrôle de sécurité relatif aux personnes poursuit l'objectif de déterminer si l'exercice d'une activité sensible par une personne dans sa fonction ou dans son mandat constitue un risque pour la sécurité de l'information (art. 27 al. 1 LSI). Ce contrôle est déjà prévu par plusieurs ordon-

37 RS 152.3.

38 FF 2017 2788.

39 FF 2017 2842 s.

40 FF 2017 2843.

41 Pour plus d'informations au sujet des contrôles de sécurité relatifs aux personnes et des procédures de sécurité relatives aux entreprises, FF 2017 2846 ss.

nances[42], mais la LSI servira de base légale formelle permettant de réviser ces ordonnances, du moins l'Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP)[43].[44] Il conviendra donc de voir si l'ordonnance relative à la LSI aura pour conséquence l'abrogation des ordonnances préexistantes au sujet de cette question.

[33] La procédure de sécurité relative aux entreprises tendra à la préservation de la sécurité de l'information lorsque des entreprises, des parties d'entreprises ou des entreprises sous-contractantes exécutent des mandats publics impliquant l'exercice d'une activité sensible (dits mandats sensibles en vertu de l'art. 49 LSI).

4. Infrastructures critiques

[34] Le chapitre sur les infrastructures critiques (chapitre 5, art. 74 à 80 LSI) prévoyait initialement dans les grandes lignes du premier projet les tâches de la Confédération en lien avec le soutien fourni aux exploitants d'infrastructures critiques en Suisse ainsi que les traitements de données personnelles y relatifs.[45] Ce chapitre de la loi a été revu dans le cadre de l'introduction de l'obligation de signaler les cyberattaques pour les infrastructures critiques, dans la mesure où cette obligation contribuera à certains changements et, qu'entre les deux projets, le NCSC a été créé et devait pouvoir, selon toute logique, fonder ses compétences sur la LSI qui devrait reprendre, à terme, l'OPCy (qui prévoyait de manière plus générale les compétences de ce dernier à son art. 12).

IV. Les deux grandes nouveautés

1. Centre national pour la cybersécurité comme autorité de référence

a. Compétences

[35] Le Centre national pour la cybersécurité (NCSC), en voie de devenir un office fédéral, est l'autorité principale en matière de cybersécurité (l'un des trois domaines de la protection de la Suisse contre les cyberrisques).[46] Ses compétences dans le domaine seront prévues au chapitre 5 de la loi.[47]

[36] Le NCSC sera d'abord compétent pour la sensibilisation du public quant aux cyberrisques. Il mettra en garde contre les cyberrisques et vulnérabilités pouvant impacter les moyens informatiques. C'est aussi à lui que reviendra la compétence de publier des informations et instructions en

42 Voir *supra* n. 2.

43 RS 120.4.

44 Conseil fédéral (n. 28), p. 15.

45 FF 2017 2869 ss.

46 Conseil fédéral, Plan de mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022, p. 5 ; Communiqué du Conseil fédéral et du Secrétariat général du Département fédéral des Finances, Le Centre national pour la cybersécurité deviendra un office fédéral, Berne 18 mai 2022, https ://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/medienmitteilungen/newslist.msg-id-88878.html (consulté le 18 août 2022).

47 NCSC (n. 9), p. 14. L'art. 73a AP-LSI2 contient une liste non exhaustive de ses compétences, étendue par les art. 73b ss de la loi.

matière de cybersécurité et protection contre les cyberrisques, ainsi que de mener, avec ses unités internes, les analyses techniques visant à évaluer et écarter les cyberrisques (art. 73a AP-LSI2).

[37] Il recevra et traitera ensuite les signalements de cyberincidents et de vulnérabilités en vertu de l'art. 73b AP-LSI2 (le traitement des cyberattaques est réglé aux art. 74a ss AP-LSI2).[48] Tout un chacun peut signaler des cyberincidents ou vulnérabilités découvertes ; il s'agit d'une faculté et non d'une obligation. Tout d'abord, le NCSC analysera ces signalements à des fins statistiques. Il émettra une recommandation si la situation ne nécessite pas d'analyses ou clarifications supplémentaires.[49] Ensuite, il pourra partager des données à ce sujet avec les autorités et organisations intéressées pour prévenir les cyberattaques. Ces données peuvent constituer des données personnelles, typiquement s'il s'agit de ressources d'adressage ou de caractères d'identification, à condition que la personne concernée y consente. Finalement, il informera les fabricants et leur fixera un délai pour remédier à la vulnérabilité ; si les fabricants n'agissent pas, le NCSC publiera la vulnérabilité et le logiciel ou matériel concerné si cela contribue à la protection contre les cyberrisques (art. 73b AP-LSI2).[50]

[38] Finalement, le NCSC soutiendra les exploitants d'infrastructures critiques dans leur lutte contre les cyberrisques. Pour ce faire, il leur mettra à disposition des instruments, dont un système de communication sécurisé, des informations techniques sur les cyberrisques, les vulnérabilités et des recommandations sur les mesures de prévention ainsi que des outils techniques et instructions de détection des cyberincidents (art. 74 al. 2 AP-LSI2). Parallèlement, le NCSC les soutiendra par des conseils techniques dans la gestion de cyberincidents et la correction de vulnérabilités engendrant un risque imminent de conséquences graves pour l'infrastructure critique. S'il s'agit d'un exploitant privé, il faudra encore que ce dernier ne puisse pas obtenir un soutien équivalent en temps utile sur le marché (art. 74 al. 3 AP-LSI2).[51] Ces prestations de soutien seront vraisemblablement limitées, du moins dans un premier temps, au cercle des exploitants d'infrastructures critiques.

b. Traitements et échanges d'informations

[39] Le NCSC va naturellement traiter des données dans le cadre de ses fonctions. Dans ce cadre, plusieurs dispositions du chapitre 5 peuvent trouver application, dont principalement les art. 73c et 75 à 79 AP-LSI2.

[40] Les données traitées et partagées ou reçues peuvent être constitutives de données techniques, à l'instar des indicateurs de compromission (*Indicator of Compromise*, IoC), des codes informatiques (malveillants) ou encore des modes opératoires.[52] Il faut veiller à ce que les informations susceptibles de présenter un risque pour l'un des intérêts de l'art. 1 al. 2 LSI soient correctement classifiées selon le risque potentiellement engendré.

48 Cf. *infra* IV.2.

49 Bien que nous comprenions que l'étendue de l'intervention du NCSC dépend de ses ressources, nous regrettons la possible limitation induite par la formulation légale.

50 NCSC (n. 9), p. 14 s. Nous préconiserions une formulation permettant de déduire expressément une obligation imposée aux fabricantes.

51 NCSC (n. 9), p. 16.

52 FF 2017 2871.

[41] En outre, il faut être attentif au fait que bien des données sont couvertes par des secrets (principalement par le secret de fonction). L'art. 73c al. 4 AP-LSI2 renvoie expressément à l'art. 320 CP pour les exigences à respecter par le NCSC lorsqu'une communication de données secrètes est envisagée, ce qui pourrait se produire lors de communications au Service de renseignement de la Confédération (SRC) ou aux autorités de poursuite pénale.[53] Dans l'autre sens et dans le cadre du soutien qu'il apporte aux exploitants d'infrastructures critiques, l'art. 74 al. 4 AP-LSI2 lui permettra d'accéder à leurs moyens informatiques moyennant leur accord malgré des obligations légales ou contractuelles de confidentialité.[54]

[42] Les informations traitées et partagées par le NCSC peuvent aussi constituer des données personnelles, voire sensibles (art. 5 lit. a et c de la loi fédérale sur la protection des données, LPD).[55] Les traitements de données personnelles effectués par le NCSC seront prévus aux art. 75 à 79 AP-LSI2. Ces dispositions prévoiront pour le NCSC la possibilité de traiter des données personnelles et certaines données sensibles. Bien qu'il s'agisse en pratique principalement de ressources d'adressage, qui peuvent contenir des informations relatives à des opinions religieuses ou politiques ou encore relatives à des poursuites ou sanctions pénales ou administratives, la loi ne limite pas les traitements de données personnelles du NCSC à ces ressources (art. 75 al. 1 AP-LSI2).

[43] Le NCSC pourra communiquer des informations sur la base de l'art. 73c AP-LSI2. Principalement, il transmettra les informations concernées au SRC dans le cas où le signalement d'un cyberincident ou son analyse révèlent des informations servant à l'art. 6 al. 1 lit. a, al. 2 et al. 5 de la Loi fédérale sur le renseignement (LRens).[56] Ces données sont pertinentes pour déceler à temps et prévenir les menaces contre la sécurité intérieure ou extérieure, pour évaluer le niveau de menace ou pour assurer un service d'alerte précoce dans le renseignement pour protéger les infrastructures critiques (art. 6 al. 1 lit. a, al. 2 et al. 5 LRens par renvoi de l'art. 73c al. 1 LSI). Parallèlement, le NCSC pourra également dénoncer une infraction éventuelle découverte dans l'exercice de ses fonctions si cela lui semble approprié au vu de sa gravité. Il n'y est cependant pas obligé, l'obligation de dénoncer de l'art. 22a de la loi sur le personnel de la Confédération (LPers)[57] s'opposant à l'exigence de confidentialité du signalement.[58]

[44] Il semblerait que l'art. 76a AP-LSI2 reprenne ce concept de coopération entre le NCSC, le SRC et les autorités de poursuite pénale. L'assistance technique prévue par cette disposition et fournie par le NCSC aux autorités précitées se traduit par une procédure d'appel. Partant, il conviendrait que la loi en prévoie les conditions précises. Il est possible que ces conditions soient celles de l'art. 73a, respectivement al. 2 pour le SRC et al. 3 pour les autorités de poursuite pénale.[59] Cela n'est pas très clair et devrait être mieux défini. De plus, la formulation très large de l'art. 6 LRens risque d'impliquer une obligation étendue de communication du NCSC au SRC. Le NCSC pourrait de ce fait se trouver dans un conflit entre son obligation d'assister le SRC en lui fournissant

53 NCSC (n. 9), p. 15.

54 NCSC (n. 9), p. 16. La LSI ne prévoit en revanche pas le partage d'informations des autorités de poursuite pénale ou du SRC au NCSC, ce qui devrait être prévu dans les lois et ordonnances régissant les communications de données de ces entités.

55 RS 235.1.

56 RS 121.

57 RS 172.220.1.

58 NCSC (n. 9), p. 15.

59 NCSC (n. 9), p. 25.

des informations susceptibles de lui servir de près ou de loin dans son activité et les obligations de confidentialité qui lient le NCSC envers ceux qui lui fournissent des informations. À terme, cela pourrait même dissuader la communication d'informations au NCSC.

[45] L'assistance du NCSC devrait aussi bénéficier d'une certaine réciprocité des autorités concernées, notamment dans la possibilité pour ce dernier de recevoir certaines informations lui permettant d'accomplir sa tâche. Il faudrait donc adapter également la législation sur les bases de données du SRC et des autorités de poursuite pénale pour que le NCSC puisse, à certaines conditions, recevoir les informations utiles à sa mission.

[46] Outre ces différentes communications, le NCSC sera également habilité à recevoir comme à transmettre des données personnelles dans le cadre de la coopération sur les plans national et international (art. 76 et 77 AP-LSI2). Sur le plan national, cette coopération liant le NCSC aux exploitants d'infrastructures critiques ou fournisseurs de services de télécommunication peut par exemple permettre au NCSC de requérir de la part d'un hébergeur dont un serveur permet un réseau de machines zombies les adresses IP des ordinateurs infectés. Le NCSC pourra par la suite remettre ces fichiers aux fournisseurs de services de télécommunication afin que ces derniers puissent alerter leurs clients. Sur le plan international, ces ressources d'adressage seront susceptibles d'être échangées avec des partenaires du NCSC, de même que des recommandations de sécurité, des analyses d'incidents ou encore des éléments d'appréciation des menaces.[60]

2. Obligation de signaler les cyberattaques contre les infrastructures critiques

a. *Ratio legis*

[47] La révision de la LSI a été lancée principalement pour introduire une obligation de signaler les cyberattaques visant les infrastructures critiques. Cette obligation a été réfléchie depuis plusieurs années, faisant notamment suite à un postulat et aux exigences de stratégies nationales.[61] Plusieurs modèles ont été examinés et celui finalement retenu a été celui d'un signalement obligatoire à la centrale d'enregistrement du NCSC, qui remplacera l'échange actuellement effectué sur une simple base volontaire et s'ajoutera aux autres obligations parallèles de signalement.[62] À l'origine, cette obligation concernait tant les cyberattaques que les cyberincidents. Au fil du temps, les cyberincidents ont été complètement écartés de cette obligation, à tort à notre avis.

[48] L'implémentation de cette obligation poursuit plusieurs objectifs de sécurité nationale. Les infrastructures critiques constituent l'un des principaux groupes cibles sur lesquels un accent doit être mis lorsque l'on parle de protection de la Suisse contre les cyberrisques.[63] Le signalement de cyberattaques va d'une part permettre au NCSC de comprendre et dresser un tableau plus

60 FF 2017 2872–2874.

61 Voir Conseil fédéral, Obligation de déclarer les incidents graves affectant la sécurité des infrastructures critiques : solutions possibles, Rapport du Conseil fédéral en réponse au postulat 17.347 Graf-Litscher du 15 juin 2017, 13 décembre 2019, p. 4 s, où référence est faite au Postulat 17.3475 Graf-Litscher « Infrastructures critiques. Prévoir une obligation de signaler les incidents graves de sécurité », à la mesure 9 de la SNPC 2018–2022, à la mesure 8 de la Stratégie nationale pour la protection des infrastructures critiques et à la recommandation 28 « Obligation de notifier » du rapport du groupe d'experts concernant le traitement et la sécurité des données.

62 NCSC (n. 9), p. 5.

63 NCSC (n. 9), p. 15.

complet des modes opératoires employés par des acteurs malveillants.[64] D'autre part, il pourra sur cette base avertir les personnes potentiellement lésées et leur transmettre des recommandations sur les mesures de sécurité s'imposant, tant de manières réactive que préventive (art. 74a AP-LSI2).

b. Qui doit signaler ?

[49] L'art. 74b AP-LSI2 prévoit de lister les catégories d'organisations et autorités soumises à l'obligation de signaler au NCSC les cyberattaques. Comme déjà soulevé, la notion d'infrastructure critique n'est pas claire. Néanmoins, la liste de l'art. 74b AP-LSI2 énumérant les infrastructures soumises à l'obligation de signaler les cyberattaques dont elles sont victimes nous semble exhaustive.[65]

[50] La liste de l'art. 74b sera en principe sujette aux exceptions de l'art. 74c, prévoyant les catégories d'exploitants d'infrastructures critiques que le Conseil fédéral exemptera si les défaillances ou dysfonctionnements provoqués par des cyberattaques contre leurs infrastructures sont peu probables (en raison typiquement d'une faible dépendance aux moyens informatiques), si ces dysfonctionnements n'ont qu'un impact limité sur le bien-être de la population et/ou le fonctionnement de l'économie car ne concernent qu'un petit nombre de personnes, sont suppléés par d'autres infrastructures critiques ou ne présentent qu'un faible potentiel de dommages économiques (art. 74c AP-LSI2). En d'autres termes, il s'agira des entreprises qui, individuellement, ne sont pas considérées comme critiques ou essentielles au bien-être de la population ou au bon fonctionnement de l'économie suisse.[66]

c. Quels évènements doivent être signalés ?

[51] Les exploitants d'infrastructures critiques de la liste de l'art. 74b AP-LSI2 non exonérés de cette obligation en vertu de l'art. 74c AP-LSI2 ne devraient pas signaler toute cyberattaque dont ils sont victimes. Selon l'art. 74d de la loi, ils ne devraient signaler au NCSC que les cyberattaques dont des indices laissent présumer :

- qu'elles mettent en péril le bon fonctionnement de l'infrastructure critique touchée ou d'une autre infrastructure critique ;
- qu'elles ont été exécutées avec le concours d'un État étranger ;[67]
- qu'elles ont entraîné ou pourraient entraîner une fuite ou la manipulation d'informations ;
- qu'elles sont passées inaperçues pendant plus de 30 jours ;

64 NCSC (n. 9), p. 5.

65 En relation avec la liste des secteurs et sous-secteurs critiques de la Stratégie nationale pour la protection des infrastructures critiques 2018–2022, FF 2018 499 s. Pour plus d'informations au sujet du cercle d'assujettis, voir NCSC (n. 9), pp. 17–20.

66 NCSC (n. 9), p. 21.

67 Interprétation reprise par les auteurs, la loi se limitant, à tort, à mentionner l'attaque « exécutée par un État étranger ou à son instigation », formulation jugée par la présente trop restrictive.

- qu'elles ont été accompagnées d'actes de chantage, de menace ou de contrainte à l'encontre de l'exploitant de l'infrastructure critique ou de ses collaborateurs.[68] Ce cas de figure renvoie principalement aux ransomwares, dont l'utilisation est aujourd'hui récurrente et peut engendrer des conséquences dramatiques.[69]

d. Quoi et comment signaler ?

[52] Le signalement devrait contenir les informations principales au sujet de la cyberattaque, à savoir quelle est l'infrastructure critique visée, quel est le type de cyberattaque perpétrée, comment elle s'est déroulée, quelles sont ses conséquences et quelles sont les mesures que compte prendre ou a pris l'exploitant de l'infrastructure touchée. Il pourra normalement transmettre ces informations de manière échelonnée s'il ne dispose pas de l'entier de ces dernières au moment du signalement (art. 74eAP-LSI2). Cette précision tient compte du fait qu'une cyberattaque n'est pas toujours tout de suite détectée.[70]

[53] Outre ces informations, les exploitants d'infrastructures critiques soumis à cette obligation de signaler les cyberattaques devront fournir au NCSC tous les renseignements prévus à l'art. 74g AP-LSI2. Cette disposition leur imposera de fournir au NCSC les informations complémentaires sur le contenu du signalement que ce dernier nécessiterait pour remplir ses tâches comme l'identification des modes opératoires ou la prévention de répercussions ou de nouvelles attaques contre d'autres infrastructures critiques.

[54] En principe, les informations transmises par l'exploitant vont être préjudiciables pour un tiers malveillant. Néanmoins, afin de prévenir le conflit d'intérêts dans lequel un exploitant, ayant un comportement à se reprocher, ne souhaiterait pas respecter son obligation de signalement, le principe *nemo tenetur*, illustré à l'art. 73c al. 3 AP-LSI2, devrait s'appliquer aux signalements obligatoires de cyberattaques en prévoyant que les informations communiquées par l'exploitant ne peuvent être utilisées contre lui dans le cadre d'une procédure pénale qu'avec son accord.[71]

[55] Dans la mesure où il est possible qu'un exploitant ait plusieurs signalements et annonces à faire à diverses autorités, le NCSC mettra vraisemblablement à disposition un système sécurisé que celui-ci peut, mais ne doit pas, utiliser (art. 74f al. 1 AP-LSI2). Ce système devrait permettre à l'exploitant d'effectuer les annonces imposées aux différentes autorités compétentes.[72] Ce système permettrait par exemple à l'établissement financier victime d'un ransomware ayant chiffré et dérobé des données de clients de procéder à une annonce au NCSC, au Préposé fédéral à la protection des données et à la transparence (PFPDT) et éventuellement aux personnes concernées sur la base de l'art. 24 LPD ainsi que, si les conditions sont réunies, à la finma sur la base de l'art. 29 al. 2 de la Loi sur l'Autorité fédérale de surveillance des marchés financiers (LFINMA).[73]

---

68 Les auteurs estiment que la limitation de ces actes à l'encontre soit de l'exploitant d'infrastructure critique ou de ses collaborateurs semble trop restrictive.

69 NCSC, Rapport semestriel 2021/II (juillet – décembre), Sécurité de l'information, Situation en Suisse et sur le plan international, 5 mai 2022, p. 18.

70 NCSC (n. 9), p. 21.

71 Et ce bien que la disposition prévoyant l'application de *nemo tenetur* ne figure pas dans la section relative à l'obligation de signaler les cyberattaques, NCSC (n. 9), p. 15. Une règle analogue est posée en droit de la protection des données personnelles à l'art. 24 al. 6 nLPD en cas d'annonces de violations de la sécurité des données.

72 NCSC (n. 9), p. 21 s.

73 RS 956.1.

[56] Ce système, bien que prometteur, pose de nombreux défis, notamment techniques. Tout d'abord, les silos servant à différencier les informations transmises aux diverses autorités sont difficiles à mettre en place. Ensuite, plusieurs signalements risquent de devoir être faits, ce qui n'allégerait que peu la tâche des exploitants d'infrastructures critiques. Il peut finalement être délicat à l'heure actuelle d'implémenter une méthode assurant que le NCSC, hébergeant le système, n'a pas d'accès aux informations destinées à d'autres autorités.

e. Non-respect de l'obligation

[57] Le NCSC informera l'exploitant de l'infrastructure critique si des indices laissent présumer que ce dernier n'a pas rempli son obligation de signalement ou de transmission de renseignements. Si l'exploitant ne remplit toujours pas son obligation, malgré l'information du NCSC, et ne fournit pas toutes les informations requises par les art. 74e et 74g AP-LSI2, ce dernier lui fixera un délai en la menaçant d'une amende. L'exploitant s'obstinant à ne pas remplir son obligation pourra être condamné, par suite de cela, à une amende allant jusqu'à CHF 100 000.–. L'art. 74i AP-LSI2 prévoit les modalités concernant cette peine.[74]

V. Conclusion

[58] La Loi sur la sécurité de l'information (LSI) reprendra les éléments contenus jusqu'à présent dans certaines ordonnances, mais elle permettra surtout d'uniformiser la sécurité de l'information au sein de la Confédération, lorsque ses moyens informatiques sont exploités ou que ses informations sont traitées par les cantons. En outre, la LSI permettra de servir de base légale pour la protection contre les cyberrisques, au-delà de la Confédération, auprès des infrastructures critiques, qui représentent aujourd'hui l'une des parties prenantes les plus importantes dans le cadre de la protection de la Suisse contre les cyberrisques. Cette loi servira de fondement principal en matière de sécurité de l'information et, sur cette base, de cybersécurité, dans la mesure où de plus en plus de traitements d'information sont informatisés et que la loi en tient compte. Source de nouvelles obligations pour divers acteurs, elle va revêtir une importance certaine en pratique. Après sa révision (AP-LSI2), cette loi servira également de base pour la nouvelle obligation de signaler les cyberattaques visant les infrastructures critiques, qui représentera une mesure importante pour mieux protéger rapidement ces infrastructures. Elle permettra en outre d'assurer aux exploitants d'infrastructures critiques qu'ils peuvent transmettre des informations au NCSC pour se protéger et au NCSC qu'il peut recevoir et traiter de telles informations à cette même fin.

[59] La loi fait son chemin dans un contexte majoritairement cyber qui évolue naturellement très rapidement. La Suisse, parfois en difficulté pour réglementer des domaines technologiques, n'a pas eu le temps de permettre l'entrée en vigueur de la LSI avant de devoir la modifier. Le champ d'application de la loi n'est à l'heure actuelle pas clair et mériterait d'intégrer de façon plus cohérente les exploitants d'infrastructures critiques. Certaines définitions ne sont toujours pas satisfaisantes, ce qui est d'autant plus important dans des domaines interdisciplinaires, où le vocabulaire est souvent source de confusion. Il est important que les parties prenantes puissent

74 NCSC (n. 9), p. 22 s.

savoir si elles doivent se considérer comme infrastructures critiques ou non et, partant, savoir si elles peuvent bénéficier du soutien du NCSC.

[60] Les partages de données ne sont pas toujours bien formulés, ce qui peut soulever un doute quant à la protection de tous les intérêts en présence. Les imprécisions de l'avant-projet montrent d'une part le retard de la Suisse par rapport à d'autres États dans l'appréhension des cyberrisques, mais, d'autre part, le fait que la SNPC concrétise le champ d'action des autorités et leur permet de s'adapter à l'évolution technologique, bien que la vitesse des processus législatifs et politiques diffère de la sienne. Les compétences du NCSC, organe capital en matière de prévention et réaction aux cyberattaques visant les infrastructures critiques en Suisse, commencent à être clarifiées, ce qui est nécessaire pour que les différentes parties prenantes, dont les exploitants d'infrastructures critiques, puissent savoir dans quelle mesure elles peuvent bénéficier du soutien du NCSC.

[61] Même si la loi manque parfois de clarté, les nouvelles sont plutôt positives et la Suisse disposera bientôt d'une vraie législation en matière de sécurité de l'information. Le processus législatif de la révision (actuellement AP-LSI2) n'étant pas terminé, il convient de rester attentif aux évolutions à venir. Il faut aussi garder un œil sur la nouvelle version de la SNPC qui démarrera en 2023. Comme on l'a vu, la protection de l'information est un domaine complexe et dynamique, et l'entrée en vigueur de la LSI ne sera ni la solution à tous les risques, ni la fin du processus.

Pauline Meyer est titulaire d'une Maîtrise universitaire en Droit en professions judiciaires et doctorante à l'Université de Lausanne. Elle y rédige sa thèse sur la gestion de cyberincidents en droit suisse, avec un accent sur les infrastructures critiques. Elle est rédactrice auprès de swissprivacy.law.

Sylvain Métille est avocat associé à l'étude HDC et Professeur associé à l'Université de Lausanne où il enseigne le droit de la protection des données et le droit pénal informatique. Il y dirige la Maîtrise universitaire en Droit, criminalité et sécurité des technologies de l'information (M DCS) et est membre de la Commission d'éthique de la recherche de l'Université (CER-UNIL). Il est également responsable scientifique du CAS Protection des données UniDistance.

Cet article est publié dans le cadre du projet de recherche FNS « L'éthique et le droit pour promouvoir la confiance en la cybersécurité » (projet PNR 77 n°197425).