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