Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Conseil fédéral

Ouverture de la consultation relative à l'introduction d'une obligation de signaler les cyberattaques

Berne, 12.01.2022 - Lors de sa séance du 12 janvier 2022, le Conseil fédéral a décidé d'ouvrir la procédure de consultation sur l'avant-projet de modification de la loi sur la sécurité de l'information relatif à l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques. Cet avant-projet crée les bases légales nécessaires à l'introduction de l'obligation de signalement et définit les tâches du Centre national pour la cybersécurité (NCSC), qu'il institue comme centrale de signalement des cyberattaques. La consultation durera jusqu'au 14 avril 2022.

Les cyberattaques sont devenues l'une des principales menaces pour la sécurité et l'économie de la Suisse. Chaque jour, des entreprises et des administrations sont victimes d'attaques. En moyenne, le NCSC reçoit plus de 300 annonces par semaine concernant des tentatives de cyberattaques et des cyberattaques réussies. Ces annonces sont faites sur une base volontaire par des entreprises, des autorités et des particuliers. Elles aident les autorités fédérales compétentes à évaluer le niveau de menace et à identifier les modes opératoires à un stade précoce. Le Conseil fédéral entend renforcer le système d'annonce en obligeant les exploitants d'infrastructures critiques à signaler au NCSC les cyberattaques dont ils sont victimes. L'obligation de signaler les cyberattaques vise à permettre au NCSC de dresser un tableau précis de la situation en se basant sur des informations complètes et, ainsi, d'alerter à temps les autres exploitants d'infrastructures critiques.

Obligation de signalement pour les infrastructures critiques

L'obligation de signalement pour les exploitants d'infrastructures critiques s'appliquera aux cyberattaques recelant un potentiel important de dommages. Il s'agit, en particulier, des attaques qui mettent en péril le bon fonctionnement des infrastructures critiques ou qui s'accompagnent d'actes de chantage, de menaces ou de contrainte. Le NCSC assumera le

rôle de centrale de signalement. Afin que les signalements soient aussi simples que possible à effectuer, le NCSC mettra à disposition un formulaire électronique qui permettra de saisir facilement les déclarations et, au besoin, de les transmettre directement à d'autres services.

Obligation pour la Confédération de fournir une assistance en cas de cyberattaque

L'avant-projet n'oblige pas seulement les entreprises à participer à la protection contre les cyberattaques, mais définit aussi les tâches de la Confédération en matière de soutien aux entreprises et à la population. À cette fin, le NCSC sera chargé d'avertir le public des cybermenaces et de le sensibiliser aux cyberrisques. Il aura également pour tâches de recevoir les signalements concernant les cyberincidents et les vulnérabilités, de réaliser des analyses techniques et de fournir aux entreprises à l'origine d'un signalement des recommandations sur la manière de procéder. Le NCSC soutiendra en outre les exploitants d'infrastructures critiques (qui comprennent aussi les autorités cantonales et communales) en les aidant dans la gestion des cyberincidents. Cette aide sera proposée en guise de premiers secours et ne devra pas concurrencer les prestations disponibles sur le marché.

Actuellement, la Confédération assume les tâches en matière de protection contre les cyberrisques sur la base des mandats existants, mais celles-ci ne sont pas définies au niveau de la loi. L'inscription de l'obligation de signaler les cyberattaques dans la loi sur la sécurité de l'information permettra également d'y définir les tâches du NCSC, et notamment sa compétence en tant que centrale de signalement.

La consultation sur l'avant-projet durera jusqu'au 14 avril 2022.

Adresse pour l'envoi de questions

Communication,
Département fédéral des finances DFF
no tél. +41 58 462 60 33, info@gs-efd.admin.ch

Documents

Loi (PDF, 819 kB)

Rapport explicatif (PDF, 678 kB)

Lettre aux cantons (PDF, 169 kB)

Lettre aux organisations (PDF, 166 kB)

Liste der Vernehmlassungsadressaten - Liste des destinataires - Elenco dei destinatari (PDF, 172 kB)

Auteur

Conseil fédéral
https://www.admin.ch/gov/fr/accueil.html

Département fédéral des finances
http://www.dff.admin.ch

Département fédéral de la défense, de la protection de la population et des sports
http://www.vbs.admin.ch

https://www.admin.ch/content/gov/fr/accueil/documentation/communiques.msg-id-86768.html

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Centre national pour la cybersécurité NCSC

Berne, le 12 janvier 2022

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

Table des matières

Condensé

Ces dernières années, les cyberincidents se sont multipliés, que ce soit chez les particuliers, dans les entreprises ou même au sein des autorités, avec, parfois, des conséquences graves. Le projet mis en consultation prévoit d'introduire une obligation de signaler les cyberattaques contre les infrastructures critiques. Une telle obligation permettra de détecter précocement les cyberattaques, d'analyser leur mode opératoire et d'avertir à temps les autres exploitants d'infrastructures critiques. Elle pourra ainsi apporter une contribution essentielle au renforcement de la cybersécurité de la Suisse.

Le 11 décembre 2020, le Conseil fédéral a chargé le Département fédéral des finances (DFF) d'élaborer un projet fournissant les bases légales nécessaires à l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques.

Le présent projet de consultation prévoit d'inscrire cette base légale dans la loi sur la sécurité de l'information (LSI), adoptée par le Parlement le 18 décembre 2020. Outre l'obligation de signalement, la LSI doit aussi fixer les tâches du Centre national pour la cybersécurité (NCSC) et l'établir dans sa fonction de centrale de signalement.

L'obligation de signalement ne doit s'appliquer qu'aux cyberattaques recelant un certain potentiel de dommages. Y seront soumis les exploitants d'infrastructures critiques, c'est-à-dire de processus, de systèmes et d'installations essentiels au fonctionnement de l'économie ou au bien-être de la population. Le NCSC assumera le rôle de centrale de signalement. Il réceptionnera également les signalements de cyberincidents et de vulnérabilités des moyens informatiques transmis à titre facultatif.

Rapport explicatif

1 Contexte

1.1 Nécessité d'agir et objectifs

Dans son rapport du 13 décembre 2019 en réponse au postulat «Infrastructures critiques. Prévoir une obligation de signaler les incidents graves de sécurité», le Conseil fédéral a constaté qu'il n'existait pas d'obligation de signaler les cyberincidents dont sont victimes les infrastructures critiques[1] et a chargé le Centre national pour la cybersécurité (NCSC) d'étudier la possibilité d'introduire une telle obligation.

Ce mandat d'examen reposait sur des bases solides telles que la stratégie nationale pour la protection des infrastructures critiques (stratégie PIC 2018-2022, mesure 2) et la stratégie pour la protection de la Suisse contre les cyberrisques (SNPC 2018-2022, mesure 9), ainsi que sur le rapport du groupe d'experts concernant le traitement et la sécurité des données[2]. La question d'introduire une obligation de signalement a aussi été soulevée dans le cadre des débats parlementaires concernant la révision totale de la loi sur la protection de la population et sur la protection civile (LPPCi, délibérations au Conseil national du 14 juin 2019) et dans le cadre de ceux concernant la loi sur la sécurité de l'information (LSI, débat au Conseil national du 4 juin 2020). Après un examen approfondi des bases légales possibles et, plus particulièrement, de la compétence fédérale[3], le Conseil fédéral a, le 11 décembre 2020, chargé le DFF d'élaborer jusqu'à la fin 2021 un projet de consultation prévoyant l'introduction d'une obligation de signaler les cyberattaques contre des infrastructures critiques.

Ce projet visait à clarifier qui doit signaler quels types d'attaques, quand et à qui. Lors de la clarification de ces questions, il est apparu clairement que le NCSC, créé en 2019 – et que le projet institue comme centrale de signalement des cyberattaques – ne disposait pas des bases légales nécessaires pour accomplir ses tâches de centre de compétence fédéral pour la cybersécurité conformément aux exigences du Parlement[4]. Le projet visant à introduire une obligation de signalement servira donc aussi à ancrer dans la loi les tâches et les compétences du NCSC.

1.2 Solutions examinées et solution retenue

1.2.1 Développement de l'échange d'informations à titre volontaire

En Suisse, l'échange d'informations entre les infrastructures critiques et la Confédération est bien en place. Les infrastructures critiques procèdent à des échanges depuis 2004, à l'époque avec la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), aujourd'hui avec le NCSC. Les limites de ce système se font toutefois de plus en plus ressentir. Un échange volontaire fructueux nécessite une solide relation de confiance entre toutes les parties. Pour établir une telle relation, il faut que le nombre de participants reste gérable et que ceux-ci aient la possibilité d'échanger directement de façon régulière. Dans la situation actuelle, où les cyberattaques constituent une

1 Obligation de déclarer les incidents graves affectant la sécurité des infrastructures critiques: solutions possibles. Rapport du Conseil fédéral du 13 décembre 2019 en réponse au postulat 17.3475 Graf-Litscher du 15 juin 2017

2 Rapport du groupe d'experts du 17 août 2018 concernant le traitement et la sécurité des données (recommandation 28). Le groupe d'experts a été engagé par le DFF le 27 août 2015 dans le cadre de la mise en œuvre de la motion Rechsteiner (13.3841) «Commission d'experts pour l'avenir du traitement et de la sécurité des données», pour un mandat limité à trois ans

3 Cf. rapport du 25 novembre 2020 «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen», annexe 01 au mandat du CF du 11 décembre 2020 (disponible en allemand uniquement)

4 17.3508 Mo. Eder «Création d'un centre de compétence fédéral pour la cybersécurité»

menace pour une multitude d'entreprises actives dans les secteurs critiques, il n'est plus possible de garantir qu'une confiance mutuelle suffisante anime tous les opérateurs concernés. Par conséquent, bien que le développement de l'échange d'informations des dernières années permette toujours le bon fonctionnement de la collaboration avec certaines entreprises et certaines organisations, il n'est plus réaliste d'envisager d'étendre ce modèle.

En cas de signalement, se concentrer sur un nombre réduit d'entreprises risque de donner une image incomplète, voire faussée de la situation. Il est en effet impossible de déterminer quel rayon d'action en Suisse possède une cybermenace. Par ailleurs, l'échange d'informations à titre volontaire peut constituer une incitation inopportune. Les entreprises qui n'y prennent pas part reçoivent tout de même des alertes et des indications techniques grâce aux signalements d'autres sociétés, puisque le NCSC ne peut pas priver les exploitants d'infrastructures critiques d'informations essentielles. Il peut donc sembler plus facile à certaines entreprises de se reposer sur la participation des autres pour recevoir les signalements importants plutôt que de participer activement à l'échange d'informations.

En définitive, l'introduction d'une obligation de signalement est donc préférable à la poursuite de l'échange facultatif d'informations: elle assure une vue d'ensemble plus complète de la situation et garantit qu'aucun opérateur ne se soustraie à l'obligation d'avertir les autres de tout incident ou danger. Il s'agira néanmoins d'entretenir la culture de la collaboration née de l'échange d'informations, ainsi que la confiance mutuelle. Pour y parvenir, il faut aussi que l'introduction de l'obligation de signalement apporte une plus-value aux entreprises et aux organisations.

1.2.2 Relation avec d'autres obligations de déclaration et l'échange d'informations entre autorités

L'introduction d'une obligation de signaler les cyberattaques affecte des obligations de déclaration déjà en vigueur et force à s'interroger quant à la manière et au moment où les signalements réceptionnés par le NCSC peuvent être transmis à d'autres autorités.

S'agissant de la relation avec des obligations de déclaration existantes, la possibilité d'intégrer l'obligation de signaler les cyberattaques à celles-ci a été examinée, car elle permettrait de renoncer à introduire une obligation de signalement intersectorielle. Cette option a été rejetée en raison du manque d'homogénéité des réglementations relatives aux incidents de sécurité dans les différents secteurs, voire de l'absence totale de dispositions dans certains d'entre eux. S'il existe une obligation de signaler les cyberattaques à une centrale d'enregistrement, il convient de définir quels signalements doivent être enregistrés, à quel moment et auprès de quel organe. Dans le cas d'espèce, l'obligation de signaler les cyberattaques ne remplace pas les obligations de déclaration existantes, mais les complète. Parallèlement, on a veillé à ce que les bases légales puissent permettre de remplir simultanément différentes obligations de déclaration, et ce, afin de réduire au minimum la charge de travail liée à leur exécution. Cela s'applique surtout – mais pas uniquement – à l'obligation d'annonce visée à l'art. 24 de la loi révisée sur la protection des données (ci-après «nLPD»)[5], étant donné que, dans la pratique, il est fréquent que les cyberattaques entraînent des pertes de données. L'option retenue offre la possibilité à l'entreprise qui signale une cyberattaque de transmettre simultanément son annonce au NCSC et à d'autres services d'enregistrement, afin de satisfaire à d'autres obligations de déclaration. Inversement, le NCSC enregistrera aussi les signalements de cyberattaques effectués pour s'acquitter d'autres obligations de déclaration, à condition que celles-ci comprennent les éléments requis. Cette possibilité évitera aux victimes de cyberattaques de devoir signaler le même incident à différents services et selon des procédures différentes.

À cet égard, il convient également de régler les modalités de l'échange d'informations entre les autorités. Lorsque des entreprises et des organisations signalent des cyberattaques au NCSC, que ce soit à titre volontaire ou pour satisfaire à l'obligation de signalement, elles doivent être au clair sur ce qui advient de leur signalement et sur les personnes qui en prendront connaissance. Les principes de l'échange d'informations appliqués jusqu'ici doivent aussi perdurer dans cette perspective

5 Loi fédérale du 25 septembre 2020 sur la protection des données (LPD; RS **235.1**), FF *2020* 7397.

également. Toute communication de signalement, complète ou partielle, doit impérativement être approuvée par l'exploitant de l'infrastructure critique concernée ou être effectuée sous couvert d'anonymat.

La transmission d'informations permettant d'identifier les auteurs du signalement ou les entreprises concernées doit toutefois être autorisée au NCSC dans deux cas, même sans leur accord. Premièrement, une transmission aux autorités de poursuite pénale est possible si le signalement contient des informations sur une infraction grave. Le NCSC n'est certes 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[6], mais le responsable du NCSC peut transmettre des informations aux autorités de poursuite pénale s'il parvient à la conclusion que la gravité de l'infraction le nécessite. La transmission aux autorités de poursuite pénale n'aura pas de conséquences pénales pour l'exploitant de l'infrastructure critique, étant donné que la procédure est généralement dirigée uniquement contre les auteurs de la cyberattaque. Si, exceptionnellement, l'exploitant de l'infrastructure critique fait l'objet de poursuites pénales, l'obligation de signalement ne doit pas le conduire à s'incriminer lui-même par le biais de ce signalement. Une disposition a par conséquent été incluse pour prendre en compte le fait que personne n'est tenu de témoigner à sa propre charge, principe essentiel de la procédure pénale. Elle s'inspire de la disposition prévue pour l'obligation d'annonce en cas de violation de la sécurité des données visée dans le nouveau droit relatif à la protection des données (cf. art. 24, al. 6, nLPD).

Le deuxième cas de transmission autorisée concerne les informations pertinentes pour le Service de renseignement de la Confédération (SRC) dans le cadre de ses tâches de détection précoce et de prévention des menaces pour la sécurité intérieure ou extérieure, d'évaluation de la menace ou de service d'alerte précoce en matière de renseignement pour la protection des infrastructures critiques, conformément à l'art. 6, al. 1, let. a, al. 2 et 5, de la loi du 25 septembre 2015 sur le renseignement (LRens)[7]. Cela permet de garantir que le SRC, en sa qualité d'autorité compétente pour l'alerte précoce concernant les infrastructures critiques et pour l'évaluation de la menace, reçoit les informations nécessaires.

1.2.3 Exécution de l'obligation de signalement au moyen d'incitations et de sanctions

Parallèlement à l'introduction de l'obligation de signalement se pose la question des outils permettant de la mettre en œuvre. Trois facteurs peuvent influencer la disposition des entreprises à se soumettre à cette obligation.

Premièrement, effectuer un signalement doit être aussi simple que possible. Le NCSC s'en assure en mettant à disposition un formulaire électronique au moyen duquel le signalement est rapide à saisir et facile à transmettre.

Deuxièmement, le fait de signaler un incident doit comporter des avantages (incitation positive): le NCSC offre notamment une évaluation technique et apporte son soutien dans la gestion de l'attaque. Cette aide est proposée en guise de «premiers secours» et ne doit pas concurrencer des prestations disponibles sur le marché. Pour les exploitants d'infrastructures critiques, il peut toutefois s'avérer très utile de bénéficier de l'appui d'un organe fédéral qui a une vue d'ensemble de la situation et des menaces pour obtenir une première appréciation et mettre en œuvre des mesures d'urgence.

Le troisième facteur consiste à mettre en place des incitations négatives sous la forme d'une amende: si un exploitant d'infrastructure critique ne se soumet pas à l'obligation de signaler ou de fournir des renseignements malgré un rappel à l'ordre, le NCSC peut, en dernier recours, rendre une décision dont le non-respect est passible de l'amende. Le montant maximal de l'amende est fixé à 100 000 francs, dont 20 000 francs peuvent être directement à la charge de l'entreprise qui exploite l'infrastructure critique. Cette possibilité de sanction relevant du droit administratif s'inspire de la loi révisée sur la protection des données, qui contient à l'art. 63 et s une disposition similaire pour le

6 RS **172.220.1**
7 RS **121**

cas d'insoumission à une décision du préposé fédéral à la protection des données et à la transparence (PFPDT).

Sur la base de sa longue collaboration avec les infrastructures critiques, le NCSC part du principe que cette disposition a plutôt un caractère symbolique et sert surtout à garantir que l'obligation de signalement reçoive l'attention requise.

1.3 Relation avec le programme de la législature et avec le plan financier, ainsi qu'avec les stratégies du Conseil fédéral

Le projet a été annoncé dans le message du 29 janvier 2020 sur le programme de la législature 2019 à 2023[8] et dans l'arrêté fédéral du 21 septembre 2020 sur le programme de la législature 2019 à 2023[9]. Le message soulignait notamment la nécessité de pouvoir identifier et maîtriser rapidement les cyberincidents affectant les infrastructures critiques, ainsi que celle d'augmenter la résilience informatique. L'objectif 18, visé à l'art. 19 de l'arrêté fédéral, stipule que «la Confédération combat les cyberrisques; elle soutient et prend des mesures visant à protéger les citoyens et les infrastructures critiques.» Le message comme l'arrêté fédéral renvoient à la stratégie nationale du 18 avril 2018 de protection de la Suisse contre les cyberrisques pour les années 2018 à 2022.

Le budget 2022 avec plan intégré des tâches et des finances pour les 2023 à 2025 définit comme une priorité stratégique l'amélioration de la cybersécurité au sein de la Confédération et en Suisse et mentionne l'obligation des infrastructures critiques de signaler les cyberattaques parmi les affaires relatives aux objectifs du Conseil fédéral. Il y est précisé que le NCSC contribue à la protection de la Suisse contre les cyberrisques[10].

La stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022 examine les modalités d'introduction d'une obligation de signaler les cyberattaques et présente la décision prise (mesure 9). Le présent projet de consultation met totalement en œuvre la mesure 9[11].

8 FF *2020* 1709, 1797
9 FF *2020* 8087, 8094
10 Budget 2022 avec PITF 2023–2025, Tome 2B, p. 11 ss, disponible à l'adresse: www.efv.admin.ch > Rapports financiers > Rapports financiers > Budget assorti d'un plan intégré des tâches et des finances
11 Cf. rapport d'août 2021 sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022, p. 10, 15 s. (www.ncsc.admin.ch > Stratégie SNPC > Rapports et études)

2 Comparaison avec le droit étranger, notamment européen

Depuis l'adoption, en juillet 2016, de la directive sur la sécurité des réseaux et des systèmes d'information (directive SRI), les membres de l'Union européenne sont soumis à l'obligation de notifier les cyberincidents. Cette obligation est mise en œuvre depuis mai 2018. Elle concerne les «opérateurs de services essentiels», terme qui désigne, selon l'article 4, les entreprises privées ou des entités publiques investies du rôle important d'assurer la sécurité dans les secteurs de la santé, des transports, de l'énergie, des banques et infrastructures de marchés financiers, des infrastructures numériques et de l'approvisionnement en eau[12]. Le cercle des assujettis à cette obligation correspond donc dans une large mesure aux infrastructures critiques soumises à l'obligation de signalement définies dans le projet mis en consultation.

En ce qui concerne l'étendue de l'obligation de notification, la directive SRI laisse une marge de manœuvre relativement importante aux États membres de l'UE. Les incidents graves doivent être déclarés, l'article 14 précisant que l'appréciation de la gravité repose notamment sur le nombre d'utilisateurs touchés, la durée de l'incident de sécurité et sa portée géographique. Contrairement au présent projet, la directive SRI ne se limite toutefois pas à l'introduction d'une obligation de notification. Elle impose en même temps aux opérateurs de services essentiels des mesures de sécurité à prendre, par exemple pour prévenir les risques, pour garantir un niveau de sécurité adapté pour les réseaux et les systèmes d'information et pour limiter l'impact des incidents compromettant la sécurité (article 14).

Le projet mis en consultation se contente quant à lui de créer les bases légales nécessaires à de telles exigences dans le secteur de l'électricité. Une étude mandatée par l'Office fédéral de l'énergie (OFEN) a en effet constaté une nécessité accrue d'améliorer la cybersécurité dans ce domaine primordial pour l'approvisionnement économique et pour la sécurité du pays.[13] Dans les autres secteurs, il conviendra de déterminer par la suite si la Confédération a la compétence de fixer des normes juridiquement contraignantes en matière de cybersécurité et quelles exigences devraient, le cas échéant, être imposées dans quels domaines.

12 DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (europa.eu)

13 Stratégie de cybersécurité du 28 juin 2021 pour l'approvisionnement suisse en électricité (www.bfe.admin.ch > Approvisionnement > La numérisation du monde de l'énergie, disponible en allemand uniquement)

3 Présentation du projet

3.1 Réglementation proposée

L'introduction d'une obligation de signaler les cyberattaques contre des infrastructures critiques se justifie principalement par les possibilités d'alerte précoce et d'amélioration de la vue d'ensemble des menaces. Comme les auteurs de cyberattaques recourent souvent à des méthodes et à des schémas similaires pour plusieurs infrastructures critiques de différents secteurs, cette obligation peut renforcer considérablement la cybersécurité des infrastructures critiques en identifiant rapidement les méthodes d'attaque et en transmettant les alertes correspondantes.

Cette obligation ne s'applique qu'aux cyberattaques renfermant un potentiel de dommages important. Les cyberincidents relevant de l'erreur humaine, par exemple une manipulation fautive commise involontairement par un collaborateur, n'ont pas besoin d'être déclarés. Enfin, il a été décidé de ne pas étendre l'obligation de signalement aux vulnérabilités des équipements informatiques. Indépendamment de l'introduction de l'obligation de signaler les cyberattaques, il reste possible de notifier les cyberincidents et les vulnérabilités à titre volontaire. Cette possibilité n'est pas réservée aux infrastructures critiques et est offerte à tout un chacun.

L'introduction de l'obligation de signaler les cyberattaques permet en même temps de régler au niveau de la loi les tâches du NCSC, qui ne sont actuellement définies que dans l'ordonnance sur les cyberrisques (OPCy)[14]. D'une part, une telle inscription est nécessaire étant donné que le NCSC remplira la fonction de centrale d'enregistrement. D'autre part, elle permet de tenir compte de la réorganisation de l'administration fédérale dans le domaine de la cybersécurité, notamment la création du NCSC, qui n'a été entreprise que pendant les débats parlementaires sur la LSI.

3.2 Adéquation entre les tâches et les moyens financiers

Le NCSC gère déjà à l'heure actuelle un service d'alerte qui recueille sur une base volontaire les signalements de cyberincidents. Il bénéficie en la matière de la longue expérience de MELANI, qui se chargeait déjà de cette tâche depuis 2004 pour les déclarations relatives aux infrastructures critiques et celles de la population.

Le NCSC utilise un formulaire électronique pour les signalements. Il est possible de l'adapter afin qu'il puisse aussi servir à la réception des signalements faisant suite à l'obligation en la matière. Les accords nécessaires avec d'autres organes qui réceptionnent également des déclarations (par ex. PFPDT, FINMA, IFSN) et la configuration du formulaire de signalement requièrent un investissement initial qui peut néanmoins être couvert par les ressources existantes du NCSC. En vue de la mise en œuvre du projet, le NCSC doit toutefois pouvoir garantir la saisie correcte, la confirmation de réception et la documentation des déclarations effectuées au titre de l'obligation de signalement, ainsi que leur transmission aux organes *ad hoc* aux fins d'alerte précoce. Ce surcroît de travail devra être pris en compte lors des développements futurs du NCSC.

Après une cyberattaque, le NCSC apportera son soutien à l'infrastructure critique touchée pour l'aider à gérer l'incident. Cet appui est lui aussi déjà bien rodé grâce à la longue expérience du NCSC (et de MELANI avant lui). Il faut cependant s'attendre à ce que l'introduction de l'obligation de signalement augmente la charge de travail du NCSC, d'une part, en raison de l'augmentation du nombre de déclarations et, d'autre part, parce que le NCSC sera désormais chargé d'effectuer au moins une première appréciation de l'incident et de formuler des recommandations pour sa gestion. Il convient par conséquent aussi d'augmenter l'effectif de l'équipe d'analyse technique du NCSC (GovCERT).

14 RS **120.73**

3.3 Modalités de mise en œuvre

3.3.1 Nécessité d'une base légale

Il découle du principe de légalité (art. 5, al. 1, de la Constitution, Cst.[15]) et des dispositions relatives à la législation de l'art. 164, al. 1, Cst. que l'obligation de signalement des cyberattaques doit être réglée au moins dans les grandes lignes au niveau de la loi. Le projet mis en consultation contient par conséquent les éléments essentiels de l'obligation de signaler les cyberattaques: il comporte les principaux éléments de l'obligation de signalement, notamment ses facteurs déclenchants et sa portée (cyberattaques avec potentiel de dommages), le cercle des assujettis (exploitants d'infrastructures critiques actives dans des domaines définis), le contenu des signalements et leur utilisation par le NCSC. Pour les exploitants d'infrastructures critiques assujettis, l'obligation de signaler les cyberattaques constitue une atteinte à leurs droits de particuliers ou, si l'organisme responsable est cantonal ou communal, à leur autonomie fédéraliste. Cette atteinte est toutefois mineure et n'a pratiquement pas de conséquences financières pour les entreprises concernées.

3.3.2 La LSI, une base légale adéquate

Dans le cadre des travaux réalisés en amont de l'avant-projet, on a examiné si les nouvelles réglementations devaient être fixées dans une loi à part ou intégrées à un acte existant dont le but, l'objet et le champ d'application seraient compatibles avec une obligation de signaler les cyberattaques contre des infrastructures critiques[16]. Les actes légaux contenant déjà des dispositions relatives aux infrastructures critiques et axés sur la protection de l'ordre public (LPPCi[17], LAP[18], LMSI[19], LRens et LSI[20]) ont notamment été pris en considération pour servir de base à l'inscription dans la loi de l'obligation de signalement. Après un examen approfondi, il est apparu que parmi ces actes, seule la LSI offrait un cadre adéquat. Son but, à savoir assurer la sécurité des informations traitées par la Confédération et des moyens informatiques qu'elle utilise, a un lien direct avec la cybersécurité (bien que la loi n'utilise pas ce terme). En outre, certains articles de la LSI prévoyaient déjà le soutien des infrastructures critiques par la Confédération, et donc une partie du mandat du NCSC. Par conséquent, la LSI n'était pas seulement adéquate, mais elle représentait également une base légale idéale pour inscrire dans la loi l'obligation de signaler les cyberattaques. De plus, l'introduction d'une obligation, pour les exploitants d'infrastructures critiques, de signaler les «incidents graves» avait été discutée lors des débats parlementaires sur le projet de loi, mais elle avait été rejetée par la majorité du Conseil national en juin 2020, après que le Conseil fédéral avait indiqué qu'un projet de loi serait élaboré à cet effet.

3.3.3 Dispositions d'exécution

Les prescriptions légales seront concrétisées dans une ordonnance. Celle-ci définira plus en détail les tâches du NCSC et la collaboration avec les autres services et précisera qui doit annoncer quelles cyberattaques à quel organe et selon quelle procédure. L'ordonnance intégrera les dispositions de l'actuelle OPCy qui portent sur la relation de la Confédération avec la population, et plus particulièrement avec les exploitants d'infrastructures critiques. Concernant le cercle des assujettis, il convient de vérifier dans chaque cas s'il est préférable d'apporter des précisions dans l'ordonnance relative à l'obligation de signalement ou dans les ordonnances propres au secteur dont il est question.

15 RS **101**
16 Cf. rapport du 25 novembre 2020 «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen», Annexe 01 au mandat du CF du 11 décembre 2020 (disponible en allemand uniquement)
17 RS **520.1**
18 RS **531**
19 RS **120**
20 Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (LSI), FF *2020* 9665

3.3.4 Applicabilité de l'obligation de signalement

En avril 2021, le NCSC a effectué un sondage auprès des exploitants d'infrastructures critiques et des autorités au sujet du projet d'introduire une obligation de signaler les cyberattaques. Il en est ressorti qu'une telle obligation est généralement bien acceptée, à condition qu'il soit possible de la mettre en œuvre sans trop de charges administratives. L'illustration 1 montre le niveau élevé d'adhésion des personnes interrogées.

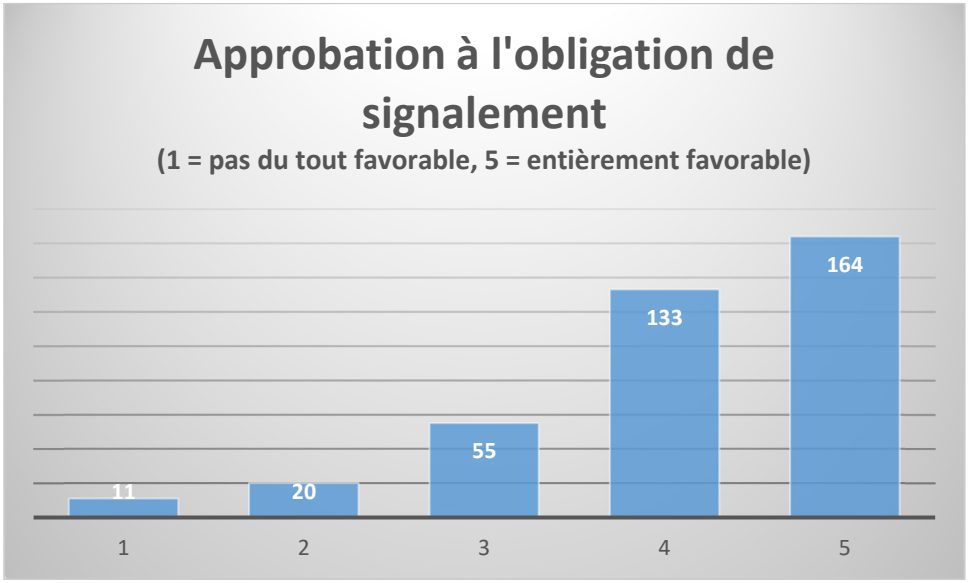

Illustration 1: Acceptation de l'obligation de signalement

Outre l'obligation d'informer le NCSC, une cyberattaque contre une infrastructure critique peut affecter d'autres processus soumis à une obligation de signalement, et donc engendrer simultanément plusieurs obligations. On peut par exemple se trouver en présence des chevauchements suivants:

- Pour les infrastructures critiques du secteur financier soumises à la surveillance de la FINMA, une obligation d'annoncer les cyberattaques à la FINMA[21] est en vigueur depuis mai 2020 déjà. Ainsi, une cyberattaque devra toujours être signalée à la fois à la FINMA et au NCSC.

- Une cyberattaque contre une infrastructure critique peut entraîner une violation de la sécurité des données qui, en fonction de sa gravité, doit être annoncée au PFPDT[22].

- Si une cyberattaque provoque des dysfonctionnements au sein de l'infrastructure critique, par ex. un incident radioactif dans une centrale nucléaire, celui-ci doit aussi être déclaré (IFSN, CENAL, etc.).

La nouvelle obligation de signaler les cyberattaques ne remplacera pas les obligations de notification existantes, qui demeurent inchangées. Il est donc important que la charge soit acceptable pour les organisations tenues de signaler si elles doivent en même temps s'acquitter d'autres obligations de notification. Voilà pourquoi le NCSC mettra à disposition un système permettant la saisie électronique du signalement (formulaire, masque ou similaire). Les organisations tenues de signaler pourront décider elles-mêmes si elles souhaitent ajouter des informations au signalement électronique et l'envoyer à d'autres organes. Si d'autres services d'enregistrement devaient proposer leur aide, le masque de saisie de la déclaration pourrait aussi être conçu de telle sorte que, hormis les informations générales sur l'infrastructure, les données spécifiques qui ne concernent que l'une ou l'autre

21 Cf. art. 29 LFINMA. L'obligation générale de renseigner et d'annoncer inclut aussi les cyberincidents (cf. communication de la FINMA du 7 mai 2020 sur la surveillance)

22 Art. 24 nLPD

obligation de signalement ne soient destinées qu'au service d'enregistrement concerné. Les organisations tenues de signaler pourraient alors gérer lors de la saisie et de la transmission quelles informations sont envoyées à quel service d'enregistrement.

4 Commentaire des différents articles

Les bases légales de l'obligation de signaler les cyberattaques sont intégrées au chapitre 5 de la LSI, à l'exception de quelques adaptations mineures du chapitre 1. Le chapitre 5 a subi un remaniement de fond pour qu'il puisse aussi définir les tâches du NCSC, qui vont au-delà de l'obligation de signalement et ne sont pas spécifiquement axées sur les infrastructures critiques. Le titre du chapitre a également été adapté en conséquence («Chapitre 5: Mesures de la Confédération afin de protéger la Suisse contre les cyberrisques»).

Les principaux contenus des dispositions légales ont déjà été décrits et motivés - pour certains de manière détaillée - dans le message relatif à la LSI (FF *2017* 2872 ss) et sous les chiffres précédents. Les commentaires relatifs aux articles suivants se limitent donc à des compléments.

Chapitre 1 Dispositions générales

Dans le premier chapitre, seuls les art. 1, 2 et 5 sont modifiés. Les autres articles sont repris tels quels.

Art. 1 But

L'al. 1 de l'article définissant le but de la LSI a été complété et subdivisé en deux lettres a et b. La let. a reprend la formulation d'origine, tandis que la let. b vient en complément pour fixer l'objectif en matière de cyberrisques. L'extension de la finalité de la loi permet de prendre en considération les nouveaux éléments qui accompagnent l'introduction d'une obligation de signaler les cyberattaques de la réglementation légale des tâches du NCSC.

Art. 2 Autorités et organisations concernées

Dans l'al. 5, le renvoi aux dispositions qui s'appliquent aux infrastructures critiques a été adapté, puisque le chapitre 5 commence désormais par l'art. 73*a* et se termine par l'art. 79. Cet article n'a par contre subi aucune modification de fond.

Art. 5 Définitions

Les définitions des let. a, b et c ne sont pas modifiées.

Let. d

La définition de «cyberincident» est reprise de l'art. 3, let. b, OPCy, avec une légère adaptation. Elle englobe également l'utilisation abusive de moyens informatiques, comme c'est le cas avec les tentatives de phishing.

Let. e

La définition de «cyberattaque» est ajoutée; il s'agit d'une forme possible de cyberincident. Il est important de distinguer «cyberattaque» et «cyberincident», car seules les attaques contre des infrastructures critiques sont soumises à l'obligation de signalement. Les cyberincidents et les vulnérabilités peuvent quant à eux être déclarés à titre facultatif par tout un chacun.

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

Aucune modification n'a été apportée aux chapitres 2, 3 et 4. Le chapitre 5, en revanche, voit l'introduction de l'obligation de signaler les cyberattaques contre les infrastructures critiques et de dispositions fondamentales concernant les tâches du NCSC. Pour garantir une meilleure vue d'ensemble, le chapitre 5 est divisé en trois sections.

Section 1 Dispositions générales

Art. 73a Principe

Les let. a à f décrivent les tâches du NCSC. Il s'agit d'une liste non exhaustive. En ce qui concerne la réception et le traitement des signalements (let. e), il faut préciser qu'il s'agit aussi bien des signalements volontaires de cyberincidents et de vulnérabilités que des signalements de cyberattaques contre des infrastructures critiques, lesquelles sont soumises à une obligation signalement.

Les différentes tâches ainsi que la collaboration avec les autorités en Suisse et à l'étranger font l'objet d'autres articles qui en concrétisent le contenu.

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

Depuis le 1er janvier 2020, le NCSC exploite un guichet national unique en matière de cyberrisques (cf. art. 12, al. 1, let. a, OPCy), qui enregistre et traite les signalements de cyberincidents et de vulnérabilités. La centrale d'enregistrement du NCSC a été développée à partir de MELANI, qui réceptionnait les déclarations depuis 2004. Elle est utilisée activement par les entreprises et la population: en 2020, elle a reçu 10 834 déclarations[23].

Depuis le 28 septembre 2021, le NCSC fait partie du réseau mondial gérant les vulnérabilités des systèmes informatiques et est autorisé à attribuer un numéro d'identification unique aux vulnérabilités qui lui sont signalées, conformément au système de référence international[24]. Il est donc important de préciser que le NCSC n'enregistre pas seulement les signalements de cyberincidents, mais aussi ceux de vulnérabilités.

Al. 1

Les cyberincidents et les vulnérabilités peuvent être signalés par des tiers et pas uniquement par les victimes elles-mêmes, et ce, également de manière anonyme. Le NCSC analyse les incidents et évalue leur importance pour la protection de la Suisse contre les cyberrisques. Si le signalement n'est pas anonyme, le NCSC peut, à la demande de son auteur et sur la base de ces analyses, donner son avis sur l'incident et émettre des recommandations pour la suite de la procédure. En outre, le NCSC utilise les signalements à des fins statistiques et pour avertir le public des cybermenaces. Aucune information concernant les auteurs des signalements ou les personnes concernées n'est publiée.

Le NCSC traite les déclarations en toute confidentialité. C'est une condition essentielle pour que les signalements soient faits et que la centrale d'enregistrement jouisse de la confiance des entreprises.

Al. 2

Le NCSC peut publier ou communiquer aux autorités et organisations intéressées des informations sur des cyberincidents, à condition que ces informations ne contiennent pas de données personnelles ou de données concernant des personnes morales. La publication de données personnelles dans le cas de cyberincidents est exclue. Il reste possible de publier des informations tirées du signalement avec l'accord de la personne ou de l'organisation concernées, par exemple en cas de détournement de logos lors d'attaques de phishing.

Al. 3

En revanche, en cas de vulnérabilité, la publication rapide de la faille avec indication du logiciel ou du matériel concernés peut s'avérer nécessaire pour prévenir d'autres cyberattaques. L'exploitation des vulnérabilités est l'un des modes opératoires les plus fréquents des cyberattaques. Ce n'est

23 Cf. rapport d'août 2021 sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022, p. 5 (www.ncsc.admin.ch > Stratégie SNPC > Rapports et études)

24 Cf. communiqué de presse du NCSC du 28 septembre 2021 (www.ncsc.admin.ch > Documentation > Communiqués de presse > Newslist > Le NCSC fait désormais partie du réseau mondial gérant les vulnérabilités des systèmes informatiques)

qu'avec ces informations que les utilisateurs du logiciel ou du matériel concernés peuvent prendre immédiatement les mesures nécessaires pour se protéger contre les cyberattaques. L'al. 3 constitue la base légale permettant au NCSC d'indiquer le nom du matériel et des logiciels concernés - et donc, implicitement, celui de leur fabricant - lors de la publication des vulnérabilités.

Art. 73c Transmission d'informations

L'art. 73*c* définit les conditions auxquelles le NCSC est autorisé à transmettre certaines informations contenues dans un signalement au SRC ou aux autorités de poursuite pénale (al. 1 et 2). En outre, il règle le traitement des informations au cas où une procédure pénale est engagée contre une personne ayant fait une communication (al. 3).

Al. 1

L'al. 1 stipule que le NCSC est autorisé à transmettre des informations au SRC si celles-ci sont 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, LRens. Cette transmission est nécessaire pour que le SRC puisse remplir ses tâches également en ce qui concerne les cybermenaces. Elle se limite toutefois aux informations nécessaires à cet effet.

Al. 2

L'al. 2 règle la transmission d'informations aux autorités de poursuite pénale. L'obligation de dénoncer qui s'applique aux employés de la Confédération ne concerne pas les informations reçues par le NCSC lors du signalement d'un cyberincident ou de son analyse, car elle entre en conflit avec le principe du traitement confidentiel du signalement. Le responsable du NCSC est toutefois autorisé à transmettre des informations aux autorités de poursuite pénale. Ce faisant, il met en balance l'intérêt de l'État à une poursuite pénale et celui de la personne qui effectué le signalement à la confidentialité des informations. La possibilité de transmettre les informations après une pesée des intérêts en jeu a été prévue pour permettre au NCSC de saisir les autorités de poursuite pénale en cas d'infractions graves.

Al. 3

La disposition visée à l'al. 3 permet de garantir que la personne effectuant un signalement ne sera pas incriminée contre son gré dans le cadre d'une procédure pénale dirigée contre elle en raison des informations contenues dans la communication. En règle générale, une procédure pénale est dirigée contre les auteurs du cyberincident, c'est-à-dire contre les pirates informatiques, et non contre la personne qui a effectué le signalement. Une règle analogue à celle de l'art. 24, al. 6, nLPD a été introduite au cas où, exceptionnellement, une procédure pénale devait être dirigée contre la victime d'une cyberattaque. Cette disposition met en œuvre le principe de l'interdiction de s'auto-incriminer (*nemo tenetur*) dans le cadre de l'obligation de signaler les cyberattaques. Elle est donc particulièrement importante pour les déclarations effectuées dans le cadre de l'obligation de signaler les cyberattaques. Par ailleurs, ce privilège doit également s'appliquer aux signalements volontaires.

Al. 4

Dans les cas exceptionnels où une transmission d'informations au SRC ou aux autorités de poursuite pénale est envisageable en vertu des al. 1 et 2, le NCSC doit se faire délier du secret de fonction, conformément aux prescriptions de l'art. 320 CP, pour autant que ces informations soient des secrets pénalement protégés.

Art. 74 Soutien aux exploitants d'infrastructures critiques

En complément aux tâches générales énoncées à l'art. 73*a* et au traitement des signalements concernant les cyberincidents et les vulnérabilités visé à à l'art. 73*b*, le NCSC fournit aux exploitants

d'infrastructures critiques d'autres prestations en matière de protection contre les cyberrisques (al. 1). La définition des infrastructures critiques visée à l'art. 5 étant très large, une certaine imprécision règne quand il s'agit de déterminer si une organisation est considérée comme une infrastructure critique ou non. Pour ce faire, le NCSC s'appuie sur les secteurs et sous-secteurs mentionnés dans la stratégie nationale pour la protection des infrastructures critiques (PIC)[25].

Al. 2

À cette fin, le NCSC met des instruments à la disposition des exploitants d'infrastructures critiques. Les plus importants d'entre eux sont énumérés dans cet alinéa à titre d'exemples. Il s'agit d'une liste non exhaustive.

Let. a

L'échange d'informations est un moyen de protection essentiel contre les cyberrisques. L'important dynamisme avec lequel la situation en matière de menace évolue et la nécessité de prendre des mesures de protection requièrent des responsables qu'ils disposent constamment des informations les plus actuelles. Échanger avec les autres responsables est le moyen le plus efficace d'y parvenir. Le NCSC poursuit une collaboration qui a fait ses preuves via MELANI en mettant à disposition des exploitants d'infrastructures critiques une plateforme destinée à cet échange d'informations.

Let. b

Les informations sur les cyberrisques et vulnérabilités actuels et les recommandations sur les mesures de prévention se limitent aux éléments susceptibles d'être utiles aux infrastructures critiques en général. Le NCSC ne fournit pas de conseils personnalisés aux entreprises.

Let. c

Les outils techniques et les instructions de détection des cyberincidents sont en partie conçus de manière à être utiles à toutes les infrastructures critiques en général. Mais ils peuvent aussi être conçus spécifiquement pour certains groupes d'infrastructures critiques ou pour certains domaines d'activité. Ils ne remplacent pas les dispositifs de protection individuels des entreprises, mais doivent y être intégrés.

Al. 3

En cas de cyberincident, le NCSC soutient les exploitants d'infrastructures critiques en leur fournissant des conseils techniques. Le soutien technique assuré par le NCSC est fourni subsidiairement aux services informatiques disponibles sur le marché, pour autant qu'il s'agisse d'exploitants privés. C'est l'organisme responsable qui est déterminant et non la forme juridique. Par ailleurs, ce soutien n'intervient pour tous les exploitants que si le risque est imminent et que l'on est en présence d'une menace de dommages considérables.

Al. 4

En cas de cyberincident, notamment sous la forme d'une cyberattaque, le NCSC doit avoir la possibilité d'accéder aux systèmes de l'infrastructure critique concernée afin de gérer l'incident ou de limiter les dommages, sous réserve que l'exploitant de l'infrastructure critique ait donné son accord. L'exploitant est délié de garder le secret vis-à-vis du NCSC. La deuxième phrase constitue la base légale permettant à l'exploitant d'autoriser le NCSC à accéder à ses informations et à ses moyens informatiques sans enfreindre ses obligations légales et contractuelles de garder le secret.

Section 2 Obligation de signaler les cyberattaques contre des infrastructures critiques

25 Stratégie nationale pour la protection des infrastructures critiques 2018-2022 (www.babs.admin.ch > Autres domaines d'activités > Protection des infrastructures critiques > Stratégie nationale PIC)

Art. 74a Obligation de signalement

Cet article définit les grandes lignes de l'obligation de signalement. Il dispose que les exploitants d'infrastructures critiques sont soumis à l'obligation de signaler les cyberattaques au NCSC le plus rapidement possible après leur découverte. Il est en effet essentiel pour l'alerte précoce et la prévention que les attaques soient déclarées immédiatement après leur découverte. L'art. 74*e* précise que l'exigence d'immédiateté ne porte pas sur toutes les informations demandées, mais seulement sur le signalement initial, effectué sur la base des informations disponibles à ce moment-là.

Art. 74b Domaines

La définition des infrastructures critiques visée à l'art. 5 est très large. Elle n'est pas assez précise pour déterminer quelles sont les entreprises ou les organisations qui sont considérées comme des infrastructures critiques et, de ce fait, sont soumises à l'obligation de signalement. C'est pourquoi l'al. 74*b* dresse une liste concrète des entreprises et des organisations auxquelles s'applique cette obligation. Cette liste se fonde sur les sous-secteurs critiques définis comme tels dans la stratégie nationale pour la protection des infrastructures critiques. Pour ces domaines, le champ d'application de l'obligation de signalement est fixé, dans la mesure du possible, avec des renvois aux bases légales existantes. Dans les domaines où un tel renvoi n'est pas possible - car il n'existe pas de bases légales appropriées pour une telle délimitation - le domaine concerné est décrit aussi précisément que possible. Cette manière de procéder garantit que le cercle des assujettis à l'obligation de signalement est défini avec suffisamment de clarté.

Let. a: hautes écoles

Les hautes écoles sont d'une grande importance pour la formation et l'économie en Suisse. Leurs activités de recherche, en particulier, constituent un moteur de l'innovation. De ce fait, elles sont également une cible privilégiée pour les cyberattaques. Les universités cantonales, les écoles polytechniques fédérales, les hautes écoles, les hautes écoles spécialisées et les hautes écoles pédagogiques sont soumises à l'obligation de signalement.

Let. b: autorités

Les cyberattaques contre les autorités de tous les niveaux fédéraux doivent être signalées, car il est important de savoir à quelle fréquence et par qui elles sont attaquées. Les dispositifs de défense peuvent ainsi être adaptés aux menaces en cause. L'obligation de signalement ne s'applique toutefois qu'aux tâches relevant de la puissance publique de ces autorités et de ces organisations.

Let. c: organisations chargées de tâches de droit public

Les organisations qui assument des tâches de droit public dans certains domaines sont soumises à l'obligation de signalement. La let. c énumère les activités concrètement visées par cette notion. Dans le domaine de la sécurité et du sauvetage, l'accent est mis sur les organisations d'intervention d'urgence (police, services du feu, services de protection et de sauvetage). Les organisations chargées de l'approvisionnement en eau potable, du traitement des eaux usées et de l'élimination des déchets sont également soumises à l'obligation de signalement.

Let. d: entreprises œuvrant dans les domaines de l'approvisionnement énergétique, du commerce, de la mesure et de la gestion de l'énergie

L'approvisionnement en énergie est essentiel pour l'économie et la société. Des attaques contre l'approvisionnement en électricité ou contre des pipelines dans d'autres États ont montré que ces infrastructures avaient été ciblées, que ce soit pour des motifs politiques ou pour extorquer des sommes aussi élevées que possible. Les entreprises dont les activités sont importantes pour l'approvisionnement en énergie sont donc soumises à l'obligation de signalement.

Let. e: banques, assurances et infrastructures de marchés financiers

Les entreprises du secteur financier sont fortement touchées par les cyberattaques, car elles représentent une cible intéressante pour les criminels en raison des moyens financiers importants qu'elles gèrent. Pour la fiabilité de la place financière suisse, il est important que les cyberattaques soient signalées. L'obligation de signaler les cyberattaques à l'Autorité fédérale de surveillance des marchés financiers (FINMA), qui existe déjà, est maintenue en parallèle. La FINMA et le NCSC se concerteront de manière à ce que la charge de travail pour les assujettis à l'obligation soit la plus faible possible.

Let. f: services numériques

Sont considérées comme fournisseurs de services numériques les entreprises qui proposent sur Internet des services sollicités par un grand nombre d'utilisateurs en Suisse, qui revêtent une grande importance pour l'économie numérique ou qui comprennent des services sensibles du point de vue de la sûreté et de la confiance. Il s'agit, en particulier, de fournisseurs de places de marché en ligne de taille importante, d'informatique en nuage et de moteurs de recherche. Cette énumération n'est pas exhaustive. Par «autres services numériques», on entend notamment les services dans les domaines de la gestion d'identité, des signatures ou du vote électronique. Les registraires de noms de domaine et les exploitants de centres de calcul sont également mentionnés. Des critères comme le nombre d'utilisateurs, le nombre de collaborateurs, le chiffre d'affaires ou le type d'activité seront fixés dans l'ordonnance pour concrétiser la nature des services numériques soumis à l'obligation de signalement.

Let.g: hôpitaux

Les cantons établissent des listes d'hôpitaux cantonaux et extracantonaux qui visent à assurer la couverture des besoins en soins médicaux de base sur le territoire du canton concerné. L'obligation de signaler les cyberattaques doit s'appliquer à ces hôpitaux, car il s'agit d'éviter que ce genre d'attaques ne compromettent la fourniture des soins de base.

Let. h: laboratoires médicaux

Les laboratoires qui effectuent des analyses microbiologiques pour détecter des maladies transmissibles sont importants pour les soins de santé. Pour leurs analyses et leur collaboration avec les médecins de premier recours, ils dépendent dans une large mesure du bon fonctionnement de l'infrastructure informatique. Les cyberattaques visant ces laboratoires doivent donc être soumises à une obligation de signalement.

Let. i: fabrication, commercialisation (ou distribution) et importation de médicaments et de dispositifs médicaux

La fabrication, la commercialisation et l'importation de médicaments revêtent une grande importance pour l'approvisionnement médical de la population. Les entreprises actives dans ces domaines sont donc soumises à l'obligation de signalement. Les fabricants et les distributeurs de dispositifs médicaux sont également soumis à cette obligation.

Let. j: assurances sociales

Les prestations des assurances sociales sont décrites en référence aux risques définis dans les dispositions générales de la loi fédérale sur la partie générale du droit des assurances sociales (LPGA[26]) afin de couvrir, si possible, toutes les branches des assurances sociales. Le législateur a renoncé à dresser une liste des différentes lois (par ex. LAI ou LAVS) pour ne pas englober uniquement les prestations légales, mais aussi les prestations surobligatoires telles que la prévoyance professionnelle ou l'assurance complémentaire à l'assurance-maladie obligatoire. En ce qui con-

26 RS **830.1**

cerne la prévoyance professionnelle, toutes les institutions de prévoyance et de libre passage, enregistrées ou non, sont concernées, mais pas la prévoyance individuelle liée ou libre (piliers 3a et 3b). Ces dernières possibilités de prévoyance sont généralement proposées par les banques et les assurances, qui sont elles-mêmes soumises à l'obligation de signalement.

Dans le cas des assurances sociales également, le Conseil fédéral pourra restreindre au niveau de l'ordonnance le cercle des assujettis à l'obligation de signalement et, par exemple, limiter par des critères appropriés le cercle des destinataires des institutions de prévoyance et de libre passage soumises à l'obligation de signalement.

Let. k: fournisseurs de services de télécommunication

Par transmission au moyen de techniques de télécommunication, on entend l'émission ou la réception d'informations, sur des lignes ou par ondes hertziennes, au moyen de signaux électriques, magnétiques ou optiques ou d'autres signaux électromagnétiques (art. 3, let. c, de la loi du 30 avril 1997 sur les télécommunications, LTC[27]). Sont également considérés comme une transmission au moyen de techniques de télécommunication l'offre de capacité de transmission et les services «over the top». Ces derniers sont des transmissions d'informations via des services Internet. Parmi les exemples connus, on peut citer Skype (Microsoft), WhatsApp (Facebook), Facetime (Apple), Hangouts (Google), Signal et Threema.

Let. l: Société suisse de radiodiffusion et télévision (SSR)

La SSR a pour mandat de fournir à l'ensemble de la population des programmes de radio et de télévision complets et de même valeur dans les trois langues officielles (art. 24, al. 1, let. a, de la loi du 24 mars 2006 sur la radio et la télévision, LRTV[28]). Elle a également pour mission de contribuer à la libre formation de l'opinion en présentant une information complète, diversifiée et fidèle, en particulier sur les réalités politiques, économiques et sociales (art. 24, al. 4, let. a, LRTV). Son mandat va donc nettement plus loin que les obligations d'information des autres médias titulaires d'une concession. Des cyberattaques contre la SSR peuvent mettre en péril l'accomplissement de ces mandats.

Let. m: agences de presse d'importance nationale

Une agence de presse est considérée comme étant d'importance nationale au sens de l'art. 44*a* de l'ordonnance du 9 mars 2007 sur la radio et la télévision[29] si elle diffuse des informations portant sur les quatre régions linguistiques et qu'elle publie régulièrement des informations dans au moins trois langues nationales (cf. art. 18, let. a, de la loi du 5 octobre 2007 sur les langues[30] en relation avec l'art. 13, al. 2, de l'ordonnance du 4 juin 2010 sur les langues[31]). Concrètement, en Suisse, il ne reste que l'agence nationale de presse Keystone-ATS (cf. ordonnance COVID-19 médias électroniques[32]).

Let. n: fournisseurs de services postaux

Les entreprises qui offrent des services postaux à des clients en leur nom propre sont également soumises à l'obligation de signalement si elles sont enregistrées auprès de la Commission de la poste conformément à l'art. 4, al. 1, de la loi du 17 décembre 2010 sur la poste[33]. Le Conseil fédéral pourra exempter les petites entreprises de l'obligation de signalement au niveau de l'ordonnance. On pourrait par exemple envisager une restriction analogue à celle prévue à l'art. 4, al. 2, de la loi sur la poste pour les entreprises qui réalisent un faible chiffre d'affaires.

27 RS **784.10**
28 RS **784.40**
29 RS **784.401**
30 RS **441.1**
31 RS **441.11**
32 RS **784.402**
33 RS **783.0**

Let. o: transports publics (transport de personnes et transport ferroviaire de marchandises)

Le renvoi à la loi du 18 juin 2010 sur les organes de sécurité des entreprises de transports publics[34] permet d'englober uniquement le principal domaine des transports publics, c'est-à-dire le transport de personnes concessionnaire ainsi que le transport de marchandises et l'infrastructure de chemins de fer.

Let. p: entreprises de l'aviation civile

Cette disposition soumet à l'obligation de signaler les cyberattaques toutes les entreprises disposant d'une autorisation de l'Office fédéral de l'aviation civile.

Let. q: navigation sur le Rhin

Les ports rhénans suisses constituent l'accès de la Suisse aux mers du monde et sont d'une grande importance pour l'approvisionnement de la Suisse en marchandises de toutes sortes. L'obligation de signaler les cyberattaques s'applique donc à la navigation sur le Rhin pour le transport de marchandises conformément à la loi fédérale du 23 septembre 1953 sur la navigation maritime sous pavillon suisse[35] et aux processus importants pour l'exploitation et le fonctionnement du port de Bâle.

Let. r: biens d'usage quotidien indispensables

Une multitude d'opérateurs sont impliqués dans l'approvisionnement de la population en biens d'usage quotidien indispensables, notamment en denrées alimentaires. Outre les producteurs et les importateurs, les transformateurs, les centres de distribution et les détaillants jouent également un rôle important. Tous ces opérateurs n'ont pas la même importance pour la sécurité de l'approvisionnement de la Suisse. L'obligation de signaler les cyberattaques ne doit s'appliquer qu'aux opérateurs qui jouent un rôle important à cet égard. Le Conseil fédéral limitera donc au niveau de l'ordonnance l'obligation de signalement dans le domaine de l'approvisionnement en biens d'usage quotidien indispensables conformément aux critères visés à l'art. 74*c*.

Let. s: fabricants de matériel et de logiciels informatiques

De plus en plus de cyberattaques d'infrastructures critiques ont lieu par le biais des fabricants de matériel et de logiciels. Les cyberpirates manipulent le matériel et les logiciels avant leur livraison aux clients finaux afin à pouvoir accéder ultérieurement aux systèmes. Les fabricants de matériel et de logiciels sont donc d'une grande importance pour la cybersécurité.

Les cyberattaques contre les fabricants de logiciels sont particulièrement importantes lorsque ceux-ci disposent d'un accès de télémaintenance. Les pirates peuvent tenter de s'introduire directement dans les systèmes des infrastructures critiques par ce genre d'accès légitime. Outre le critère de l'accès de télémaintenance, les fabricants de matériel et de logiciels sont soumis à l'obligation de signalement lorsque leurs produits sont utilisés dans des domaines particulièrement sensibles. Cela concerne le matériel et les logiciels de commande et de surveillance de systèmes (*industrial control systems*) (ch. 1) ainsi que l'exploitation de dispositifs médicaux et d'installations de télécommunication (ch. 2). Une attention particulière est également portée au matériel et aux logiciels utilisés pour garantir la sécurité publique (ch. 3). On pense ici, en particulier, à la communication des organisations d'intervention d'urgence ou aux systèmes d'enquête policière. En outre, les fabricants de matériel et de logiciels dotés de fonctions particulièrement sensibles (sécurité informatique, cryptage, identification, autorisation d'accès et contrôle d'accès) (ch. 4) doivent être soumis à l'obligation de signalement, car la manipulation de tels produits - qui sont justement utilisés en cas de besoin de protection accru - est dans tous les cas sensible.

34 RS **745.2**
35 RS **747.30**

Art. 74c Exceptions à l'obligation de signalement

Le cercle des assujettis visé à l'art. 74*b* est large et peut aussi englober des entreprises qui, prises individuellement, ne sont pas essentielles au bon fonctionnement de l'économie ou au bien-être de la population, bien qu'elles soient actives dans un sous-secteur critique. L'art. 74*c* précise donc que le Conseil fédéral limite davantage le cercle des assujettis. Il utilise à cette fin les critères énumérés et exempte de l'obligation de signalement les entreprises ou les catégories d'entreprises qui sont peu exposées au risque de cyberattaques, de telles attaques étant jugées improbables état donné que l'exploitation des entreprises concernées ne dépend que dans une faible mesure des moyens informatiques (let. a). L'exemption peut également advenir si la défaillance ou le dysfonctionnement n'ont qu'un faible impact sur l'économie ou le bien-être de la population, l'impact se mesurant à l'aune du nombre de personnes concernées, de la substituabilité de la prestation ou du potentiel de dommages économiques (let. b).

Art. 74d Cyberattaques à signaler

Al. 1

La portée de l'obligation de signalement, c'est-à-dire le type de cyberattaques qui doivent être signalées, doit être fixée dans la loi. L'al. 1 énumère, aux let. a à d, les critères permettant de conclure qu'une cyberattaque a un potentiel de dommages important ou une grande pertinence pour la protection d'autres infrastructures critiques. Si une cyberattaque remplit l'un de ces critères, elle doit être signalée. Les critères pourront au besoin être précisés dans l'ordonnance.

Al. 2

L'al. 2 stipule qu'une cyberattaque doit toujours être signalée lorsqu'elle s'accompagne d'actes pénalement répréhensibles. De nombreux cybercriminels tentent de faire chanter les exploitants d'infrastructures critiques ou certains collaborateurs de ces entreprises en menaçant de lancer des attaques ou en les exécutant (par ex. en chiffrant les données à l'aide d'un rançongiciel [*ransomware*], en menaçant de compromettre la disponibilité au moyen d'attaques de déni de service distribué [DDoS] ou en menaçant de publier des informations compromettantes sur des personnes). Les attaques de ce genre doivent être signalées afin de pouvoir évaluer l'ampleur de la menace que les cybercriminels font peser sur les infrastructures critiques.

Art. 74e Contenu du signalement

L'al. 1 indique les informations essentielles à fournir en vue du respect de l'obligation du signalement. Le contenu concret de ces diverses informations sera précisé dans les dispositions d'exécution.

L'al. 2 précise le caractère immédiat du signalement *(«le plus rapidement possible»*) visé à l'art. 74*a*, indiquant que celui-ci ne concerne que les informations déjà connues. En cas de cyberattaque, on ignore très souvent pendant un certain temps à quel point l'attaque est grave et ce qui s'est passé précisément. Si ces informations sont incomplètes au moment du signalement, les entreprises concernées doivent par conséquent avoir la possibilité de ne transmettre les informations exigées conformément au ch. 1 que lorsqu'elles disposent de plus de détails sur la cyberattaque.

Art. 74f Communication du signalement

Al. 1

Afin que l'obligation de signalement puisse être remplie avec le moindre effort possible, il incombe au NCSC de mettre à disposition un formulaire électronique sécurisé. Compte tenu des développements technologiques, le formulaire est décrit de manière générique comme «un système sécurisé qui permet de lui communiquer le signalement». Hormis ce formulaire, il est néanmoins possible dans tous les cas de communiquer d'une autre manière (par courriel ou par téléphone) la cyberattaque au NCSC.

Al. 2

Le système de communication offre à l'auteur du signalement la possibilité de communiquer simultanément à d'autres services et autorités tout ou partie du signalement de la cyberattaque ou de ses conséquences (par ex. sur la sécurité des données ou sur le fonctionnement de l'infrastructure critique). Cette communication via le système du NCSC n'est pas soumise à obligation légale de signalement vis-à-vis d'autres services et autorités; elle est également possible pour les signalements volontaires à des organismes tiers. Il est important de noter que la communication du signalement ne peut être effectuée que par l'exploitant de l'infrastructure critique concernée. C'est lui seul qui détermine quel service ou quelle autorité - en dehors du NCSC - doit recevoir la communication de la cyberattaque ou de ses conséquences. Le NCSC ne transmet aucune communication à d'autres services ou autorités. Sont réservés les cas exceptionnels visés à l'article 73*c*, al. 1 et 2.

Al. 3

Sur demande et en collaboration avec d'autres services de communication, le NCSC peut aménager le système de manière à ce que l'exploitant d'une infrastructure critique soumis à l'obligation de signalement puisse saisir d'éventuelles données supplémentaires qui ne sont pas nécessaires pour le signalement au NCSC, afin de les transmettre à un ou plusieurs autres services de communication. Cette fonction doit servir à réduire au minimum la charge de travail des auteurs d'un signalement. Elle doit les aider, notamment en cas de cumul de plusieurs obligations de signalement, à pouvoir informer les services et autorités concernés le plus rapidement possible, en temps utile et avec le mois d'effort possible. Les informations supplémentaires que les auteurs d'un signalement saisissent pour d'autres services et autorités dans le système de communication du NCSC sont uniquement transmises par ce dernier, sans être enregistrées. Le NCSC lui-même n'a pas la possibilité d'accéder à ces informations.

Art. 74g Obligation de fournir des renseignements

L'obligation de fournir des renseignements est limitée aux informations dont le NCSC a besoin pour identifier le mode opératoire et la méthode d'une cyberattaque signalée (alerte précoce) et, ainsi, pour en prévenir les répercussions sur d'autres infrastructures critiques.

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

Al. 1

En cas d'infraction à l'obligation de signalement ou à l'obligation de fournir des renseignements, le NCSC doit, dans un premier temps, rendre l'exploitant de l'infrastructure critique attentif à l'infraction commise. Ce dernier a ainsi encore l'occasion de s'acquitter de ses obligations. S'il y a un malentendu à ce sujet, il est alors possible de le régler. Le NCSC est tenu de prendre ce premier contact. Il s'agit d'une condition préalable à l'adoption d'une décision en vertu de l'al. 2.

Al. 2

Dans un second temps, soit si l'exploitant ne fait rien alors même qu'il a manifestement manqué à ses obligations, le NCSC rend une décision assortie d'une menace d'amende. Dans sa décision, le NCSC doit préciser les obligations enfreintes de façon à ce qu'il n'y ait aucun doute pour l'exploitant de l'infrastructure critique sur ce qu'il doit faire ou ne pas faire. Cela facilite également le travail des autorités de poursuite pénale, qui, en cas de non-observation de cette décision, doivent établir les faits et rendre un arrêt ou une ordonnance pénale (cf. art. 74*i*).

Art. 74i Non-observation de décisions du NCSC

Cet article reprend en grande partie la réglementation prévue aux art. 63 ss nLPD en cas d'insoumission à une décision du préposé par les entreprises commerciales. Comme l'indique le message

de la loi révisée sur la protection des données[36], il s'agit aussi dans le cas d'espèce de veiller à ce que soit punissable la personne responsable qui, au sein de l'infrastructure critique, aurait dû faire exécuter la décision du NCSC (cf. art. 29 CP[37]). Le devoir violé qui incombe à l'entreprise est ici imputé à cette personne physique. Le renvoi à l'art. 6 de la loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA)[38] permet d'attribuer la responsabilité pénale à la direction de l'entreprise, c'est-à-dire aux personnes occupant une fonction dirigeante et disposant de pouvoirs de décision et de direction. Cela permet d'imputer de manière appropriée la responsabilité pénale au sein des infrastructures critiques.

Al. 1

Le montant maximal de l'amende a été fixé à 100 000 francs afin de tenir dûment compte de l'importance des infrastructures critiques pour le bon fonctionnement de l'économie et de l'État ainsi que de bien montrer leur responsabilité dans le domaine de la cybersécurité. Un montant aussi élevé se justifie également par le fait que l'amende n'est prononcée qu'en dernier ressort, après toute une succession de mesures. Tant le niveau de cybersécurité, qui varie d'un secteur à l'autre, que les exigences supplémentaires liées au nouveau régime de signalement des cyberattaques ont conduit à ne pas reprendre le montant maximal de 250 000 francs prévu dans la loi révisée sur la protection des données. La menace d'une amende de 100 000 francs devrait déjà amener les responsables d'infrastructures critiques à agir en conformité avec leurs obligations.

Al. 2 et 3

Pour les amendes infligées à des entreprises, la réglementation a été reprise par analogie à la loi révisée sur la protection des données (art. 64 nLPD). Jusqu'à un montant de 20 000 francs, l'amende peut ainsi être directement infligée à l'infrastructure critique à la place de la personne physique responsable, afin d'éviter une coûteuse enquête. Étant donné qu'une amende ne peut dépasser 100 000 francs, le législateur a fixé à 20 000 francs le montant pour ces cas de faible importance afin de responsabiliser les infrastructures critiques en tant que telles et de renoncer à des enquêtes supplémentaires concernant les personnes responsables. Si l'on pense que l'obligation de signaler se concentre sur les principales infrastructures critiques, lesquelles peuvent bien souvent prétendre à une part de marché significative, aucun argument ne justifie de fixer le montant maximal de 20 000 francs à un niveau plus bas.

Al. 4

Pour des raisons de transparence, l'al. 4 mentionne, par analogie à l'art. 65 nLPD, la compétence des autorités cantonales de poursuite pénale au cas où une décision du NCSC ne serait pas suivie d'effet. Le législateur a décidé de ne pas mentionner le droit de dénonciation du NCSC, car cette circonstance découle du contexte.

Section 3 Protection des données et échange d'informations

Les art. 75 à 79, qui sont désormais regroupés dans la section 3, ont dû être adaptés tant sur le plan linguistique que sur le plan du contenu afin de correspondre à l'ancrage légal des tâches du NCSC. Avec sa centrale d'enregistrement, le NCSC remplace MELANI, qui était exploité conjointement par l'ancienne Unité de pilotage informatique de la Confédération (UPIC) et le SRC. Comme le SRC a un mandat légal d'évaluation de la menace et de détection précoce pour les exploitants d'infrastructures critiques, la collaboration du NCSC avec le SRC et la transmission d'informations et de données doivent, dans la mesure nécessaire, être réglées dans la LSI.

36 Message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF *2017* 6597, 6603, 6718.
37 RS **311.0**
38 RS **313.0**

Art. 75 Traitement des données personnelles

Al. 1

En lieu et place d'une description générique des services fédéraux compétents, le NCSC a été ajouté, étant précisé que celui-ci peut traiter non seulement des données personnelles, mais aussi des données sensibles et les données sensibles qui s'y rapportent. On entend par ressource d'adressage au sens de l'art. 3, let. f, LTC «la suite de chiffres, de lettres ou de signes ou toute autre information permettant d'identifier une personne, un processus informatique, une machine, un appareil ou une installation de télécommunication qui intervient dans une opération de télécommunication». À la let. a, le terme de «cybersécurité» a été ajouté.

Al. 2

L'al. 2 reprend l'ancien al. 3, la formulation ayant été transformée à la voix active dans la version allemande pour montrer plus clairement que le traitement des données est effectué par le NCSC. En outre, les conditions qui doivent être remplies lorsque la personne concernée n'est pas informée du traitement des données ont été concrétisées.

Al. 3

Le contenu de l'al. 3 a été précisé, à savoir que la personne concernée par une utilisation abusive de ressources d'adressage doit être informée de ce fait.

Art. 76 Collaboration sur le plan national

Cet article constitue la base légale pour l'échange d'informations entre le NCSC et les exploitants d'infrastructures critiques (al. 1 et 2) ainsi qu'entre le NCSC et les fournisseurs de services de télécommunication (al. 3 et 4).

Des adaptations formelles ont également été apportées. On a par exemple précisé dans chaque alinéa que la collaboration est soumise à la condition qu'elle soit nécessaire à la protection des infrastructures critiques contre les cyberrisques.

Al. 1 et 2

L'échange d'informations entre le NCSC et les exploitants d'infrastructures critiques réglé à l'al. 1 ne se limite pas aux infrastructures critiques assujetties à l'obligation de signalement, mais s'adresse à toutes les infrastructures critiques intéressées ayant leur siège en Suisse.

Al. 3 et 4

L'échange d'informations entre le NCSC et les fournisseurs de services de télécommunication a été explicitement réglé aux al. 3 et 4, car si la plupart de ces fournisseurs sont considérés comme des infrastructures critiques, ce n'est probablement pas le cas de tous.

Art. 76a Assistance technique aux autorités

Cette disposition est nouvelle. Elle règle les informations que le NCSC met à la disposition d'autres autorités, dans quelle mesure et à quelles fins. Elle détermine notamment le contenu et l'ampleur ainsi que les modalités de l'échange d'informations du NCSC avec le SRC, les autorités de poursuite pénale et les services cantonaux chargés de la cybersécurité (al. 2 à 4). Un des aspects importants de la collaboration du NCSC avec ces autorités concerne l'échange d'informations sur les pirates eux-mêmes et sur leurs méthodes et tactiques.

Al. 1

Contrairement aux alinéas suivants, l'al. 1 ne règle pas l'échange mutuel d'informations, mais établit le principe selon lequel le NCSC apporte son appui au SRC dans ses tâches en procédant à des évaluations spécifiques des cyberattaques quant à leur nombre, leur type et leur ampleur ainsi qu'à des analyses techniques des cyberrisques. Ces situations ne contiennent pas de données personnelles ou d'informations concrètes et spécifiques à chaque cas, mais se limitent aux évaluations statistiques et techniques nécessaires à l'évaluation de la menace et à l'alerte précoce. En vertu de l'art. 6, al. 2, LRens, le SRC a pour tâche d'apprécier la menace. Or le NCSC dispose, avec sa centrale d'enregistrement et l'obligation d'annonce, d'une importante source d'informations sur le niveau de menace lié aux cyberincidents. Il faut par conséquent qu'il puisse transmettre au SRC des informations sur le nombre de cyberattaques, leur type et leur ampleur. En outre, le NCSC doit pouvoir apporter son appui au SRC, en effectuant les analyses techniques des cyberattaques et en lui transmettant les résultats de ces analyses.

Al. 2, 3 et 4

Les al. 2 à 4 règlent le contenu, l'étendue et les modalités de l'échange d'informations du NCSC avec le SRC, les autorités de poursuite pénale et les services cantonaux chargés de la cybersécurité. Un des aspects importants de la collaboration du NCSC avec ces autorités est, comme déjà mentionné, l'échange d'informations sur les agresseurs eux-mêmes et sur leurs méthodes et tactiques. Ces informations peuvent être de nature purement technique (par ex. mode opératoire ou valeurs de hachage des maliciels) et ne pas renfermer de données personnelles. Mais ces autorités échangent également entre elles des informations personnelles ou permettant d'établir un lien avec des personnes données. Aussi une base légale est-elle créée ici pour les échanges d'informations se rapportant à ces données personnelles. Concrètement, il s'agit de ressources d'adressage (comme le nom de domaine, l'adresse IP ou les adresses de messagerie utilisées de manière abusive) ou d'indications sur des transactions financières (comptes bancaires, numéro IBAN, etc.).

Les autorités habilitées en vertu des al. 2 à 4 peuvent également accéder en ligne aux informations susmentionnées. Cette procédure est indiquée en raison du grand nombre de cyberattaques et d'informations techniques associées. La transmission au SRC ou aux autorités de poursuite pénale de signalements contenant des informations sur les personnes concernées n'a lieu que dans des cas exceptionnels et reste soumise aux conditions prévues à l'art. 73*c*, al. 1 et 2.

Art. 77 Coopération internationale

Cette disposition a été adaptée sur le plan formel par une mention expresse au NCSC. En outre, le terme de «données» a été remplacé par le terme générique d'«informations», qui ne désigne pas spécifiquement les données personnelles au sens de l'art. 75. On a ajouté concrètement à propos de l'étendue, du contenu et de la finalité de l'échange d'informations que celui-ci est autorisé avec les services chargés de la cybersécurité. Le terme «cybersécurité» remplace l'expression «protection des infrastructures critiques», dont la formulation est trop restrictive, pour décrire les organisations d'envergure internationale actives dans le domaine de la cybersécurité.

Art. 78 Système d'information pour le soutien aux infrastructures critiques

Cet article a été supprimé au vu des modifications de bases légales relatives à la révision de la LPD. Les buts du traitement des données par le NCSC découlent de ses tâches, lesquelles sont décrites avec une précision suffisante dans les articles consacrés à la question. Ils fixent déjà ce qui peut être fait avec les systèmes d'information du NCSC, lors du traitement des données personnelles.

Art. 79 Conservation et archivage des données

Cet article n'a subi qu'une légère modification à son al. 1. On y a précisé que les données personnelles peuvent être conservées pendant cinq ans au plus à compter de leur dernière utilisation. Cette réglementation tient au fait que certaines informations techniques sur les cyberincidents, à l'instar du nom de domaine, de l'adresse IP ou des adresses de messagerie utilisées de manière abusive, revêtent une importance centrale lors des rapprochements entre les cyberincidents nouvellement signalés et l'analyse des méthodes d'attaque ou des modes opératoires. Faute de telles données de comparaison, le NCSC ne pourrait pas effectuer - ou du moins pas de manière ciblée - ses analyses, qui constituent une condition essentielle de l'accomplissement de ses tâches. Mais comme ces données techniques renferment aussi des éléments à caractère personnel et, à ce titre, sont soumises en tant que données personnelles à la protection des données, leur durée de conservation doit être clairement délimitée. Pour des raisons tenant à la protection des données, il a été précisé dans la deuxième partie de la phrase que les données personnelles sensibles peuvent être conservées au maximum deux ans à compter de leur dernière utilisation.

Art. 80 Dispositions édictées par le Conseil fédéral

Cet article a été supprimé. Le texte de loi ayant été suffisamment concrétisé, les délégations au Conseil fédéral qui sont prévues dans cette disposition sont devenues obsolètes. La compétence d'édicter des dispositions d'exécution revient au Conseil fédéral, même sans réserve de la loi. En outre, les dispositions d'exécution prévues à la let. c (responsabilité en matière de protection et de sécurité des données) sont déjà couvertes par les art. 8, al. 3, et 33 nLPD.

Annexe 1 (Art. 89 Modification d'autres actes)

La liste des modifications d'autres actes visée à l'art. 89 de l'annexe 1 est complétée comme suit.

Loi du 23 mars 2007 sur l'approvisionnement en électricité[39]

La protection contre les cyberrisques, qui figurera désormais explicitement à l'art. 8*a* de la loi sur l'approvisionnement en électricité, contribue à la sécurité d'approvisionnement. Les mesures prévues à l'al. 1 doivent permettre soit de prévenir, soit de régler au plus vite les cyberincidents et donc, en particulier, les dysfonctionnements des installations concernées. Outre les gestionnaires de réseau qui interviennent directement dans l'exploitation au moyen de technologies de pilotage, l'obligation vaut aussi pour les producteurs (par ex. exploitants d'éoliennes ou de centrales hydro-électriques) et pour les agents de stockage, d'autant plus qu'ils peuvent exercer une influence majeure sur la sécurité d'approvisionnement, lors de leurs activités d'injection et de prélèvement de courant. Pour juger du degré de protection adéquat, il faut examiner l'influence que l'opérateur en question peut avoir sur la sécurité d'approvisionnement (par ex. niveau du réseau, puissance, nombre de consommateurs finaux concernés).

Le Conseil fédéral formulera dans l'ordonnance les exigences en la matière, notamment en ce qui concerne le niveau de protection visé et les audits à effectuer. Pour ce faire, il pourra s'appuyer sur les normes spécialisées pertinentes (par ex. le manuel de l'Association du secteur électrique suisse, AES Protection de base pour les «technologies opérationnelles» [OT] dans l'approvisionnement en électricité, édition de juillet 2018, en cours de révision), qu'il pourra également déclarer contraignantes. Des exceptions ou des allégements seront à prévoir pour les plus petits opérateurs du marché.

Étant donné le but de cette disposition, seuls entrent en ligne de compte comme autres parties en vertu de l'al. 2 les opérateurs qui exercent une influence déterminante sur la sécurité d'approvisionnement, à l'instar des grands prestataires de services du secteur de l'électricité actifs, par exemple,

39 RS **734.7**

dans le commerce et la mesure de l'énergie, la gestion de la flexibilité, le traitement des données ou la mobilité électrique.

Modification du 25 septembre 2020 de la loi sur la protection des données[40]

Afin que le PFPDT puisse faire appel aux spécialistes techniques du NCSC lors de l'analyse d'une violation de la sécurité des données que le responsable lui a signalée en vertu de l'art. 24 nLPD et de l'art. 19 P-OLPD, l'art. 24, al. 5bis, nLPD prévoit que le PFPDT peut transmettre au NCSC le signalement d'une violation de la sécurité des données.

La transmission peut contenir toutes les indications prévues à l'art. 19, al. 1, P-OLPD, mais doit en même temps se limiter aux données nécessaires au NCSC pour qu'il analyse l'incident. L'annonce transmise par le PFPDT au NCSC peut également renfermer des données personnelles, y compris des données sensibles relatives à des poursuites ou à des sanctions administratives et pénales visant le responsable du traitement. Les informations nécessaires en vue de l'analyse d'un incident sont sélectionnées dans chaque cas d'espèce mais, dans certaines circonstances, des informations concernant une procédure en cours peuvent très bien parvenir indirectement au NCSC. Il faut par conséquent créer une base légale en vue de la divulgation de données sensibles.

La condition est ici que le responsable tenu d'informer le PFPDT ait donné son consentement préalable à la transmission de l'annonce. En outre, la transmission ne doit pas conduire à éluder l'art. 24, al. 6, révLPD, selon lequel l'annonce ne peut être utilisée dans le cadre d'une procédure pénale contre la personne tenue d'annoncer qu'avec son consentement. À l'art. 24 nLPD, le nouvel al. 5bis ne permet pas au PFPDT de transmettre systématiquement les signalements au NCSC. Au contraire, il ne peut faire usage de cette possibilité que dans les cas où il a besoin de l'expertise technique du NCSC pour élucider les circonstances d'un incident.

40 Loi fédérale du 25 septembre 2020 sur la protection des données (LPD), FF *2020* 7397.

5 Conséquences

5.1 Conséquences pour la Confédération

Le NCSC gère déjà à l'heure actuelle un service d'alerte qui recueille sur une base volontaire les signalements de cyberincidents. Il bénéficie en la matière de la longue expérience de MELANI, qui se chargeait déjà de cette tâche depuis 2004 pour les annonces spécifiques aux infrastructures critiques.

Le NCSC utilise déjà aujourd'hui un formulaire électronique pour la collecte des annonces. Il serait possible de l'adapter afin qu'il puisse aussi servir à la réception des données faisant suite à l'obligation de signalement. Un investissement initial sera certes indispensable en vue de l'harmonisation nécessaire avec les autres services collectant des annonces (par ex. PFPDT, FINMA, IFSN) et de la configuration du formulaire de signalement, mais il sera gérable avec les ressources dont dispose le NCSC. Celui-ci devra toutefois s'assurer, au stade de l'exploitation, que les signalements faisant suite à l'obligation en la matière soient correctement enregistrés, qu'ils fassent l'objet d'un accusé de réception, qu'ils soient dûment documentés et, enfin, qu'ils soient transmis aux services compétents à des fins de détection précoce. Ce surcroît de travail devra être pris en compte lors des développements futurs du NCSC.

Après une cyberattaque, le NCSC aide l'exploitant de l'infrastructure critique concernée à gérer l'incident. Cette prestation de soutien fonctionne déjà bien, grâce à la longue expérience du NCSC (et, auparavant, de celle de MELANI). Il faut toutefois s'attendre à ce que la charge de travail du NCSC augmente en raison de l'obligation de signalement. Outre que ceux-ci seront plus nombreux, le NCSC devra procéder à une première évaluation et émettre les recommandations utiles pour régler l'incident. Il faudra dès lors étoffer encore son équipe chargée des analyses techniques (GovCERT).

Il s'agit de prendre en compte ces besoins supplémentaires dans l'actuel chantier d'extension du NCSC. Ceux-ci ne peuvent pas être suffisamment évalués indépendamment des autres tâches du NCSC, raison pour laquelle on attend le résultat de l'évaluation de l'efficacité de la cyberorganisation de la Confédération, actuellement en cours. Les besoins en ressources seront concrétisés au vu des résultats de la présente consultation dans le cadre du message.

5.2 Conséquences pour les cantons et les communes

Ce projet n'attribue pas de nouvelles tâches aux cantons et aux communes, mais ceux-ci sont concernés par l'obligation de signalement pour deux raisons: premièrement, les autorités cantonales et communales sont elles-mêmes soumises à l'obligation de signalement en vertu de l'art. 74*b*, let. b, et deuxièmement, de nombreuses entreprises soumises à cette obligation sont soutenues par des organismes cantonaux ou communaux.

En contrepartie, les cantons et les communes profitent également des prestations du NCSC pour mieux se protéger contre les cyberrisques. Aujourd'hui déjà, beaucoup de cantons et de villes participent aux échanges d'informations entre infrastructures critiques et sont intégrés au NCSC.

5.3 Conséquences pour l'économie et la société

Il ne devrait y avoir aucune conséquence directe pour l'économie, la société ou l'environnement. L'économie et la société profiteront indirectement de l'introduction d'une obligation d'annoncer les cyberattaques, étant donné que l'amélioration de la cybersécurité des infrastructures critiques sera positive pour la cybersécurité de tout le pays. Par ailleurs, l'obligation de signalement contribuera à éviter, grâce à des mesures de prévention et de défense précoce, que des cyberattaques lancées contre des infrastructures critiques n'entraînent des perturbations ou des pannes de services essentiels, mettant en péril le bon fonctionnement de l'économie et de l'État.

L'introduction d'une obligation de signaler les cyberattaques subies par les infrastructures critiques n'aura aucun impact pour l'économie ou les entreprises concernées, ou du moins ses conséquences resteront négligeables. Il est par conséquent possible de renoncer à une analyse d'impact de la réglementation (AIR).

L'obligation de signalement aide à faire la transparence sur la menace liée aux cyberattaques et contribue à sensibiliser la population aux cyberrisques. Des cybercompétences accrues au sein de la population sont la condition essentielle d'une fructueuse transformation numérique de la société.

6 Aspects juridiques

6.1 Constitutionnalité

La possibilité d'introduire une obligation de signaler les cyberattaques n'est pas expressément prévue dans la Constitution fédérale. Pour introduire une obligation de signaler les cyberattaques visant des infrastructures critiques, la Confédération peut s'appuyer sur sa compétence fédérale inhérente en matière de protection de la sécurité intérieure et extérieure de la Confédération.

Pour leur sécurité, la société, l'économie et l'État dépendent largement des infrastructures critiques. De par leurs conséquences potentiellement graves sur le plan suisse, les cyberattaques dirigées contre les infrastructures critiques menacent la prospérité du pays et risquent de compromettre sa sécurité tant intérieure qu'extérieure. L'introduction d'une obligation de signalement aide donc à préserver la stabilité économique, sociale et étatique du pays. Elle constitue la base de la coordination et de la rapidité de la gestion des événements. L'obligation de signaler les cyberattaques contre les infrastructures critiques a en outre pour but d'établir, à partir des signalements, une analyse du niveau de menace à des fins d'alerte précoce et de prévention des dangers. Il ressort de l'objectif de cette obligation que son champ d'application doit être limité aux cyberattaques visant des infrastructures critiques. Le droit de signaler les cyberincidents et les vulnérabilités, ouvert à tous, est complémentaire à la collecte d'informations supplémentaires et sert à la protection des infrastructures critiques.

En conséquence, la compétence dévolue à la Confédération de sauvegarder la sécurité intérieure et extérieure – avec des responsabilités qui, sans lui être expressément accordées, lui reviennent en tant qu'État – constitue une base constitutionnelle adéquate pour introduire des dispositions légales relatives à une obligation de signaler les cyberattaques et à un droit de signaler les cyberincidents et les points faibles.

L'art. 173, al. 2, Cst. est cité comme place réservée pour cette compétence dévolue à la Confédération en raison d'une convention formelle de technique législative[41]. Or la loi sur la sécurité de l'information mentionne en préambule (outre les art. 54, al. 1, 60, al. 1, 101, 102, al. 1, et 173, al. 1, let. a et b) également l'art. 173, al. 2, comme base de compétence déterminante. Il n'est donc pas nécessaire de compléter les dispositions constitutionnelles indiquées dans la LSI.

6.2 Compatibilité avec les obligations internationales de la Suisse

L'introduction d'une obligation de signaler les cyberattaques ne contrevient à aucune obligation internationale de la Suisse. Elle est comparable aux réglementations introduites au cours des dernières années par bien d'autres États, dont en particulier les États membres de l'UE.

6.3 Forme de l'acte à adopter

Le choix de compléter la LSI déjà adoptée pour en faire la base légale nécessaire à l'introduction de l'obligation de signalement semble idéal. Outre que le but, l'objet et le champ d'application de la LSI sont compatibles avec l'obligation de signalement faite aux infrastructures critiques, elle constitue la base légale formelle du NCSC en tant que centrale d'enregistrement. D'un point de vue systématique, l'obligation de signaler les cyberattaques ainsi que les tâches de protection de la cybersécurité incombant au NCSC peuvent être introduites au chapitre 5.

Il faudra encore décider, à propos des dispositions d'exécution relatives à l'obligation de signalement, si cette obligation doit faire l'objet d'une ordonnance à part entière ou compléter l'ordonnance en vigueur sur les cyberrisques.

41 Ch. marg. 25 des directives de la Confédération sur la technique législative (www.chf.admin.ch > Documentation > Accompagnement législatif > Directives sur la technique législative DTL)

6.4 Frein aux dépenses

Le projet ne contient pas de dispositions relatives aux subventions et ne prévoit ni crédits d'engagement, ni plafonds de dépenses (qui entraîneraient des dépenses supérieures à l'un des seuils définis par la loi).

6.5 Conformité aux principes de subsidiarité et d'équivalence fiscale

L'attribution et l'accomplissement de tâches étatiques se fondent sur le principe de subsidiarité (art. 5*a* Cst.). Conformément à l'art. 43*a*, al. 1, Cst., la Confédération n'assume que les tâches qui excèdent les possibilités des cantons ou qui nécessitent une réglementation uniforme par la Confédération. Simultanément, la Confédération doit faire un usage modéré de ses compétences et laisser suffisamment de latitude aux cantons dans l'accomplissement de leurs tâches.

Une obligation de signaler les cyberattaques ne peut être mise en œuvre de manière efficace qu'à condition de s'étendre à tout le territoire suisse et à tous les secteurs d'activités. Sans procédure de signalement uniforme ni centrale d'enregistrement, il sera impossible de venir à bout de cyberattaques déployées au-delà des frontières cantonales et des domaines de spécialisation. En vertu de la compétence dévolue à la Confédération, cette obligation a été limitée aux cyberattaques subies par les infrastructures critiques, dont l'impact constitue une menace pour la sécurité nationale et le bon fonctionnement de l'État. L'introduction de l'obligation de signalement constitue par conséquent une mesure conciliable avec le principe de subsidiarité (art. 5*a* en relation avec l'art. 43*a* Cst.).

Selon le principe d'équivalence fiscale statué à l'art. 43*a*, al. 2 et 3, Cst., toute collectivité bénéficiant d'une prestation de l'État prend en charge les coûts de cette prestation et toute collectivité qui prend en charge les coûts d'une prestation de l'État décide de cette prestation. Ce principe est respecté dans le cadre de l'introduction de l'obligation de signalement, étant donné que la Confédération couvrira les coûts d'exploitation de la centrale d'enregistrement. Pour les infrastructures critiques, cette obligation ne change pas grand-chose: elles pourront compter, comme jusqu'ici, sur le soutien du NCSC pour la gestion des incidents. L'obligation de signalement n'entraînera qu'un léger surcroît de charges par rapport aux signalements de cyberincidents effectués sur une base volontaire. Par conséquent, il n'y aura pas de véritables coûts supplémentaires, même dans le cas des infrastructures critiques gérées par les cantons ou les communes.

6.6 Délégation de compétences législatives

Selon le présent projet mis en consultation, les éléments centraux pour l'introduction de l'obligation de signaler les cyberincidents doivent être inscrits dans la loi.

Si nécessaire, le Conseil fédéral édictera des dispositions d'exécution pour concrétiser les dispositions légales. Il lui incombe notamment, en vertu de l'art. 74*c*, de restreindre davantage le cercle des assujettis à l'obligation de signalement. La loi définit les critères à appliquer à cet effet, mais il appartient au Conseil fédéral de déterminer par secteur quels critères seront appliqués et comment (par ex., en définissant des valeurs seuils appropriées).

6.7 Protection des données

Le projet mis en consultation a pratiquement repris telles quelles les exigences en matière de protection des données que le Parlement avait initialement adoptées au chapitre 5 de la LSI, dans le contexte du soutien apporté par la Confédération aux exploitants d'infrastructures critiques.

Le PFPDT a été consulté pour l'élaboration du projet mis en consultation. Il a également été question à cette occasion des possibilités de le coordonner avec l'obligation d'annoncer les infractions à la sécurité des données.

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le chef du Département fédéral des finances DFF

Berne, le 12 janvier 2022

Destinataires:
Partis politiques
Associations faîtières des communes, des villes et des régions de montagne
Associations faîtières de l'économie
Autres milieux intéressés

Obligation de signaler les cyberattaques contre des infrastructures critiques: ouverture de la procédure de consultation

Madame, Monsieur,

Le 12 janvier 2022, le Conseil fédéral a chargé le Département fédéral des finances (DFF) de mener auprès des cantons, des partis politiques, des associations faîtières des communes, des villes et des régions de montagne, des associations faîtières de l'économie et des autres milieux intéressés une procédure de consultation relative à l'introduction d'une obligation de signaler les cyberattaques et à la modification de la loi sur la sécurité de l'information (LSI) qui en découle.

La consultation se terminera le **14 avril 2022**.

Les cyberrisques représentent l'une des principales menaces pour la sécurité et l'économie de la Suisse. Il est essentiel que les attaques contre les entreprises et les autorités suisses puissent être détectées à un stade précoce et que les menaces puissent être évaluées aussi précisément que possible. À cette fin, l'avant-projet de loi qui vous est soumis vise à instaurer une obligation de signalement pour les exploitants d'infrastructures critiques. Cette obligation doit permettre au Centre national pour la cybersécurité (NCSC) d'avoir une meilleure vue d'ensemble des cyberattaques en Suisse, d'aider les victimes concernées à gérer les cyberattaques et d'avertir les autres exploitants d'infrastructures critiques. L'introduction de l'obligation de signalement comble une lacune dans le dispositif de la cybersécurité. Des obligations de signaler les cyberattaques sont déjà établies dans de nombreux pays. Dans les États membres de l'UE, elles sont en vigueur depuis 2018.
L'avant-projet de loi est harmonisé avec les obligations de déclaration existantes (notamment avec celles prévues par le nouveau droit sur la protection des données) et conçu de manière à entraîner le moins de charges administratives possible pour les entreprises et les autorités concernées. Dans ce cadre, la création d'une centrale d'enregistrement au niveau fédéral (NCSC) est nécessaire, seul un organisme central pouvant garantir que l'obligation de signalement remplit les objectifs d'alerte précoce et d'une meilleure vue d'ensemble des cybermenaces. L'avant-projet de loi crée également les bases d'une collaboration du NCSC avec d'autres services, en particulier avec les autorités d'exécution pénale.

Nous vous invitons à prendre position sur les commentaires figurant dans le rapport explicatif, en particulier en ce qui concerne la mise en œuvre de la réglementation proposée.

La consultation est menée par voie électronique.
La documentation correspondante peut être téléchargée sur le site:

http://www.admin.ch/ch/f/gg/pc/pendent.html

Nous nous efforçons de publier les documents sous une forme accessible aux personnes handicapées, conformément à la loi sur l'égalité pour les handicapés (LHand; RS 151.3). Aussi vous saurions-nous gré de nous faire parvenir dans la mesure du possible votre avis sous forme électronique (**prière de joindre une version Word en plus d'une version PDF**) à l'adresse suivante, dans la limite du délai imparti:

ncsc@gs-efd.admin.ch

Nous vous serions également reconnaissants de bien vouloir nous communiquer le nom et les coordonnées des personnes auxquelles nous pourrons faire appel si nous avons des questions.

M. Manuel Suter, bureau du NCSC (tél.: 058 461 43 20) et M^{me} Angelika Spiess, service juridique du Secrétariat général du DFF (tél.: 058 467 68 03), se tiennent à votre disposition pour toute question ou information complémentaire.

Veuillez recevoir, Madame, Monsieur, l'assurance de ma considération distinguée.

Ueli Maurer

Liste der Vernehmlassungsadressaten
Liste des destinataires consultés
Elenco dei destinatari della consultazione

Art. 4 Abs. 3 Vernehmlassungsgesetz (SR 172.061)

1. Kantone / Cantons / Cantoni

Staatskanzlei des Kantons Zürich	Neumühlequai 10 Postfach 8090 Zürich
Staatskanzlei des Kantons Bern	Postgasse 68 3000 Bern 8
Staatskanzlei des Kantons Luzern	Bahnhofstrasse 15 6002 Luzern
Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf
Staatskanzlei des Kantons Schwyz	Regierungsgebäude Bahnhofstrasse 9 Postfach 1260 6431 Schwyz
Staatskanzlei des Kantons Obwalden	Rathaus 6061 Sarnen
Staatskanzlei des Kantons Nidwalden	Dorfplatz 2 Postfach 1246 6371 Stans
Staatskanzlei des Kantons Glarus	Rathaus 8750 Glarus
Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug
Chancellerie d'Etat du Canton de Fribourg	Rue des Chanoines 17 1701 Fribourg
Staatskanzlei des Kantons Solothurn	Rathaus Barfüssergasse 24 4509 Solothurn
Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel
Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal

Staatskanzlei des Kantons Schaffhausen	Beckenstube 7 8200 Schaffhausen
Kantonskanzlei des Kantons Appenzell Ausserrhoden	Regierungsgebäude 9102 Herisau
Ratskanzlei des Kantons Appenzell Innerrhoden	Marktgasse 2 9050 Appenzell
Staatskanzlei des Kantons St. Gallen	Regierungsgebäude 9001 St. Gallen
Standeskanzlei des Kantons Graubünden	Reichsgasse 35 7001 Chur
Staatskanzlei des Kantons Aargau	Regierungsgebäude 5001 Aarau
Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld
Cancelleria dello Stato del Cantone Ticino	Piazza Governo 6 6501 Bellinzona
Chancellerie d'Etat du Canton de Vaud	Place du Château 4 1014 Lausanne
Chancellerie d'Etat du Canton du Valais	Planta 3 1950 Sion
Chancellerie d'Etat du Canton de Neuchâtel	Le Château Rue de la Collégiale 12 2000 Neuchâtel
Chancellerie d'Etat du Canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3
Chancellerie d'Etat du Canton du Jura	2, rue de l'Hôpital 2800 Delémont
Konferenz der Kantonsregierungen (KdK) Conférence des gouvernements cantonaux (CdC) Conferenza dei Governi cantonali (CdC)	Sekretariat Haus der Kantone Speichergasse 6 Postfach 3001 Bern

2. In der Bundesversammlung vertretene politische Parteien / partis politiques représentés à l'Assemblée fédérale / partiti rappresentati nell'Assemblea federale

Die Mitte Le Centre Alleanza del Centro	Generalsekretariat Hirschengraben 9 Postfach 3001 Bern
Eidgenössisch-Demokratische Union EDU Union Démocratique Fédérale UDF Unione Democratica Federale UDF	Postfach 3602 Thun
Ensemble à Gauche EAG	Case postale 2070 1211 Genève 2
Evangelische Volkspartei der Schweiz EVP Parti évangélique suisse PEV Partito evangelico svizzero PEV	Nägeligasse 9 Postfach 3001 Bern
FDP. Die Liberalen PLR. Les Libéraux-Radicaux PLR. I Liberali Radicali	Generalsekretariat Neuengasse 20 Postfach 3001 Bern
Grüne Partei der Schweiz GPS Parti écologiste suisse PES Partito ecologista svizzero PES	Waisenhausplatz 21 3011 Bern
Grünliberale Partei Schweiz glp Parti vert'libéral Suisse pvl Partito verde liberale svizzero pvl	Monbijoustrasse 30 3011 Bern
Lega dei Ticinesi (Lega)	Via Monte Boglia 3 Case postale 4562 6904 Lugano
Partei der Arbeit PDA Parti suisse du travail PST	Postfach 8721 8036 Zürich
Schweizerische Volkspartei SVP Union Démocratique du Centre UDC Unione Democratica di Centro UDC	Generalsekretariat Postfach 8252 3001 Bern
Sozialdemokratische Partei der Schweiz SPS Parti socialiste suisse PSS Partito socialista svizzero PSS	Zentralsekretariat Theaterplatz 4 Postfach 3001 Bern

3. Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete / associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national / associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna

Schweizerischer Gemeindeverband Association des Communes Suisses Associazione dei Comuni Svizzeri	Laupenstrasse 35 3008 Bern
Schweizerischer Städteverband Union des villes suisses Unione delle città svizzere	Monbijoustrasse 8 Postfach 3001 Bern
Schweizerische Arbeitsgemeinschaft für die Berggebiete Groupement suisse pour les régions de montagne Gruppo svizzero per le regioni di montagna	Seilerstrasse 4 Postfach 3001 Bern

4. Gesamtschweizerische Dachverbände der Wirtschaft / associations faîtières de l'économie qui œuvrent au niveau national / associazioni mantello nazionali dell'economia

economiesuisse Verband der Schweizer Unternehmen Fédération des entreprises suisses Federazione delle imprese svizzere Swiss business federation	Hegibachstrasse 47 Postfach 8032 Zürich
Schweizerischer Gewerbeverband (SGV) Union suisse des arts et métiers (USAM) Unione svizzera delle arti e mestieri (USAM)	Schwarztorstrasse 26 Postfach 3001 Bern
Schweizerischer Arbeitgeberverband Union patronale suisse Unione svizzera degli imprenditori	Hegibachstrasse 47 Postfach 8032 Zürich
Schweiz. Bauernverband (SBV) Union suisse des paysans (USP) Unione svizzera dei contadini (USC)	Laurstrasse 10 5201 Brugg
Schweizerische Bankiervereinigung (SBV) Association suisse des banquiers (ASB) Associazione svizzera dei banchieri (ASB) Swiss Bankers Association	Postfach 4182 4002 Basel
Schweiz. Gewerkschaftsbund (SGB) Union syndicale suisse (USS) Unione sindacale svizzera (USS)	Monbijoustrasse 61 Postfach 3000 Bern 23

Kaufmännischer Verband Schweiz Société suisse des employés de commerce Società svizzera degli impiegati di commercio	Hans-Huber-Strasse 4 Postfach 1853 8027 Zürich
Travail.Suisse	Hopfenweg 21 Postfach 5775 3001 Bern

5. Weitere interessierte Kreise / autres milieux concernés / altre cerchie interessate

Schweizerische Informatikkonferenz (SIK) Conférence suisse sur l'informatique (CSI) Conferenza svizzera sull'informatica (CSI)	Haus der Kantone Speichergasse 6 3011 Bern sekretariat@sik.swiss
Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)	Haus der Kantone Speichergasse 6 3011 Bern info@kkjpd.ch
Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (GDK)	Haus der Kantone Speichergasse 6 3011 Bern office@gdk-cds.ch
Regierungskonferenz Militär, Zivilschutz, Feuerwehr	Haus der Kantone Speichergasse 6 3011 Bern Alexander.Krethlow@rkmzf.ch
Schweizerische Staatsanwälte-Konferenz	Haus der Kantone Speichergasse 6 3011 Bern info@ssk-cps.ch
Bau-, Planungs- und Umweltdirektoren-Konferenz BPUK	Haus der Kantone Speichergasse 6 3011 Bern info@bpuk.ch
Verein eCH Association eCH	Mainaustrasse 30 Postfach 8034 Zürich info@ech.ch
Geschäftsstelle eJustice.CH Secrétariat eJustice.CH Segreteria eJustice.CH	Postfach 3134 3001 Bern info@eJustice.ch
digitalswitzerland	Waisenhausplatz 14 3011 Bern info@digitalswitzerland.ch

Schweizer Informatik Gesellschaft SI	Schwarztorstrasse 31 3007 Bern admin@s-i.ch
Geschäftsstelle Digitale Schweiz (GDS) Direction opérationnelle Suisse numérique (GDS) Direzione operativa Svizzera digitale (GDS)	Zukunftstrasse 44 2501 Biel / Bienne www.digitaldialog.swiss
privatim, Konferenz der schweizerischen Datenschutzbeauftragten privatim, Conférence des Préposé(e) suisses à la protection des données	c/o Dr. Beat Rudin, Advokat, Postfach 205 4010 Basel kommunikation@privatim.ch
eHealth Suisse	Schwarzenburgstrasse 157 3003 Bern info@e-health-suisse.ch
asut – Schweizerischer Verband der Telekommunikation	Hirschengraben 8 3011 Bern info@asut.ch
ASIP – Schweizerischer Pensionskassenverband	Kreuzstrasse 26 8008 Zürich info@asip.ch
Stiftung Auffangeinrichtung BVG	Elias-Canetti-Strasse 2 8050 Zürich
Verein Vorsorge Schweiz VVS	Aeschengraben 29 4051 Basel info@verein-vorsorge.ch
Inter-pension Interessengemeinschaft autonomer Sammel- und Gemeinschaftseinrichtungen	Gartenstrasse 2 3063 Ittigen info@inter-pension.ch
PK-Netz 2. Säule	Monbijoustrasse 61 3007 Bern info@pk-netz.ch
Konferenz der kantonalen BVG- und Stiftungsaufsichtsbehörden	Sekretariat Monica Schiesser Aeberhard m.schiesser@gmx.ch
IV-Stellen-Konferenz (IVSK)	Sempacherstrasse 15 6003 Luzern Schweiz
Konferenz der kantonalen Ausgleichskassen (KKAK)	Genfergasse 10 3011 Bern info@ahvch.ch
Vereinigung der Verbandsausgleichskassen (VVAK)	Kapellenstrasse 14 Postfach 3001 Bern info@vvak.ch

Seilbahnen Schweiz	Giacomettistrasse 1 3006 Bern info@seilbahnen.org
Verband Schweizerischer Schifffahrtsunternehmen VSSU	Mythenquai 333 8038 Zürich info@vvssu.ch
RAILplus AG	Hintere Bahnhofstrasse 85 5001 Aarau info@railplus.ch
swissnuclear	Postfach 1663 4601 Olten info@swissnuclear.ch
SwissGrid AG	Bleichemattstrasse 31 5001 Aarau info@swissgrid.ch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Berne, 2 décembre 2022

Avant-projet de 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 sur les résultats de la consultation

Table des matières

1 Contexte

Le 12 janvier 2022, le Conseil fédéral a adopté l'avant-projet de modification de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information (LSI) et le rapport explicatif correspondant, et il a chargé le Département fédéral des finances (DFF) de mener une procédure de consultation. La procédure de consultation a duré du 12 janvier au 14 avril 2022. La liste des participants à la consultation, avec les abréviations utilisées dans le présent rapport, figure en annexe.
Au total, 99 avis ont été reçus:

99	**avis reçus au total**
25	gouvernements cantonaux
4	conférences cantonales
7	partis
1	association faîtière des communes, des villes et des régions de montagne qui œuvre au niveau national
4	associations faîtières de l'économie qui œuvrent au niveau national
19	entreprises concernées
39	autres milieux intéressés

Les prises de position sont mises en ligne sur la plateforme de publication du droit fédéral «Fedlex».[1].

2 Objet de l'avant-projet mis en consultation

L'avant-projet vise à inscrire dans la loi sur la sécurité de l'information (LSI) adoptée par le Parlement le 18 décembre 2020 la base légale nécessaire à l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques.

L'obligation de signalement ne s'appliquera qu'aux cyberattaques recelant un certain potentiel de dommages. Les cyberincidents relevant de l'erreur humaine, par exemple une manipulation fautive commise involontairement par un collaborateur, n'auront pas besoin d'être déclarés. Il a également été décidé de ne pas étendre l'obligation de signalement aux vulnérabilités des moyens informatiques. L'obligation de signalement s'appliquera aux exploitants d'infrastructures critiques dans les sous-secteurs critiques. Le Centre national pour la cybersécurité (NCSC) assumera le rôle de centrale de signalement. Il réceptionnera également les signalements de cyberincidents et de vulnérabilités des moyens informatiques transmis à titre facultatif.

Les bases légales de l'obligation de signaler les cyberattaques sont intégrées au chapitre 5 de la LSI, à l'exception de quelques adaptations mineures du chapitre 1. Le chapitre 5 a subi un remaniement de fond pour qu'il puisse aussi régler les tâches du NCSC – qui, à l'heure actuelle, sont définies uniquement dans l'ordonnance sur les cyberrisques (OPCy)[2] – ainsi que le rôle de centrale de signalement des cyberattaques qu'endossera le NCSC.

L'introduction d'une obligation de signalement permettra à l'avenir de détecter précocement les cyberattaques, d'analyser le mode opératoire et d'avertir à temps les autres exploitants d'infrastructures critiques. L'obligation de signalement apportera ainsi une contribution essentielle au renforcement de la cybersécurité de la Suisse.

L'avant-projet ne porte pas sur l'introduction de normes minimales contraignantes en matière de cybersécurité pour les exploitants d'infrastructures critiques ni sur les exigences en matière de sécurité des produits informatiques.

1 www.fedlex.admin.ch > Procédures de consultation > Procédures de consultation terminées > 2022 > DFF
2 RS **120.73**

3 Résultats de la procédure de consultation

3.1 Évaluation globale du projet

89 participants à la consultation **approuvent** sur le fond les **objectifs et les orientations de l'avant-projet**, tout en émettant certaines réserves.

Avis positifs (sur 99 au total)	**89**
Gouvernements cantonaux	25
Conférences cantonales	4
Partis	6
Associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national	1
Associations faîtières de l'économie qui œuvrent au niveau national	3
Entreprises concernées	17
Autres milieux intéressés	33

7 participants à la consultation se sont expressément prononcés **contre l'avant-projet**.

Avis négatifs (sur 99 au total)	**7**
Gouvernements cantonaux	-
Conférences cantonales	-
Partis	1
Associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national	-
Associations faîtières de l'économie qui œuvrent au niveau national	1
Entreprises concernées	2
Autres milieux intéressés	3

Le Ministère public de la Confédération, SwissDigital et le parti pirate ont proposé des modifications matérielles, mais n'ont pas évalué le projet.
Le canton d'Obwald, la Conférence des procureurs de Suisse et la Fondation institution supplétive LPP ont explicitement renoncé à prendre position.

3.2 Résumé des réponses et des critiques principales

Tous les cantons (à l'exception du canton d'Obwald, qui a renoncé à prendre position), 4 conférences cantonales (CCDJP, CCPCS, CGMPS, CDS), 6 partis (PS, UDC, PLR, le Centre, les Verts, PVL), l'Union des villes suisses, 3 associations faîtières de l'économie qui œuvrent au niveau national (economiesuisse, Swiss Banking, USS), 17 entreprises (Abraxas, Axpo, les aéroports de Genève et Zurich, Helvetia Assurances, Migros, CFF, la Poste, Raiffeisen, Romande Energie, Salt, Sunrise, Suva, Swisscom, Swissgrid, SWITCH, les TPG) et la commune de Gachnang, 34 organisations intéressées (AEROSUISSE, asut, Association des banques étrangères en Suisse, Centre Patronal, CH++, Digitale Gesellschaft, digitalswitzerland, eAVS/AI, eGov-Schweiz, FER, GEM, Härting Rechtsanwälte, IG eHealth, Inter-pension, ASIP, Opération Libero, Pour Demain, Privatim, Santésuisse, , ISSS, RAILplus, USS, ASA, Swico, swissICT, Swissmem, SSIGE, Trust Valley, UniBE, VUD, UTP, AES, ABG, AEIS, UZH/UNIL PNR 77, UniGE) **saluent l'objectif et l'orientation du projet**.

La majorité des prises de position en faveur du présent projet demande expressément que l'obligation de signalement n'entraîne **pas de coûts élevés** pour l'économie publique ou privée (notamment les entreprises signalant un cyberincident), que la mise en œuvre de l'obligation de signalement se fasse de manière non bureaucratique et que la **charge administrative soit faible**. Tous les participants souhaitent des précisions et beaucoup de participants émettent des réserves sur certaines dispositions.

Les demandes de **précisions** concernent principalement les définitions (art. 5), la liste des domaines soumis à l'obligation de signalement (art. 74*b*) et les critères d'exception (art. 74*c*), la définition des cyberattaques à signaler (art. 74*d*), ainsi que les modalités de communication du signalement (art. 74*f*).

Des **réserves** ont été émises notamment sur les sanctions en cas de non-respect de l'obligation de signalement (art. 74*h* et 74*i*). 24 participants à la consultation **rejettent toute possibilité de sanctions**. Le principal argument avancé par ces derniers est que les amendes ne sont en principe pas le bon moyen pour faire respecter l'obligation de signalement. La mise en œuvre de l'obligation de signalement devrait, selon eux, plutôt être encouragée par des incitations au sens de prestations de soutien.

Il est également ressorti de cette consultation que la protection des informations issues des signalements – en particulier les données personnelles – revêt une importance majeure. En effet, six participants à la consultation (Swico, Privatim, le parti pirate, Digitale Gesellschaft, Romande Energie, VUD) ont exprimé de nombreuses réserves quant à **la transmission de données personnelles aux services de renseignement et aux autorités de poursuite pénale**.

De plus, certains participants à la consultation souhaitent que le projet soit élargi et ne se limite pas à l'introduction d'une obligation de signalement. Le NCSC devrait avoir la compétence d'**imposer des standards minimaux** aux exploitants d'infrastructures critiques et d'exiger la mise en œuvre de mesures telles que l'**installation de mises à jour de sécurité**. Dans ce contexte, il est également proposé que les exploitants d'infrastructures critiques soient soumis aux art. 6 à 10 LSI.

Les participants saluent le fait que les vulnérabilités puissent aussi être signalées au NCSC, et que celui-ci informe d'abord les fabricants des produits concernés selon les principes de la ***coordinated vulnerability disclosure*** et leur fixe un délai pour remédier aux vulnérabilités. Il est souhaité que les institutions signalant des vulnérabilités ne puissent pas être poursuivies pénalement et que les fabricants qui ne remédient pas à ces vulnérabilités dans le délai fixé par le NCSC puissent être exclus des marchés publics.

L'avant-projet tel qu'il est présenté est **rejeté** par l'UDC, l'usam, scienceindustries, swissuniversities, Coop, SWISS et une personne individuelle. Le MPC ne s'est pas expressément positionné pour ou contre l'avant-projet.

3.3 Demandes et remarques concernant l'avant-projet

3.3.1 Remarque préliminaire

Les remarques, propositions de modification et critiques portant sur les différentes dispositions sont exposées ci-après. Seuls les arguments principaux avancés dans une prise de position sont mentionnés. Les avis particulièrement détaillés sont retranscrits uniquement lorsque des modifications matérielles concrètes sont demandées. Pour plus de détails, il est renvoyé aux prises de position publiées sur Internet.
Le présent rapport ne mentionne pas le consentement tacite ou l'absence de commentaire relatif à un article. Ainsi, si le rapport fait état de nombreuses remarques concernant les dispositions, il n'en reste pas moins que la majorité des participants à la consultation approuvent fondamentalement de larges pans de la législation proposée. Aucun participant à la consultation ne s'est par ailleurs exprimé sur la systématique de la loi.

3.3.2 Demandes et remarques concernant les dispositions

3.3.2.1 Titre

Le canton **TG** propose de modifier le titre de l'acte, car selon lui, l'intitulé actuel suggère que le champ d'application de la loi est limité à la Confédération, alors que ce ne sera plus le cas après l'introduction d'une obligation de signalement.

3.3.2.2 Art. 1, al. 1 (But)

> [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.

Cet article a suscité 4 réactions portant essentiellement sur des adaptations conceptuelles.

❖ **Remarques générales sur l'art. 1, al. 1**

Migros propose de compléter l'art. 1 par une réglementation sur le champ d'application territorial.

Le canton **TG** estime que la séparation en let. a et b ne fait ici pas de sens.

❖ **Approbation de l'art. 1, al. 1**

Swiss Banking salue le fait que l'art. 1 inclue expressément «la capacité de résistance de la Suisse aux cyberrisques». L'art. 1 renforce ainsi les tâches du NCSC définies aux art. 73*a* ss.

❖ **Demandes de modification et suggestions concernant l'art. 1, al. 1**

- **Let. a**

L'ISSS et Härting Rechtsanwälte demandent que l'art. 1 soit complété de manière à préciser que la let. a s'applique à moins qu'une loi spéciale prévoie une compétence différente.

- **Let. b**

Swico demande que le terme «cyberrisques» soit remplacé par «menace», car le premier, selon **Swico**, ne peut pas être défini.

3.3.2.3 Art. 2, al. 5 (champ d'application)

> [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.

5 remarques d'ordre général ont été formulées concernant le champ d'application proposé.

❖ **Remarques générales sur l'art. 2, al. 5**

Swissmem ainsi que l'UZH, l'UNIL et le PNR 77 soulignent la nécessité de prendre en compte l'art. 6 LSI en plus des art. 73*a* à 79.

L'UZH, l'UNIL et le PNR 77 considèrent qu'il serait utile de prévoir la possibilité de saisir le NCSC pour constater si un exploitant est ou non soumis à la loi ou à l'obligation de signaler, à la manière de ce qui est prévu dans l'OSCPT par exemple (voir notamment l'art. 51 OSCPT).

Le canton **GE** demande une définition du terme «critiques».

❖ **Demandes de modification et suggestions concernant l'art. 2, al. 5**

L'ISSS et Härting Rechtsanwälte demandent que l'art. 2, al. 5, s'applique aussi aux infrastructures critiques *visées par l'art. 74b*, afin de préciser que l'on parle d'infrastructures critiques telles que définies dans la LSI.

3.3.2.4 Art. 5, let. d et e (Définitions)

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.

23 participants à la consultation se sont exprimés sur les deux définitions et tous ont soumis des propositions de modification.

❖ **Remarques générales sur l'art. 5**

Economiesuisse, IG eHealth, la Poste et VUD considèrent qu'il faudrait définir avec plus de précision les termes «cyberincident» et «cyberattaque» à l'art. 5.

Le **Centre de droit du numérique de l'UNIGE** demande que les définitions de «cyberattaque» et «cyberincident» soient précisées, afin que ces événements puissent être qualifiés comme tels aussi en l'absence de toute violation de la sécurité des données ou d'autres dispositions légales ou réglementaires.

❖ **Demandes de modification et suggestions concernant l'art. 5**

IG eHealth, l'ISSS, Härting Rechtsanwälte, le canton GE et la Poste considèrent qu'il faut ajouter une définition des notions de «vulnérabilité» et de «cyberrisque» à l'art. 5.
La **commune de Gachnang** est d'avis qu'il faut définir le préfixe «cyber».

- **Let. d**

Pour Demain suggère de mentionner explicitement l'intelligence artificielle dans le cadre de la définition de «cyberincident».

Migros, Sunrise, les TPG et digitalswitzerland demandent que la formulation «et pouvant avoir pour conséquence» soit modifiée. Les trois derniers estiment qu'il faudrait la remplacer par «et ayant pour conséquence», tandis que **Migros** demande une meilleure définition.

Santésuisse considère que la définition n'est pas assez précise, car de tels événements peuvent également se produire sans être déclenchés par une cyberattaque, par exemple en raison de la défaillance de composants informatiques ou d'erreurs de programmation. Santésuisse estime que ces événements ne doivent pas être couverts par l'obligation de signalement.

L'UZH, l'UNIL et le PNR 77 sont d'avis qu'il est nécessaire d'harmoniser la définition de «cyberincident» avec celle prévue à l'art. 3, let. b, OPCy. En outre, ils considèrent que la formulation «lors de l'exploitation de moyens informatiques» n'est pas optimale, dans la mesure où elle pourrait être considérée comme trop restrictive en excluant tout comportement passif.

- **Let. e**

Swissgrid demande si la définition de «tiers non autorisé» inclut uniquement des personnes externes ou aussi des internes.

3.3.2.5 Art. 73*a* 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.

16 participants à la consultation se sont exprimés, parfois de manière très détaillée, sur les principes proposés. 2 participants sont satisfaits de l'art. 73*a* en l'état, 5 demandent qu'une tâche soit ajoutée à la liste, et 9 autres ont émis des commentaires et demandent d'autres modifications.

❖ **Remarques générales sur l'art. 73*a***

CH++ soutient l'article, mais considère que le NCSC devrait y ajouter la détection active des vulnérabilités et des menaces.

La **commune de Gachnang** soutient l'article, mais considère qu'un reporting régulier à des fins d'assurance qualité et de contrôle des résultats doit être inclus dans les tâches énumérées à l'art. 73*a*.

Migros demande une liste non exhaustive d'exemples pour soutenir le propos de l'art. 73*a*.

Le canton **BE** demande que l'art. 73*a* soit complété par un deuxième alinéa précisant que le NCSC accomplit ses tâches en collaboration avec les autorités policières des cantons.

Swisscom soutient l'article, mais considère qu'en plus des tâches et compétences mentionnées, il est nécessaire que la loi précise que le NCSC soutient non seulement la Confédération, mais aussi l'économie et la société.

❖ **Approbation de l'art. 73*a***

Swico, Suissedigital et swissICT saluent expressément la création de bases légales pour les tâches du NCSC.

❖ **Demandes de modification et suggestions concernant l'art. 73*a***

- **Let. b**

Pour Demain souhaite que les tâches du NCSC incluent les risques liés à l'intelligence artificielle.

- **Let. c**

Swiss Banking et Raiffeisen soutiennent l'article mais considèrent que des «instructions sur les mesures préventives et réactives à prendre contre les cyberrisques» ne sont utiles que si elles ne sont pas obligatoires.

- **Let. f**

Les Verts demandent que le "soutien aux exploitants d'infrastructures critiques" (art. 73a, let. F) doit également être envisagé de manière plus large que ne le prévoient les explications et les définitions actuelles.

3.3.2.6 Art. 73*b* 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.

21 participants à la consultation se sont exprimés. De manière générale, c'est l'al. 3 qui a suscité les plus vives réactions.

- **Remarques générales sur l'art. 73*b***

Scienceindustries considère que la mise en œuvre de l'obligation de signalement nécessite que celle-ci représente une plus-value pour les entreprises concernées, qu'elle suive une approche proportionnée et subsidiaire, qu'elle n'engendre pas de coûts supplémentaires pour l'économie suisse et qu'elle fonctionne sur une base coopérative.

Les Verts, Digitale Gesellschaft et le Parti Pirate soutiennent l'art. 73*b* et considèrent que pour pouvoir assumer les tâches visées par cet article, le NCSC doit répondre à certaines exigences minimales, à savoir disposer de compétences plus importantes en cas d'incidents graves et mettre en place une procédure de *responsible disclosure* pour les infrastructures critiques.

Les Verts et CH++ demandent que le NCSC puisse édicter des directives assorties de délais contraignants obligeant les organisations de fabricants et d'exploitants à remédier rapidement aux vulnérabilités et à réduire les dommages.

Le canton **VD** demande que l'art 73*b* soit coordonné avec l'ordonnance sur les dispositifs médicaux (ODim).

- **Demandes de modification et suggestions**

- **<u>Al. 1</u>**

Selon **l'UZH, l'UNIL et le PNR 77**, la formulation «pour autant que la situation ne nécessite pas d'analyses ou de clarifications supplémentaires» n'est pas claire. Ils préconisent de la remplacer par «lorsque des cyberincidents ou des vulnérabilités sont portés à la connaissance du NCSC» afin de ne pas se limiter à un signalement que l'on pourrait confondre avec le signalement de cyberattaques par la personne concernée.

- **<u>Al. 2</u>**

Selon **les Verts et CH++**, sauf exception justifiée, le NCSC devrait mettre en place une obligation de principe de publication, alors que **l'ISSS, Härting Rechtsanwälte, l'AES, l'UTP, Swissgrid, le canton GE et RAILplus** soulignent au contraire que les données personnelles et les données des personnes morales ne doivent être publiées qu'avec un consentement explicite et préalable et qu'il

convient de réglementer de manière plus précise les circonstances dans lesquelles un cyberincident doit être publié et les informations à mentionner, en raison des principes de la protection des données et du secret des informations confidentielles.

L'UZH, l'UNIL et le PNR 77 considèrent que le consentement à requérir devrait être celui de la personne partageant les données et non pas celui des personnes concernées, dans la mesure où l'obtention du consentement de toutes les personnes concernées pourrait requérir des efforts disproportionnés.

- **Al. 3**

Le **Parti Pirate** salue le fait que l'art. 73*b*, al. 3, prévoie que les failles de sécurité sont immédiatement partagées avec les exploitants d'infrastructures critiques et demande qu'il soit ajouté que ceux-ci ne peuvent pas en abuser pour des cyber-jeux offensifs selon la LRens. De même, les hackers doivent se voir automatiquement accorder l'impunité dans le cadre de la *responsible disclosure.*

CH++ propose que les fabricants qui ne réagissent pas aux signalements de vulnérabilités puissent être exclus des marchés publics.

L'UZH, l'UNIL et le PNR 77 considèrent qu'il serait opportun de compléter l'al. 3 par une possibilité de sanction en plus de la publication, alors que **la Poste** estime au contraire que des sanctions auraient un effet néfaste sur le nombre de signalements.
Le canton **GE** demande de remplacer «le fabricant» par «le fabricant et/ou l'éditeur».

Selon **Digitale Gesellschaft**, si le NCSC a connaissance d'une faille de sécurité affectant un produit tiers et dont on ne peut pas supposer qu'elle est déjà connue du fabricant, la faille doit être immédiatement signalée par le NCSC au fabricant concerné dans le cadre d'une procédure de *responsible disclosure*. De plus, le NCSC devrait, selon **Digitale Gesellschaft**, disposer de moyens lui permettant d'insister auprès des organisations qui signalent une faille de sécurité pour que celle-ci soit corrigée.

Selon **l'ISSS et Härting Rechtsanwälte**, les signalements de vulnérabilités faits par le NCSC aux fabricants devraient être exclus du principe de transparence.

Pour Demain et Opération Libero sont d'avis que des délais devraient aussi être fixés pour les exploitants afin garantir la mise en œuvre effective des mises à jour de sécurité.

Selon **l'UVS et VUD**, une publication prématurée de la vulnérabilité avec indication du logiciel ou du matériel concerné pourrait faire courir un risque supplémentaire à l'instance qui a fait le signalement. Ainsi **VUD** propose que toutes les informations et mesures de communication du NCSC soient soumises à la réserve légale qu'elles n'encouragent ou ne facilitent pas les cyberattaques.

3.3.2.7 Art. 73*c* 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), 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 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.

25 participants à la consultation se sont exprimés sur cet article, qui a beaucoup été discuté et a suscité de nombreuses propositions de modification. 2 participants soutiennent l'art. 73*c*, al. 3, alors que 3 autres rejettent l'art. 73*c*, al. 2.

❖ Remarques générales sur l'art. 73*c*

Privatim demande que les données transmises au Service de renseignement de la Confédération (SRC) ou aux autorités de poursuite pénale soient effacées des serveurs du NCSC après leur transmission.
Le canton **GR** demande que l'articulation entre la notion d'obligation de confidentialité des exploitants et celle de transmission d'informations dans le cadre de l'obligation de signalement soit plus explicite.

Swico soutient l'article mais demande qu'il y soit précisé que seules les informations relatives à la sécurité sont communiquées.

❖ Approbation de l'art. 73*c*

AEROSUISSE soutient cette disposition.

Le canton **AG** approuve le fait que les collaborateurs du NCSC ne soient pas soumis à l'obligation de dénoncer et que le NCSC puisse dénoncer les infractions.

Les Verts et CH++ soutiennent l'art. 73*c*, al. 3.

❖ Rejet de l'art. 73*c*

Le **Parti Pirate et eGov-Schweiz** refusent que le SRC traite les données transmises au NCSC dans le cadre de l'obligation de signalement.

Le canton **BE et la CCPCS** demandent la suppression de l'art. 73*c*, al. 2, car selon eux, le NCSC doit continuer à transmettre tous les délits officiels aux autorités de poursuite pénale.

Le canton **NW** demande la suppression de l'art. 73*c*, al. 2, au motif que cet article serait potentiellement arbitraire.

❖ Demandes de modification et suggestions concernant l'art. 73*c*

- **<u>Al. 1</u>**

Le **pvl** demande que l'art. 73*c*, al. 1, prévoie expressément la possibilité d'un signalement anonyme au NCSC.

Les Verts et VUD demandent que les données puissent être transmises au NCSC de manière anonyme et que ceci soit réglé juridiquement.

- **<u>Al. 2</u>**

Le canton **SZ** insiste sur le fait que le NCSC doit garantir que les infractions graves soient systématiquement portées devant les tribunaux.

De manière générale, les cantons **BL, NW et SZ** s'inquiètent du potentiel arbitraire d'une telle disposition.

- **<u>Al. 3</u>**

Digitalswitzerland, Sunrise, VUD, swissICT et l'asut sont d'avis que la personne effectuant le signalement risque de s'incriminer elle-même et demandent donc un changement du texte.

Digitalswitzerland demande que l'art. 73*c*, al. 3, soit précisé de sorte que les informations communiquées au NCSC par une personne dans le cadre d'un signalement et *qui pourraient incriminer cette personne* ne puissent être utilisées dans une procédure pénale contre cette personne qu'avec l'accord de celle-ci.

VUD propose que l'obligation de consentement soit étendue à tous les collaborateurs et organes d'une entreprise ou d'une organisation signalant un cyberincident.

3.3.2.8 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 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.

22 participants à la consultation se sont exprimés concrètement sur cette disposition. La plupart des interventions ont constitué soit en demandes de modification du texte, soir en demandes de clarifications. Un seul participant rejette l'art. 74.

❖ **Remarques générales sur l'art. 74**

Les Verts saluent vivement le fait que le NCSC soutienne les exploitants en ce qui concerne les cyberrisques.

L'UVS demande plus de clarifications quant au soutiens aux villes, notamment concernant la mise en œuvre de moyens de détection et d'identification de cyberattaques et le financement de ces derniers.

Raiffeisen est d'avis que l'utilisation des outils mis à disposition par le NCSC doit rester volontaire et qu'il ne faut pas prévoir d'obligation d'utiliser ces outils.

UniBE demande que le NCSC informe les exploitants d'infrastructures critiques des cyberattaques signalées contre d'autres exploitants d'infrastructures critiques.

❖ **Demandes de modification et suggestions concernant l'art. 74**

- **Al. 2, let. a**

L'ISSS, Härting Rechtsanwälte et la Poste demandent que le NCSC, en plus de la mise à disposition d'un système de communication pour l'échange sécurisé d'informations, garantisse un stockage sécurisé des données.

- **Al. 2, let. b**

Le canton **SH** insiste sur la nécessité de mettre en place une plateforme commune d'échange d'informations.

- **Al. 2, let. c**

La Poste demande une reformulation afin de garantir sans ambiguïté que l'utilisation de telles techniques est certes recommandée, mais qu'elle est en fin de compte facultative et pas obligatoire.

- **Al. 3**

L'AES salue la volonté de ne pas concurrencer les offres de l'économie privée mais suggère que le NCSC, en tant que GovCERT, chapeaute les CERT du secteur privé et les soutienne dans la gestion des crises en fonction de la situation et des besoins. **L'AES** demande aussi que des critères de distinction plus pertinents quant à qui a droit ou pas au soutien du NCSC soient définis et propose de supprimer la deuxième partie de la phrase («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 l'infrastructure critique.»).

L'UZH, l'UNIL et le PNR 77 considèrent que la disposition devrait élargir les conséquences dommageables aux collaborateurs, bénéficiaires et prestations de l'infrastructure critique, ainsi qu'à (une partie de) la société.

La Poste et le canton GE demande des précisions quant aux termes «risque imminent» et «conséquences graves».

- **Al. 4**

Digitalswitzerland demande qu'il soit plus clairement expliqué comment le NCSC protège les obligations de confidentialité.

L'ISSS et Härting Rechtsanwälte demandent une modification de la deuxième phrase de cet alinéa, afin de préciser que l'accès peut être octroyé sans enfreindre d'éventuelles obligations de garder le secret.

L'UZH, l'UNIL et le PNR 77 insistent sur le fait que cette disposition doit être reformulée pour prévoir que le NCSC assure la confidentialité et que l'exploitant ne viole pas de secret en transmettant des informations et en lui fournissant l'accès à ses moyens informatiques pour analyser un incident.

3.3.2.9 Art. 74*a* 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.

27 participants à la consultation se sont exprimés sur cet article, et 14 d'entre eux ont fortement insisté sur l'importance de la définition d'un délai de signalement.

- ❖ **Demandes de modification et suggestions concernant l'art. 74*a***

Les Verts, AEROSUISSE et economiesuisse demandent expressément que l'obligation de signalement n'entraîne pas de coûts supplémentaires, ni pour l'économie nationale ni pour les institutions procédant au signalement. Ils souhaitent en outre que la charge administrative du processus de signalement soit réduite au minimum.

Les Verts, le pvl, l'ISSS, Härting Rechtsanwälte et Pour Demain considèrent que l'obligation de signalement devrait également s'appliquer aux cyberattaques et aux cyberincidents généraux ainsi qu'aux vulnérabilités.

Sunrise et SWITCH estiment que l'obligation de signalement ne devrait s'appliquer qu'aux entreprises ayant subi des cyberattaques sur leur propre infrastructure (pas de déclaration de tiers).

Digitale Gesellschaft propose que l'obligation de signalement soit étendue à tous les secteurs de l'économie suisse ainsi qu'aux autorités étatiques et aux ONG, alors que le **Parti Pirate** considère que cette obligation devrait être étendue au minimum aux organisations qui exécutent des tâches pour le compte de l'État, ainsi qu'à toutes les entreprises qui sont tenues de procéder à un contrôle ordinaire ou de déclarer un fichier conformément à l'art. 11*a* LPD.

eAVS/AI estime qu'il doit être ici spécifié qu'un signalement peut aussi inclure toutes les organisations concernées et que l'annonce peut aussi être faite explicitement par des tiers.

Le Parti Pirate et les Verts considèrent que l'intelligence artificielle devrait être abordée dans le texte de loi.

Le PS demande que les personnes concernées par des cyberattaques soient averties en temps réel par le NCSC.

L'asut souligne qu'il est difficile d'obliger un fournisseur d'accès à Internet à signaler toutes les cyberattaques dont sont victimes les exploitants d'infrastructures critiques via son réseau. Il se peut également qu'une déclaration par le fournisseur d'accès ne soit pas possible en raison des dispositions de la loi sur la protection des données ou des accords contractuels.

L'Association des banques étrangères en Suisse, CH++, Pour Demain, Swiss Banking, scienceindustries, les cantons FR, GR et UR, Raiffeisen, SWITCH et les Verts insistent sur l'importance de fixer des délais explicites pour le signalement et la communication des informations détaillées au NCSC. **Swiss Banking** considère que cet article doit être complété par un al. 2 explicitant un délai de signalement, alors que **Raiffeisen et le Centre de droit du numérique de l'UNIGE** recommandent de reprendre les délais en deux temps de la communication prudentielle 05/2020 de la FINMA.

Digitalswitzerland propose d'introduire la notion de « personnes soumises à l'obligation de signaler » («Meldepflichtigen») afin d'obtenir une plus grande précision et d'éviter tout malentendu. De plus, **digitalswitzerland et economiesuisse** considèrent qu'il est nécessaire de renforcer la confiance de l'économie dans l'utilité de l'art. 74*a* en explicitant que les avantages de cette disposition sont immédiats et supérieurs par rapport aux obligations, la proportionnalité des mesures étant un critère important, en particulier pour les PME et les start-up.

L'**aéroport de Zurich et Raiffeisen** demandent que l'obligation de signalement se concentre sur les attaques réussies. Dans ce contexte, l'**aéroport de Zurich** propose de compléter le texte comme suit « im Sinne von Art. 74d ».

L'UZH, l'UNIL et le PNR 77 demandent que le terme «découverte» soit remplacé par «détection» et que «celui-ci» soit remplacé par «ce dernier».

3.3.2.10 Art. 74*b* 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;
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 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, à la loi du 17 décembre 2004 sur la surveillance des assurances ou à la loi du 19 juin 2015 sur l'infrastructure des marchés financiers;
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,
   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;
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;
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) 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;
o. aux entreprises de transport soumises à la loi fédérale du 18 juin 2010 sur les organes de sécurité des entreprises de transports publics;
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 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:
   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.

Cet article a suscité beaucoup de réactions; 39 participants à la consultation se sont notamment exprimés sur les domaines concernés par l'obligation de signalement.

❖ **Remarques générales sur l'art. 74*b***

Le **Parti Pirate** considère que les domaines mentionnés à l'art. 74*b* doivent être étendus aux grandes entreprises de médias.

Le **PS** demande quant à lui de maintenir cette liste à jour en la réexaminant tous les cinq ans.

Digitalswitzerland demande de limiter l'obligation de signalement aux seuls domaines dont la défaillance ou la détérioration entraînerait des pénuries d'approvisionnement à effet durable, des perturbations importantes de la sécurité publique ou d'autres conséquences dramatiques.

Scienceindustries, l'USAM, le canton UR et Swico demandent que la liste soit plus explicite, notamment en définissant clairement ce qu'on entend par «infrastructure critique». En ce sens, **swissICT** propose une différenciation qualitative entre infrastructures critiques et infrastructures hautement critiques.

Le canton **ZG et swissuniversities** demandent que la liste soit révisée et réduite.

Coop et Migros proposent que l'obligation de signalement soit limitée aux activités considérées comme critiques au sein de l'entreprise.

Le canton **AG** demande que la liste comprenne en outre le domaine des objets, organisations et entreprises qualifiés, par les services compétents de la Confédération ou du canton, d'infrastructures critiques au sens de la législation sur la protection de la population.

Le canton **GR** propose de faciliter la mise en œuvre de l'art. 74*b* en examinant s'il y a lieu de fixer des priorités et d'échelonner les délais en conséquence afin de réduire la liste pendant une phase pilote.

Le canton **SZ** demande que les exploitants de dossiers électroniques des patients visés à l'art. 10 de la loi fédérale du 19 juin 2015 sur le dossier électronique du patient (RS *816.1*) soient également soumis à l'obligation de signalement.

Le canton **UR** propose qu'en plus de l'obligation de signalement, le signalement des cyberincidents soit recommandé pour toutes les autres organisations.

Les Verts suggèrent que ce domaine soit étendu afin d'inclure la démocratie (partis politiques au sein du Parlement et politiciens occupant des postes importants), en plus des services postaux, de la navigation sur le Rhin ou des agences de presse.

- ❖ **Approbation de l'art. 74*b***

EGov-Schweiz, les cantons AI, GR et BE ainsi que privatim estiment que la disposition proposée est appropriée.

- ❖ **Rejet de l'art. 74*b***

VUD rejette l'art. 74*b*, au motif que celui-ci serait disproportionné. L'association propose de limiter d'emblée l'obligation de signalement aux cyberattaques qui menacent gravement des infrastructures critiques au sens de l'art. 5, let. c, LSI et qui sont donc d'intérêt national.

- ❖ **Demandes de modification et suggestions concernant l'art. 74*b***

- **<u>Let. b (autorités)</u>**

L'UVS demande que la responsabilité de l'obligation de signalement incombant aux autorités communales soit clarifiée.

- **<u>Let. c (sauvetage, eau potable, eaux usées, déchets)</u>**

Selon le canton **AI**, si les autorités cantonales et communales ont le même exploitant informatique, un seul signalement doit suffire.

- **<u>Let. f (services numériques)</u>**

Digitalswitzerland propose, pour plus de clarté, de supprimer «de places de marché en ligne» à la let. f.

SwissICT demande que la let. f définisse plus clairement les ch. 1, 2 et 3.

Swissmem approuve la présente disposition mais souhaiterait une distinction plus claire entre un exploitant ou un fournisseur de services et un fournisseur d'infrastructures de données (services en nuage).

Migros demande que cette définition soit formulée de manière plus technologiquement neutre.

SWITCH ainsi que l'UZH, l'UNIL et le PNR 77 demandent que l'aspect extraterritorial de cette disposition soit abordé, notamment quant à l'application du droit suisse.

L'UZH, l'UNIL et le PNR 77 souhaiteraient plus de précisions sur les fournisseurs de services de télécommunication dérivés qui sont également concernés.

Le canton **GE** demande une définition plus précise de la notion de «services de sécurité et de confiance».

Switch demande que la gestion des noms de domaine .ch soit inclue dans cette disposition.

Selon **les Verts et CH++**, le nombre d'utilisateurs n'est pas un bon indicateur de l'importance de la cible.

Les Verts et CH++ demandent que le terme «numérique» soit supprimé à la let. f, ch. 2.

- **Let. g (hôpitaux)**

Le canton **GL** demande des précisions sur les hôpitaux (taille des infrastructures) considérés comme infrastructures critiques. Il souhaite en outre que les plateformes utilisées pour le dossier électronique du patient soient elles aussi soumises à l'obligation de signalement.

- **Let. i (médicaments)**

Scienceindustries demande une définition exacte et une désignation spécifique des entreprises qui sont soumises à cette disposition.

- **Let. j (assurances sociales)**

Inter-pension considère que la notion d'assurance sociale n'est pas clairement définie dans la prévoyance professionnelle (prestations surobligatoires).

- **Let. k (services de télécommunication)**

L'UZH, l'UNIL et le PNR 77 considèrent que la let. k comporte un aspect extraterritorial, raison pour laquelle il faudrait prévoir l'application du droit suisse (voir par ex. la théorie des effets de l'art. 3 rév LPD).

- **Let. p (aviation civile)**

AEROSUISSE ainsi que les aéroports de Genève et Zurich insistent sur la nécessité de modifier le texte afin que cette disposition ne porte pas uniquement sur les compagnies aériennes disposant d'une autorisation de l'Office fédéral de l'aviation civile.

- **Let. r (approvisionnement de base)**

Migros demande l'introduction de critères facilement mesurables, tels que le nombre de collaborateurs ou le chiffre d'affaires, sur la base desquels certains allégements ou exceptions sont prévus directement dans la loi.

Le canton **GE et les TPG** demandent que le terme «chiffrement» soit utilisé au lieu de «cryptage» dans la version française de cette disposition.

- **Let. s (fabricants de matériel et de logiciels informatiques)**

Les Verts et CH++ estiment que la disposition proposée est appropriée et proposent de mentionner les chaînes d'approvisionnement.

eAVS/AI considère qu'il faut aussi mentionner les fournisseurs de technologies de l'information des organes exécutifs, dont la situation n'est pas clairement définie ici.

Economiesuisse considère que le fait de mentionner les fabricants accroît le manque de clarté quant aux instances concernées par l'obligation de signalement.

L'UVS s'inquiète de l'applicabilité de cette disposition, notamment car de nombreux fabricants de matériel et de logiciels ne sont pas établis en Suisse**.**

Swico propose de supprimer les ch. 1 à 4 de cette disposition et de définir à leur place la notion de télémaintenance afin d'aussi traiter de la problématique des chaînes d'approvisionnement.

SwissICT demande qu'il soit précisé à la let. s que les fournisseurs de logiciels en tant que service (SaaS) n'exploitent pas d'infrastructures critiques.

Swissmem demande que l'art. 74*b*, let. s, soit supprimé.

3.3.2.11 Art. 74*c* 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.

Au total, 20 participants à la consultation se sont exprimés sur les exceptions. Ils ont principalement émis des remarques générales et de nombreuses propositions d'adaptation de la formulation. Seuls 5 participants à la consultation se sont prononcés contre l'inscription de cette disposition dans la loi.

❖ Remarques générales sur l'art. 74*c*

Swiss Banking propose de modifier cette disposition afin qu'elle prévoie que le Conseil fédéral définisse par voie d'ordonnance des critères clairs sur la base desquels les infrastructures critiques sont soumises à l'obligation de signalement, l'objectif de ces critères étant d'exempter les exploitants de l'obligation de signalement lorsque les défaillances ou les dysfonctionnements provoqués par des cyberattaques remplissent les conditions énumérées aux let. a et b.

Swico considère que les critères mentionnés dans cet article seront difficilement applicables et propose de les remplacer par le critère de l'impact potentiel d'un dommage.
De plus, **Swico** propose d'ajouter une lettre supplémentaire à la disposition, afin de prévoir également une exemption lorsque des mesures de mitigation rendent une cyberattaque inoffensive.

VUD considère que les dispositions de l'art. 74*c*, let. a et b, sont contradictoires ou peu claires et demande qu'elles soient clarifiées, notamment les expressions «d'une faible dépendance à l'égard des moyens informatiques» et «n'ont qu'un impact limité sur le fonctionnement de l'économie ou sur le bien-être de la population».

Le canton **BE** demande l'ajout d'une disposition 74*c*^{bis} prévoyant que les cantons peuvent, après consultation du NCSC et dans le respect des conditions visées à l'art. 74*c*, exempter de l'obligation de signalement des autorités ou organismes investis de tâches publiques à l'échelle cantonale ou

communale. Le canton **BE** souhaite que cet art. 74*c*[bis] prévoie par ailleurs que les cantons puissent désigner les personnes responsables du signalement au sein des autorités ou organismes investis de tâches publiques à l'échelle cantonale ou communale.

Migros déplore l'absence d'une réglementation basée sur les risques.

Le canton **LU et SWITCH** demandent que les petites organisations soient exemptées de l'obligation de signalement, le processus étant, selon le canton **LU**, trop coûteux.

❖ **Approbation de l'art. 74*c***

EGov-Schweiz ainsi que les cantons AI et NW considèrent que cet article est approprié.

❖ **Rejet de l'art. 74*c***

Les Verts, CH++, Opération Libero, ainsi que les cantons TG et UR demandent la suppression de cet article.

❖ **Demandes de modification et suggestions concernant l'art. 74*c***

- **Let. a**

Selon **les Verts, Opération Libero et Pour Demain**, une faible dépendance aux moyens informatiques semble de moins en moins probable au XXIe siècle. Ils demandent donc la suppression de la let. a.

Le canton **GE** est d'avis que cette disposition est en contradiction avec la LPD.

- **Let. b**

VUD estime que seule la question de savoir si une cyberattaque porte gravement atteinte à la sécurité nationale peut être déterminante.

Selon le canton **GE,** cette disposition est en contradiction avec l'objectif de l'art. 74*b*, qui énumère les organisations d'importance majeure.

Migros considère que la dérogation prévue à la let. b est inapplicable.

3.3.2.12 Art. 74*d* 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.

La définition des cyberattaques à signaler a suscité un grand nombre de réactions, principalement des remarques générales ou des propositions concrètes de modification.
En tout, 36 participants se sont exprimés; 1 s'est expressément prononcé en faveur de cette disposition, tandis que 4 l'ont explicitement rejetée.

❖ **Remarques générales sur l'art. 74*d***

Pour **AEROSUISSE**, il est important pour la sécurité juridique des entreprises concernées qu'il soit clairement établi que l'art. 74*d* est le critère permettant de déterminer quand une attaque contre une infrastructure critique doit être signalée.

Selon **economiesuisse, eGov-Schweiz, le canton ZH et santésuisse**, l'art. 74*d* doit impérativement être révisé, notamment parce que les critères sont trop larges et difficilement compréhensibles ou applicables pour les entreprises. Ainsi, selon **economiesuisse**, il serait plus judicieux de mettre à disposition une liste (positive) plus restreinte d'incidents à signaler et de limiter l'obligation de signalement aux tentatives réussies ou particulièrement graves.

Le canton **GR** demande une liste claire des cas à signaler.

L'ISSS, Härting Rechtsanwälte, ainsi que l'UZH, l'UNIL et le PNR 77 demandent que le titre de l'art. 74*d* mentionne également les cyberincidents.

Privatim demande une définition plus précise de ce qui est entendu par «grave», car, selon cette conférence, il est ici sous-entendu que les incidents doivent être signalés même si leur gravité ne peut pas encore être évaluée. Ainsi, si le NCSC conclut qu'il ne s'agit pas d'un incident de sécurité grave et qu'il n'y a pas de consentement de la ou des personnes concernées, les informations personnelles doivent être immédiatement effacées ou traitées sous forme anonymisée.

Scienceindustries demande qu'il soit expressément spécifié à l'art. 74*d* que l'obligation de signalement se limite aux attaques contre des installations en Suisse et exclut les attaques contre des installations situées à l'étranger, alors que **l'UZH, l'UNIL et le PNR 77** demandent que la disposition couvre aussi les installations situées à l'étranger.

Pour **Coop**, la définition proposée est trop générique et ne permet pas de différenciation claire entre les incidents qui n'ont pas ou peu d'influence sur les processus commerciaux et ceux qui concernent directement l'exploitation d'infrastructures critiques ou qui présentent un risque élevé. Elle ne permet pas non plus de savoir quelles cyberattaques signaler entre les réussies et celles qui ont échoué.

L'**aéroport de Zurich** demande que seules les cyberattaques réussies soient soumises à l'obligation de signalement.

Selon le canton **AG**, le tri des attaques à signaler devrait être effectué par le NCSC, car même les signalements d'attaques considérées comme sans importance peuvent s'avérer importants.

- **Approbation de l'art. 74*d***

L'AES soutient cette disposition.

- **Rejet de l'art. 74*d***

Swiss Banking et Raiffeisen proposent la suppression de l'art. 74*d* et son remplacement par une formulation correspondant à celle de la FINMA: ils demandent de prévoir une obligation de signaler les cyberattaques ayant des conséquences considérables sur l'activité de l'entreprise, en particulier les attaques, qu'elles aient atteint leur but entièrement ou partiellement, sur des fonctions d'importance critique dont la défaillance ou le dysfonctionnement auraient des conséquences sur la protection des individus ou sur le bon fonctionnement des marchés.

SwissICT demande que la présente disposition soit effacée, au motif qu'en pratique, toute cyberattaque devra être déclarée.

VUD rejette la solution législative proposée, qui définit les événements à signaler de la manière la plus large possible (art. 5, let. d et e, LSI) pour ensuite limiter l'obligation de signalement (art. 74*d* LSI).

❖ Demandes de modification et suggestions concernant l'art. 74*d*

- **Al. 1**

Selon l'**ISSS,** le fait que les indices de cyberattaque soient déjà soumis à l'obligation de signalement en vertu de l'art. 74*d* est contraire à la ratio legis. L'ISSS propose donc de modifier la phrase introductive de sorte d'une part qu'elle porte aussi sur les cyberincidents et d'autre part que l'obligation s'applique en cas de *craintes sérieuses* et non de simples indices.

- **Al. 1, let. a**

Swissmem demande de modifier la condition visée à la let. a afin qu'une mise en péril *considérable* soit exigée.

Les **aéroports de Genève et Zurich, Swissgrid, santésuisse et le canton GE** proposent de supprimer le passage «ou une autre infrastructure critique», parce que les entreprises ne peuvent souvent pas évaluer une telle menace.

- **Al. 1, let. b**

Economiesuisse, Coop, IG eHealth, SWITCH, le canton TG, l'ISSS, l'aéroport de Zurich, Axpo, l'UZH, l'UNIL et le PNR 77, scienceindustries, VUD, l'UTP et RAILplus se questionnent sur la pertinence de cette deuxième condition, les cyberattaques perpétrées par les États étant souvent trop complexes pour être détectées et leur attribution étant une démarche politique et compliquée. Pour ces raisons, **l'ISSS, l'aéroport de Zurich, Axpo, l'UZH, l'UNIL et le PNR 77, scienceindustries, VUD, l'UTP et RAILplus** proposent de supprimer cette condition. **RAILplus** suggère de la remplacer par un critère cumulatif lié à l'impact (par ex. le nombre d'utilisateurs ou de systèmes touchés).

- **Al. 1, let. c**

Swissgrid considère que les points suivants doivent ici être développés: données sensibles, informations sur les systèmes critiques, données relatives à l'exploitation du réseau électrique, infrastructures et systèmes de l'exploitation principale.

- **Al. 1, let. d**

Economiesuisse, l'aéroport de Zurich, l'ASA, VUD et Coop considèrent que le délai de 30 jours n'a pas de sens.

IG eHealth propose de ne pas soumettre à l'obligation de signalement les cyberattaques passées inaperçues pendant plus de 30 jours si les conditions des let. a (mise en péril du bon fonctionnement) et c (fuite ou manipulation possible d'informations) ne sont pas remplies, c'est-à-dire si l'attaque était mineure ou d'une gravité faible à moyenne.

L'ASA considère que le délai n'est pas réaliste notamment car cela créerait une obligation de réagir à un événement dont on n'a pas connaissance et dont on ne peut peut-être pas savoir quand il s'est produit. L'ASA propose de remplacer la let. d par le texte suivant : « über einen längeren Zeitraum unentdeckt blieb ».

Le **canton TG** propose de remplacer la let. d par le texte suivant : «*d. die direkt und unmittelbar für das Ziel des Cyberangriffs verwendeten Instrumente länger als 30 Tage unentdeckt blieben*».

Selon **Migros ainsi que l'UZH, l'UNIL et le PNR 77**, un délai de non-détection ne devrait pas constituer un critère unique de signalement.

- **Al. 2**

Selon **scienceindustries,** l'obligation de signalement doit être limitée à l'extorsion, aux menaces ou à la contrainte en ce sens qu'elle ne prend effet qu'en présence d'un lien avec l'activité commerciale.

Le MPC considère que la formulation exhaustive de la liste soulève la question de savoir si l'obligation de déclarer ne doit pas également s'appliquer lorsqu'une cyberattaque est liée à un chantage, à des menaces ou à une contrainte à l'égard de clients ou de patients d'un exploitant.

Le canton **BL** suggère de compléter le présent texte en y intégrant les infractions de détérioration de données, commises par le cryptage ou l'introduction de données (malware).

Le canton **GE** signale que les institutions qui violeraient cet article encourraient un risque de double peine.

L'UZH, l'UNIL et le PNR 77 considèrent que le présent texte doit être modifié de sorte qu'il prévoie une obligation de signaler dès que «des actes pénalement répréhensibles» seraient commis et non seulement dans les «cas accompagnés d'infractions contre la liberté».

3.3.2.13 Art. 74*e* 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.

Lors de la consultation, 15 participants se sont exprimés sur cette disposition. La majorité demande des clarifications et une description plus détaillée des informations requises en vertu de l'art. 74*e*.

- **Remarques générales sur l'art. 74*e***

Les Verts estiment que l'art. 74*e* doit être révisé pour faire en sorte que l'automatisation des signalements soit possible.

L'Association des banques étrangères en Suisse considère que les signalements doivent pouvoir être rédigés en anglais et dans les langues nationales.

Economiesuisse demande que les exigences en matière de notification restent simples afin de limiter les obstacles pour les entreprises. De plus, les limites des faits à signaler doivent être clairement définies.

SwissICT, la Poste ainsi que les cantons GR et TG demandent que les informations requises en vertu de l'art. 74*e* soient décrites de manière plus précise, éventuellement au moyen d'une liste.

SwissICT et la Poste demandent que les informations exigées par l'art. 74 e soient coordonnées avec d'autres autorités (par ex. la FINMA).

Selon **Axpo,** le signalement doit être immédiat, quel que soit le niveau d'information.

- **Approbation de l'art. 74*e***

Swiss Banking soutient cette disposition.

- **Demandes de modification et suggestions concernant l'art. 74*e***

- **<u>Al. 1</u>**

L'ISSS et Härting Rechtsanwälte demandent à ce que la présente disposition soit modifiée comme suit : « Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, des Cybervorfalles, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.».

Le canton **GE** propose de remplacer «ainsi que les mesures que compte prendre l'exploitant de l'infrastructure» par «ou que l'entité concernée a commencé à mettre en œuvre».

L'UZH, l'UNIL et le PNR 77 proposent de modifier la formulation afin que le signalement doive contenir des informations concernant les mesures «prises ou prévues».

- **Al. 2**

Le canton **GE** demande de modifier l'al. 2 afin que l'exploitant soit tenu de compléter le signalement non seulement dès que les informations requises lui parviennent, mais aussi dès que celles-ci peuvent être obtenues.

3.3.2.14 Art. 74*f* 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.

L'art. 74*f* a été commenté par 34 participants à la consultation; 4 d'entre eux (RAILplus, santésuisse, UniBE et la Poste) en ont accepté le texte tel quel. Aucun participant n'a complètement rejeté cet article. La grande majorité des avis portent sur la question de la centralisation des canaux de transmission des informations au NCSC et aux autorités autorisées par la loi.

- **Remarques générales sur l'art. 74*f***

CH++ considère que l'art. 74*f* devrait être adapté de manière à mentionner explicitement la transmission de données via une interface sécurisée. De plus, une approche centrée sur l'API, telle qu'elle est pratiquée par les réseaux de partenaires de Meta/Facebook ou AT&T, doit être poursuivie par le NCSC. CH++ estime qu'une base légale appropriée doit être créée à cet effet.

Pour Demain et Opération Libero considèrent qu'une interface informatique (API) doit également être mise en place pour permettre d'envoyer des messages automatisés au NCSC.

L'UVS, swissuniversities, le canton ZH et Swico demandent que le signalement puisse se faire sous une forme simple.

Le canton **GR** demande de clarifier quelles informations sont transmises à quelles autorités et qui peut les consulter.

L'UZH, l'UNIL et le PNR 77 demandent que les autorités n'aient pas accès aux informations à destination d'autres services.

Swico demande un mécanisme de signalement aussi libre que possible, afin de permettre par exemple des signalements automatiques par flux RSS ou AP ou par l'échange de données existant via le système MISP, dont disposent de nombreuses infrastructures critiques. De plus, **Swico** demande que le canal de transfert d'informations actuellement utilisé entre le GovCERT et les infrastructures critiques puis continuer d'être utilisé pour le signalement des cyberattaques au NCSC.

SwissICT considère que la transmission des informations à d'autres autorités en plus du NCSC est obligatoire uniquement pour les autorités et non pour les entreprises.

Raiffeisen soutient la disposition et demande l'ajout d'un alinéa précisant que le système en question doit également être utilisé par les autres autorités fédérales qui imposent des obligations de signalement dans le cadre de cyberattaques.

Swissgrid demande que le système permette un envoi simultané des données de signalement au Préposé fédéral à la protection des données et à la transparence (PFPDT).

SWITCH demande que les signalements puissent également être effectués via une CERT sectorielle commune. Puisque la loi ne l'exclut pas expressément, **SWITCH** part du principe que les organisations concernées auront la liberté de s'organiser en conséquence.

❖ **Approbation de l'art. 74*f***

RAILplus, santésuisse, UniBE et la Poste soutiennent l'art. 74*f*, notamment la possibilité de transmettre les informations via la plateforme sécurisée respectant les normes de sécurité les plus élevées ainsi que le fait de pouvoir aussi utiliser d'autres moyens pour faire le signalement, en particulier le formulaire existant du NCSC, le courrier électronique ou le téléphone.

❖ **Demandes de modification et suggestions concernant l'art. 74*f***

- **Al. 1**

Le canton **GE** demande qu'il soit précisé que ce système est gratuit.

- **Al. 2**

L'Association des banques étrangères en Suisse, Swiss Banking, les Verts, CH++, l'asut, l'ISSS et le pvl sont d'avis qu'il convient de s'assurer, lors de la mise en œuvre, que les obligations de signaler qui se recoupent (LPD, FINMA, etc.) puissent être remplies par une seule procédure de signalement. **Le pvl, l'AES, digitalswitzerland, economiesuisse et Digitale Gesellschaft** vont plus loin en proposant la mise en œuvre d'un guichet fédéral de signalement, auprès duquel toutes les obligations de signaler pourraient être satisfaites au moyen d'un seul formulaire en ligne.

L'ISSS et Härting Rechtsanwälte salueraient la création d'un guichet unique, mais demandent des clarifications concernant les informations qui peuvent être transmises, à qui et avec quel contenu. Ils estiment par exemple qu'il faudrait clarifier si les informations fournies au NCSC qui sont transmises par celui-ci au PFPDT entreront également dans le champ d'application de l'art. 24, al. 6, de la rév LPD (non-incrimination dans la procédure pénale). Comme l'art. 74*g* LSI permet au NCSC de demander des informations supplémentaires, cela élargit le champ de la communication à des tiers. Une telle communication, souvent très informelle au niveau technique, ne doit pas pouvoir faire l'objet d'une procédure pénale selon la rév LPD si des données personnelles sont impliquées. Il faut donc une réglementation plus détaillée pour savoir avec qui quelles informations peuvent être partagées et quelles conséquences cela peut avoir ou ne pas avoir.

L'UZH, l'UNIL et le PNR 77 soulignent qu'il est nécessaire de modifier l'art. 73*c* afin de prévoir un renvoi exprès s'il existe effectivement une volonté d'application de l'art. 73*c*, al. 1 à 3, AP-LSI aux communications sur les cyberattaques signalées, afin que le NCSC puisse en toute légalité transmettre à d'autres autorités des informations dans les cas de l'art. 73*c*, al. 1 et 2.

- **Al. 3**

L'ISSS et Härting Rechtsanwälte demandent que l'al. 3 soit supprimé afin de s'assurer que les autres institutions et autorités ne reçoivent que les informations qu'ils sont légalement en droit de recevoir ou qui sont justifiées dans le cadre de l'objectif de la législation applicable.

Le canton **GE** demande que cet alinéa précise que le service ou l'autorité concernés doit avoir «légitimement» besoin des informations concernées.

3.3.2.15 Art. 74*g* 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'art. 74*e* dont le NCSC a besoin pour remplir ses tâches en matière de prévention de toute nouvelle cyberattaque contre des infrastructures critiques.

9 participants à la procédure de consultation se sont exprimés sur cet article; aucun ne l'a accepté en l'état.

- **Remarques générales sur l'art. 74*g***

Selon **l'ISSS et Härting Rechtsanwälte**, cette disposition élargit le champ de la communication avec des tiers. Il convient donc ici de définir l'étendue de l'obligation d'information.

De plus, **scienceindustries** considère qu'il convient de définir clairement les informations supplémentaires que le NCSC est autorisé à demander.

Selon **swissICT**, afin de ne pas alourdir la charge pesant sur les entreprises, les établissements, les autorités et les communes en période de difficultés, il faudrait que les informations supplémentaires ne soient demandées pendant la crise que si cela est absolument nécessaire pour la sécurité de l'approvisionnement concerné.

Le canton **TG** demande que cet article soit plus nuancé afin de permettre aux cantons de respecter aussi leurs propres directives en matière de cybersécurité.

UniBE demande des clarifications quant aux attentes en termes de contenu et aux attentes temporelles liées à cette obligation.

- **Rejet de l'art. 74*g***

Selon **VUD**, cette disposition est trop imprécise et devrait être supprimée sans être remplacée, le contenu du signalement étant réglé de manière exhaustive par l'art. 74*e* LSI.

- **Demandes de modification et suggestions concernant l'art. 74*g***

Scienceindustries demande une modification de cette disposition, afin que les exploitants doivent fournir les informations en question uniquement dans la mesure du possible.

Le canton **GE** demande que les informations soient fournies au NCSC «dans les meilleurs délais».

3.3.2.16 Art. 74*h* 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*.

Seuls 4 participants à la consultation ont abordé la question de l'infraction à l'obligation de signalement ou à l'obligation de fournir des renseignements.

- **Approbation de l'art. 74*h***

Le **Centre Patronal** soutient cet article.

- **Rejet de l'art. 74*h***

Scienceindustries, l'aéroport de Genève et digitalswitzerland se positionnent contre cet article car selon eux, une obligation de signalement peut conduire une entreprise à enfreindre les lois sur la protection des données dans le pays où elle a son siège ou à enfreindre l'obligation de signalement en Suisse.

❖ **Demandes de modification et suggestions concernant l'art. 74*h***

L'UZH, l'UNIL et le PNR 77 demandent que cet article garantisse le respect du droit d'être entendu aux institutions incriminées.

3.3.2.17 Art. 74*i* 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)[3].
[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 de non-observation d'une décision du NCSC, la poursuite et le jugement sont du ressort des cantons.

30 des participants à la procédure de consultation se sont exprimés au sujet de l'art. 74*i*; 13 en ont demandé la suppression.

❖ **Remarques générales sur l'art. 74*i***

Selon **les Verts et CH++**, le texte de l'article doit rendre plus explicite le fait que les sanctions prévues s'appliquent au niveau de la direction des organisations, et non au niveau des spécialistes.

RAILplus propose que seules les personnes morales soient punissables (quel que soit le montant de la sanction). **RAILplus** demande en outre que les situations où les sous-traitants sont situés hors du territoire helvétique soient réglées.

Le Parti Pirate et le canton GE déclarent que, afin de garantir une proportionnalité des amendes, le législateur devrait les définir proportionnellement au chiffre d'affaires de l'entreprise (par ex. à 4 % du chiffre d'affaires annuel).

Le PS considère que les mesures prévues à l'art. 74*i* sont judicieuses. Toutefois, il convient de vérifier après cinq ans si les possibilités de sanctions mentionnées à l'art. 74*i* LSI sont suffisantes et si les principes de l'égalité de traitement et de la proportionnalité ont été respectés.

Les cantons **SO et UR** demandent qu'une amende ne soit prononcée qu'après consultation (écrite) du NCSC avec l'auteur de l'infraction.

L'UZH, l'UNIL et le PNR 77 ne considèrent pas que le montant de l'amende soit dissuasif, notamment en comparaison avec le montant prévu dans la LPD.

❖ **Rejet de l'art. 74*i***

AEROSUISSE, la Poste, Raiffeisen, Swisscom, Sunrise, SWITCH, Coop, l'asut, economiesuisse, digitalswitzerland, Swico, ISSS, Härting Rechtsanwälte, Swiss Banking, Scienceindustries, l'aéroport GE et Helvetia Assurances ne voient pas l'intérêt d'imposer les nouvelles obligations par des dispositions pénales et rejettent ces dernières par principe.

[3] RS **313.0**

De plus, **scienceindustries, les cantons SO et TG, l'UTP et l'usam** sont d'avis que le montant maximal des amendes infligées crée un danger existentiel sur le plan administratif en raison d'une menace d'amende exagérément élevée et disproportionnée, en particulier pour les petites et moyennes entreprises.

❖ **Demandes de modification et suggestions concernant l'art. 74*i***

- **Al. 1**

L'UTP demande que le montant de l'amende visée à l'al. 1 soit fixé à 10 000 francs au plus.

- **Al. 3**

Selon **swissICT**, le montant visé à l'al. 3 devrait être augmenté, et s'élever à 50 000 francs au lieu de 20 000. Cela permettrait d'une part de mieux éviter des frais d'enquête disproportionnés dans les cas de peu d'importance et, d'autre part, d'être en phase avec l'art. 64, al. 2, de la rév LPD.

L'UTP demande que le montant de l'amende visée à l'al. 3 soit fixé à 5000 francs au plus.

3.3.2.18 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[4] 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[5] sont réservés.

Aucune des instances interrogées n'a souhaité garder le présent article en l'état.

❖ **Remarques générales sur l'art. 75**

Privatim soutient l'art. 75 mais demande que le traitement doive être effectué avec des données anonymisées si des données sans référence à des personnes sont suffisantes.

Scienceindustries demande que les possibles incompatibilités avec les diverses législations étrangères sur la protection des données lors de la transmission de données personnelles soient prises en compte et réglées juridiquement.

La Poste demande que le traitement des informations confidentielles soit réglementé de manière plus précise afin que la confidentialité des signalements soit garantie.

Swisscom et la Poste demandent l'introduction, dans le cadre de l'actuel projet de révision de la LSI, d'une règle d'exception qui, au sens d'une *lex specialis*, prévaudrait sur le principe de transparence selon la LTrans.

[4] RS **784.10**
[5] RS **235.1**

Raiffeisen est d'avis que les signalements au sens de la nouvelle réglementation doivent respecter le secret professionnel et en ce sens propose l'ajout d'un alinéa prévoyant que les informations transmises doivent être traitées de manière confidentielle par les autorités et qu'elles ne peuvent pas être transmises si cela mettrait en péril la sécurité de l'entreprise ou des personnes concernées.

❖ **Rejet de l'art. 75**

Le canton **TG** considère que le NCSC ne devrait pas avoir accès à des données personnelles et rejette par conséquent l'art. 75.

❖ **Demandes de modification et suggestions concernant l'art. 75**

- **Al. 1**

EGov-Schweiz estime que les compétences de traitement de données sensibles par le NCSC visées à l'art. 75, en particulier en relation avec les possibilités de transmission en Suisse et à l'étranger selon les art. 76 et 77, sont problématiques. **EGov-Schweiz** part donc du principe qu'en cas de besoin, le NCSC fera appel à l'aide de la police et du SRC et ne cherchera pas à traiter lui-même les données.

Selon **privatim**, compte tenu du fait que le NCSC n'assume pas les tâches du SRC et n'est pas une autorité de poursuite pénale, le volume des données personnelles traitées conformément à l'art. 75, al. 1, AP-LSI ne semble pas proportionné sans autres restrictions (notamment sur la nécessité impérative d'accomplir les tâches). **Privatim** recommande de prévoir les restrictions nécessaires.

- **Al. 1, let. a**

Le canton **GR** demande la suppression de cette disposition.

Le **PVL** critique l'étendue des données personnelles que le NCSC est autorisé à traiter selon l'avant-projet et demande que la transmission des données sensibles entre le NCSC, les autorités pénales et le SRC soit explicitée. À cela s'ajoute le fait qu'aucune surveillance particulière n'est prévue dans le cas présent. Il n'est donc pas garanti qu'il n'y ait pas d'utilisation abusive de ces données.

- **Al. 2**

Privatim est d'avis que la séparation des compétences entre le NCSC, les autorités pénales et le SRC devrait faire l'objet d'une attention nettement plus grande. Ainsi, l'art. 75, al. 2, LSI (traitement de données personnelles à l'insu de la personne concernée) devrait être limité aux cas de procédures pénales en cours.

- **Al. 3**

Migros estime que cette disposition doit être harmonisée avec les dispositions correspondantes de l'art. 24 revLPD.

3.3.2.19 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.

7 participants se sont exprimés sur le présent texte de loi.

❖ **Remarques générales sur l'art. 76**

Scienceindustries considère que les al. 1 et 2 devraient au moins prévoir de manière restrictive que la transmission de telles informations, notamment à des concurrents opérant sur des marchés similaires, ne puisse pas avoir lieu sans l'accord du détenteur des données.

Swico insiste sur l'importance de la conservation des canaux de communication préétablis entre le NCSC, les infrastructures critiques et d'autres parties prenantes.

L'UTP demande que le rapport entre les dispositions de l'art. 76, al. 1, d'une part, et celles des art. 73*b*, al. 2, et 73*c*, d'autre part, soit clarifié de telle manière que le NCSC communique les données personnelles aux exploitants d'infrastructures critiques à la condition que cela soit nécessaire à la protection des infrastructures critiques contre les cyberrisques.

Le canton **GE** demande de clarifier s'il s'agit ici des infrastructures critiques selon l'art. 74*b* avec (ou sans) les exceptions de l'article 74*c*. En outre, le canton **GE** demande que le PFPDT soit mentionné.

❖ **Demandes de modification et suggestions concernant l'art. 76**

- **Al. 1**

L'UZH, l'UNIL et le PNR 77 demandent de remplacer «utiles» par «nécessaires» à l'al. 1.

- **Al. 2**

L'ISSS demande que l'al. 2 soit modifié afin de prévoir que les exploitants d'infrastructures critiques peuvent communiquer au NCSC des données personnelles dans la mesure où elles sont utiles à la protection de *leurs* infrastructures critiques contre les cyberrisques.

- **Al. 3**

L'ISSS demande que l'al. 3 soit modifié pour préciser qu'il s'applique uniquement aux fournisseurs de services de télécommunication qui ne sont pas également exploitants d'infrastructures critiques.

- **Al. 4**

L'ISSS demande que l'al. 4 soit modifié pour préciser qu'il s'applique uniquement aux fournisseurs de services de télécommunication qui ne sont pas également exploitants d'infrastructures critiques.

L'UZH, l'UNIL et le PNR 77 demandent que la disposition prévoie plutôt que «les fournisseurs de services de télécommunication peuvent communiquer au NCSC des données personnelles, y compris des ressources d'adressage».

3.3.2.20 Art. 76*a* 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[6] en procédant à des évaluations des cyberattaques quant à leur nombre, leur type et leur ampleur et à des analyses techniques des cyberrisques.

[6] RS **121**

[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.

7 participants à la consultation se sont exprimés sur l'assistance technique aux autorités.

❖ **Remarques générales sur l'art. 76*a***

Le canton **UR** demande que les informations sur les auteurs des cyberattaques, les méthodes et les tactiques soient transmises dans leur intégralité.

Le canton **NW** estime que les informations partagées avec le SRC doivent également être mises à disposition de toutes les autorités de poursuite pénale.

Le canton **ZG** considère que le cercle des destinataires des évaluations et des analyses techniques doit être étendu aux autorités de poursuite pénale.

❖ **Approbation de l'art. 76*a***

Swiss Banking approuve la présente réglementation.

❖ **Demandes de modification et suggestions concernant l'art. 76*a***

- **Al. 2**

L'UTP demande que l'al. 2 soit modifié pour prévoir que les informations en question peuvent renseigner *uniquement* sur l'identité et le mode opératoire des auteurs de cyberattaques.

- **Al. 3**

L'UTP demande que l'al. 3 soit modifié pour prévoir que les informations en question peuvent renseigner *uniquement* sur l'identité et le mode opératoire des auteurs de cyberattaques.

Le **canton BE** demande la suppression de la présente disposition si l'art. 73*c* est supprimé.

Selon **privatim**, l'accès par procédure d'appel, aux informations obtenues par le NCSC grâce à l'obligation de signaler, doit être limité ou réalisé au moyen d'une procédure «push». Ceci doit être valable pour le SRC (art. 76*a*, al. 2, LSI), pour les autorités de poursuite pénale (art. 76*a*, al. 3, LSI) et pour les services cantonaux chargés de la cybersécurité (art. 76*a*, al. 3, LSI).

- **Al. 4**

Le **canton BE** demande la suppression du présent alinéa si l'art. 73*c* est supprimé.

3.3.2.21 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[7] est applicable.

[7] RS **235.1**

[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.

7 participants à la consultation se sont exprimés sur la question de la coopération internationale. Aucun n'a rejeté cette disposition.

❖ **Remarques générales sur l'art. 77**

Swiss Banking soutient l'art. 77 si les informations sont nécessaires à la lutte contre les cyberrisques et notamment aux fins de la LSI (une restriction expressément prévue à l'art. 77, al. 1, 1re phrase). Si des données personnelles au sens de l'art. 75 sont impliquées, l'art. 6 LPD doit être respecté lors de leur transmission à l'étranger.

Scienceindustries est critique à l'égard de la transmission de données confidentielles, notamment de données personnelles. Il conviendrait ici de prévoir, de manière restrictive et avec validité pour les al. 1, 2 et 3, que la transmission de telles informations ne peut avoir lieu sans le consentement du détenteur des données.

VUD demande que l'échange d'informations avec les autorités étrangères conformément à l'art. 77 LSI se fasse strictement de manière anonyme.

Selon le **MPC**, l'art. 77 LSI devrait s'inscrire dans le cadre des dispositions déjà existantes en matière de coopération internationale, notamment dans le domaine de l'entraide judiciaire**.**

❖ **Demandes de modification et suggestions concernant l'art. 77**

- **<u>Al. 1</u>**

L'UTP considère que le rapport entre les dispositions de l'art. 77, al. 1, d'une part, et celles des art. 73*b*, al. 2, et 73*c*, d'autre part, n'est pas clair. **L'UTP** demande par conséquent que l'al. 1 prévoie que les art. 73*b*, al. 2, et 73*c* LSI soient applicables en plus de l'art. 6 LPD.

Privatim soutient l'al. 1.

L'ISSS demande que l'al. 1 prévoie que l'art. 10*a* LPD soit applicable en plus de l'art. 6 LPD.

- **<u>Al. 2</u>**

Afin de garantir que lors de l'échange d'informations, l'autorité étrangère utilise les informations reçues uniquement dans le but de lutter contre les cyberrisques, **Swiss Banking** propose de compléter la réglementation afin de prévoir que les informations transmises doivent être traitées de manière confidentielle par l'autorité en question et qu'elles ne peuvent pas être transmises si cela mettrait en péril la sécurité de l'entreprise ou des personnes concernées.

L'ISSS demande d'ajouter à l'al. 2 que l'échange d'informations n'est autorisé que si les services étrangers ou internationaux garantissent que les données seront utilisées conformément à la législation sur la protection des données.

- **<u>Al. 3</u>**

Le MPC demande qu'un mécanisme de coordination soit prévu et propose par conséquent d'ajouter une 2e phrase à l'al. 3 prévoyant que les informations transmises peuvent être utilisées pour justifier une demande d'assistance administrative ou d'entraide judiciaire.

Sachant que le NCSC n'est pas une autorité de poursuite pénale, **privatim** demande plus de précisions quant aux dispositions d'où découlent les compétences nationales en matière d'assistance administrative et d'entraide judiciaire.

3.3.2.22 Art. 79, al. 1 (Conservation et archivage des données)

[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.

10 participants à la consultation se sont exprimés sur le délai de conservation des données personnelles par le NCSC.

❖ **Remarques générales sur l'art. 79, al. 1**

CH++ propose ici de qualifier la notion d'«utilisation», par exemple qu'il soit question d'«utilisation obligatoire». La simple ouverture d'un enregistrement ne peut évidemment pas entraîner une prolongation de la durée de conservation autorisée.

L'UTP, Migros ainsi que l'UZH, l'UNIL et le PNR 77 demandent plus de précisions quant à l'expression «dernière utilisation».

Selon **l'ISSS, Härting Rechtsanwälte et privatim**, le principe de proportionnalité en matière de protection des données impose que les données ne soient conservées que le temps nécessaire à la réalisation de l'objectif. Des modèles anonymisés peuvent être générés à partir des données personnelles. **L'ISSS et Härting Rechtsanwälte** proposent de limiter à six mois la durée de conservation des données sensibles et d'autoriser la conservation pour une durée illimitée des enseignements tirés de données personnelles, sous la forme de modèles identifiés ou sous une forme anonymisée.

La CCPCS demande que le délai de conservation des données soit aligné sur les art. 97 et 109 du code pénal.

Le canton **BE** demande que la disposition soit adaptée afin que les données ne soient en règle générale pas effacées avant la fin du délai de prescription de l'action pénale pour les infractions concernées.

3.3.2.23 Modification d'autres lois

Les lois mentionnées ci-après sont modifiées comme suit:

1. Loi du 23 mars 2007 sur l'approvisionnement en électricité[8]

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[9]

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.

8 RS **734.7**
9 RS **235.1**, FF **2020** 7397

Seuls 6 participants à la consultation ont pris position sur la modification de la loi sur l'approvisionnement en électricité (LApEl) et de la LPD. Aucun n'a demandé la suppression de l'art. 8*a* LApEl. **L'ISSS et Härting Rechtsanwälte** ont demandé la suppression de l'art. 24, al. 5bis, LPD.

- **Remarques générales sur l'art. 24, al. 5bis, LPD**

L'UTP demande que l'art. 24, al. 5bis, LPD soit modifié de sorte que le PFPDT puisse transmettre le signalement *uniquement* avec l'accord du responsable.

Le canton **GE** considère qu'il faut prévoir une communication contraignante de la part du NCSC au PFPDT ; la communication du PFPDT n'a pas à obtenir l'autorisation de la personne responsable du signalement si ce dernier remplit les conditions de la présente loi.

UZH, l'UNIL et le PNR 77 soulignent que la totalité des données sensibles doivent pouvoir être transmises et pas seulement certaines d'entre elles.

- **Rejet de l'art. 24, al. 5bis, LPD**

L'ISSS et Härting Rechtsanwälte demandent la suppression de cette disposition, car si un service central est créé pour enregistrer tous les signalements , ce complément n'est plus nécessaire.

3.4 Autres demandes et suggestions concernant l'avant-projet

Swiss Banking demande que le présent texte de loi soit harmonisé avec la Communication FINMA sur la surveillance 05/20 – Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA.-

IG eHealth demande que le Conseil fédéral et le Parlement garantissent que le NCSC obtienne suffisamment de ressources en personnel.

Le canton **ZH** propose d'instaurer l'obligation de signalement par étapes (par ex. secteur par secteur), afin de commencer par recueillir des expériences.

La CCPCS demande de régler la manière dont les autorités de poursuite pénale doivent traiter les signalements lorsqu'elles reçoivent un signalement à la place du NCSC.

L'asut, Swisscom et Sunrise demandent une bonne coordination entre ce projet et la révision de l'ordonnance sur les services de télécommunication.

3.5 Demandes et suggestions sur d'autres thèmes

CH++ et Pour Demain soutiennent la transformation du NCSC en un office fédéral. Le **Parti Pirate** demande la création d'un département de la transformation numérique.

Le canton **FR** demande qu'outre l'introduction d'une obligation de signalement, d'autres mesures soient mises en œuvre afin de lutter contre la cybercriminalité (par ex. des mesures de sensibilisation de la population).

Le **Parti Pirate** demande que les infrastructures critiques utilisent à l'avenir uniquement des logiciels *open source* (OSS). Par ailleurs, il estime qu'il faut créer un fonds bien doté pour financer des audits de sécurité de logiciels courants (par ex. OSS / FOSS). À long terme, la Suisse doit se doter des ressources nécessaires pour développer et produire elle-même le matériel et les logiciels requis pour les infrastructures critiques.

4 Annexe

4.1 Cantons

ZH	Staatskanzlei des Kantons Zürich	Neumühlequai 10 Postfach 8090 Zürich staatskanzlei@sk.zh.ch
BE	Staatskanzlei des Kantons Bern	Postgasse 68 3000 Bern 8 info@sta.be.ch
LU	Staatskanzlei des Kantons Luzern	Bahnhofstrasse 15 6002 Luzern staatskanzlei@lu.ch
UR	Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf ds.la@ur.ch
SZ	Staatskanzlei des Kantons Schwyz	Regierungsgebäude Bahnhofstrasse 9 Postfach 1260 6431 Schwyz stk@sz.ch
OW	Staatskanzlei des Kantons Obwalden	Rathaus 6061 Sarnen staatskanzlei@ow.ch
NW	Staatskanzlei des Kantons Nidwalden	Dorfplatz 2 Postfach 1246 6371 Stans staatskanzlei@nw.ch
GL	Staatskanzlei des Kantons Glarus	Rathaus 8750 Glarus staatskanzlei@gl.ch
ZG	Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug info@zg.ch
FR	Chancellerie d'État du Canton de Fribourg	Rue des Chanoines 17 1701 Fribourg chancellerie@fr.ch
SO	Staatskanzlei des Kantons Solothurn	Rathaus Barfüssergasse 24 4509 Solothurn kanzlei@sk.so.ch
BS	Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel staatskanzlei@bs.ch
BL	Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal landeskanzlei@bl.ch
SH	Staatskanzlei des Kantons Schaffhausen	Beckenstube 7 8200 Schaffhausen

		staatskanzlei@ktsh.ch
AR	Kantonskanzlei des Kantons Appenzell Ausserrhoden	Regierungsgebäude 9102 Herisau Kantonskanzlei@ar.ch
AI	Ratskanzlei des Kantons Appenzell Innerrhoden	Marktgasse 2 9050 Appenzell info@rk.ai.ch
SG	Staatskanzlei des Kantons St. Gallen	Regierungsgebäude 9001 St. Gallen info.sk@sg.ch
GR	Standeskanzlei des Kantons Graubünden	Reichsgasse 35 7001 Chur info@gr.ch
AG	Staatskanzlei des Kantons Aargau	Regierungsgebäude 5001 Aarau staatskanzlei@ag.ch
TG	Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld staatskanzlei@tg.ch
TI	Cancelleria dello Stato del Cantone Ticino	Piazza Governo 6 6501 Bellinzona can-scds@ti.ch
VD	Chancellerie d'État du Canton de Vaud	Place du Château 4 1014 Lausanne info.chancellerie@vd.ch
VS	Chancellerie d'État du Canton du Valais	Planta 3 1950 Sion Chancellerie@admin.vs.ch
NE	Chancellerie d'État du Canton de Neuchâtel	Le Château Rue de la Collégiale 12 2000 Neuchâtel Secretariat.chancelle-rie@ne.ch
GE	Chancellerie d'État du Canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3 service-adm.ce@etat.ge.ch
JU	Chancellerie d'État du Canton du Jura	2, rue de l'Hôpital 2800 Delémont chancellerie@jura.ch
CCDJP	CCDJP Conférence des directrices et directeurs des départe-ments cantonaux de justice et police (CCDJP)	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@kkjpd.ch
CDS	CDS Conférence suisse des directeurs de la santé	Haus der Kantone Speichergasse 6 Postfach 3001 Bern office@gdk-cds.ch
CG MPS	CG MPS Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers	Haus der Kantone Speichergasse 6 Postfach

		3001 Bern
CCPS	CCPS Conférence des Commandants des Polices Cantonales de Suisse	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@kkpks.ch
CPS	Conférence des procureurs suisses	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@ssk-cps.ch

4.2 Partis politiques représentés à l'Assemblée fédérale

Le Centre	Le Centre	Generalsekretariat Hirschengraben 9 Postfach 3001 Bern info@die-mitte.ch
PLR	Les Libéraux-Radicaux	Generalsekretariat Neuengasse 20 Postfach 3001 Bern info@fdp.ch
Les VERT-E-S suisses	Les VERT-E-S suisses	Waisenhausplatz 21 3011 Bern gruene@gruene.ch
PVL	Parti vert'libéral Suisse	Monbijoustrasse 30 3011 Bern schweiz@grunliberale.ch
UDC	Union démocratique du centre	Generalsekretariat Postfach 8252 3001 Bern gs@svp.ch
PS	Parti socialiste suisse	Zentralsekretariat Theaterplatz 4 Postfach 3001 Bern verena.lo-embe@spschweiz.ch

4.3 Associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national

UVS	Union des villes suisses	Monbijoustrasse 8 Postfach 3001 Bern info@staedteverband.ch

4.4 Associations faîtières de l'économie qui œuvrent au niveau national

economiesuisse	Fédération des entreprises suisses	Hegibachstrasse 47 Postfach 8032 Zürich info@economiesuisse.ch bern@economiesuisse.ch sandra.spieser@economiesuisse.ch
Swissbanking	L'Association suisse des banquiers	Hotelgasse 10, 3011 Bern
USAM	Union suisse des arts et métiers	Schwarztorstrasse 26 Postfach 3001 Bern info@sgv-usam.ch
USS	Union syndicale suisse	Monbijoustrasse 61, 3007 Bern, info@sgb.ch

4.5 Autres milieux concernés – avis sur invitation

eGov-Schweiz	Association eGov-Schweiz	c/o mundi consulting ag Marktgasse 55 Postfach 3001 Bern info@eGov-Schweiz.ch
privatim	Conférence des Préposé(e)s suisses à la protection des données	c/o Dr. Beat Rudin, Advokat, Postfach 205 4010 Basel kommunikation@privatim.ch
Digitale Gesellschaft	Digitale Gesellschaft	4000 Basel office@digitale-gesellschaft.ch
eHealth	Interessengemeinschaft eHealth	Amthausgasse 18 3011 Bern info@ig-ehealth.ch
asut	ASSOCIATION SUISSE DES TÉLÉCOMMUNICATIONS	Hirschengraben 8 3011 Bern info@asut.ch
Interpension	Inter-pension Interessengemeinschaft autonomer Sammel- und Gemeinschaftseinrichtungen	Gartenstrasse 2 3063 Ittigen info@inter-pension.ch
RAILplus AG	RAILplus AG	Hintere Bahnhofstrasse 85 5001 Aarau info@railplus.ch

AEROSUISSE	Fédération faîtière de l'aéronautique et de l'aérospatiale suisses	Kapellenstrasse 14 Postfach 3001 Bern info@aerosuisse.ch

4.6 Autres milieux concernés – commentaires spontanés

eAVS/AI	eAVS/AI	p.a. mundi consulting ag Marktgasse 55 Postfach 3001 Bern jerome.brugger@mundicon-sulting.com
ISSS	Information security society switzerland	Kochergasse 6 3011 Bern sekretariat@isss.ch

Centre Patronal	Centre Patronal	Route du Lac 2 1094 Paudex info@centrepatronal.ch
CH++	CH++	marcel.salathe@chplus-plus.org
Ausland-banken	Verband der Auslandsbanken in der Schweiz	Usteristrasse 23 8001 Zürich info@afbs.ch
MPC	Ministère public de la Confédération	Guisanplatz 1 3003 Bern info@ba.admin.ch
la Poste	La Poste Suisse SA	Wankdorfallee 4 Postfach 3030 Bern regulatoryaffairs@post.ch
digitals-wit-zerland	digitalswitzerland	Waisenhausplatz 14 3011 Bern office@digitalswitzerland-bern.ch
FER	Fédération des entreprises romandes	98 rue de Saint-Jean 1211 Genève 11 yannic.forney@fer-ge.ch
Swico	Swico	Lagerstrasse 33 8004 Zürich info@Swico.ch
GEM	Groupement des Entreprises Multinationales	Rue de Saint-Jean 98 1211 Genève 3 info@gemonline.ch
Pour de-main	Pour demain	Marktgasse 46 3011 Berne info@pourdemain.ch
Santésui sse	Association de la branche de l'assurance-maladie sociale	Römerstrasse 20 Postfach CH-4502 Solothurn mail@santesuisse.ch

Swis-sICT	SwissICT	Vulkanstr. 120 8048 Zürich info@swissict.ch
Swiss-mem	Association pour les PME et les grandes entreprises de l'industrie technologique suisse	Pfingstweidstrasse 102 Postfach CH-8037 Zürich r.rudolph@swissmem.ch
swissuni versities	Assocaition des des hautes écoles suisses	swissuniversities Effingerstrasse 15 Case Postale 3001 Berne weiss@swissuniversities.ch
VUD	Verein Unternehmendatenschutz	Verein Unternehmens-Daten-schutz VUD c/o IT & Law Consulting GmbH Sternenstrasse 18, 8002 Zürich info@vud.ch
UTP	Union des transports publics	Dählhölzliweg 12 CH-3000 Bern 6 info@voev.ch
AES	Association des entreprises électriques suisses	Hintere Bahnhofstrasse 10 5000 Aarau info@strom.ch
ASIP	Association Suisse des Institutions de Prévoyance	Kreuzstrasse 26 8008 Zurich info@asip.ch
Sci-encein-dustries	Association des Industries Chimie Pharma Life Sciences	Nordstrasse 15 Postfach 8021 Zürich Schweiz info@scienceindustries.ch
Suisse-digital	Association des réseaux de communication	Bollwerk 15 CH-3011 Bern info(at)suissedigital.ch
SSIGE	Société Suisse de l'Industrie du Gaz et des Eaux SSIGE	Grütlistrasse 44 | Postfach | 8027 Zürich info@svgw.ch
ASA	Association suisse d'assurances	Conrad-Ferdinand-Meyer-Strasse 14 Case postale CH-8022 Zurich info@svv.ch
ABG	Association de banques suisses de gestion	
Gachn-ang	Commune de Gachnang (TG)	Hôtel de ville de Gachnang Islikonerstrasse 7 8547 GACHNANG Suisse
NFP 77 ETHZ UNIL	Prise de position commune	
Opera-tion Li-bero	Mouvement	OPERATION LIBERO CH-3000 Bern futur@operation-libero.ch
AEIS	Fondation institution supplétive LPP	Elias-Canetti-Strasse 2 Postfach 8050 Zurich

		urs.mueller(S)aeis.ch
Trust Valley	Fondation Trust Valley	Trust Valley EPFL Innovation Park, Bâtiment C CH-1015 Lausanne
UniBE	Université de Berne	Dr. Cord-Ulrich Fündeling Leiter Informatikdienste Hochschulstrasse 6 3012 Bern cord.fuendeling@unibe.ch
UniGE Digital Law Centre	Université de Genève	Digital Law Center - Uni Mail - Bd du Pont d'Arve 40 - CH-1211 Genève 4 Suisse digitallawcenter@unige.ch
Abraxas	Entreprise Abraxas Informatik AG	The Circle 68 | CH-8058 Zürich-Flughafen peter.gassmann@abraxas.ch
Axpo	Axpo services AG	Axpo Services AG Parkstrasse 23 | 5401 Baden | Switzerland thomas.porchet@axpo.com
Beat Lehmann		Acting Counsel Alcan Holdings Switzerland AG Kongoweg 9 (Home Office) 5034 Suhr b.lehmann-aarau@bluewin.ch
Coop	Coop Genossenschaft	Thiersteinerallee 12 Postfach 2550 4002 Basel Damian.Misteli@coop.ch
Aéroport de ZH		Zürich Flughafen CH-8058 Andrew.karim@zurich-airport.ch
Aéroport de GE		Aéroport international de Genève CP100 CH 1215 Genève
Härting Rechtsanwälte		Landis Gyr Strasse 1 6300 Zug office@haerting.ch
Helvetia	Helvetia assurances AG	Helvetia Versicherungen Hauptsitz St. Alban-Anlage 26 4002 Basel martin.jara@helvetia.ch
Migros	Migros-Genossenschafts-Bund	
Raffeisen		cecile.kessler@raiffeisen.ch
Romande Energei		Rue de Lausanne 53 1110 Morges Oscar.parado@romande-energie.ch
Salt		Salt Mobile SA Rue du Caudray 4

		CH-1020 Renens 1
CFF		
Sunrise	Sunrise UPC	Sunrise UPC GmbH Thurgauerstrasse 101B, 8152 Glattpark (Opfikon) Marcel.Huber@sunrise.net
Suva		Fluhmattstrasse 1 Case postale 4358 6004 Luzern Marc.epelbaum@suva.ch
Swiss		Swiss International Air Lines AG P.O. Box ZRHS/V/ABRO CH-8 ronald.abegglen@swiss.com 058 Zürich-Flughafen
Swisscom		Alte Tiefenaustrasse 6 3048 Worblaufen Lorenz.Ing-lin@swisscom.com
Swiss-grid		Bleichemattstrasse 31 Postfach 5001 Aarau info@swissgrid.ch
Switch		Werdtstrasse 2 Postfach 8021 Zürich
TPG	Transports publics genevois	Route de la Chapelle 1 -.Case postale 950 - 1212 Grand-Lancy 1 - Suisse Meyer.G@tpg.ch
Parti pirate suisse	Parti pirate suisse	Piratenpartei Bern, 3000 Bern info@be.piratenpartei.ch