UNIVERSITÉ DE GENÈVE
FACULTÉ DE DROIT
Centre de droit du numérique

Digital Law Center
www.digitallawcenter.ch

Département fédéral des finances DFF
Monsieur Ueli Maurer
Conseiller fédéral
Bundesgasse 3
3003 Berne

ncsc@gs-efd.admin.ch

Genève, le 14 avril 2022

Procédure de consultation relative à l'obligation de signaler les cyberattaques pour les infrastructures critiques – prise de position

Monsieur le Conseiller fédéral, Mesdames, Messieurs,

Nous avons pris connaissance du projet cité en titre, qui a retenu toute notre attention et vous adressons, par la présente, notre position quant à celui-ci.

Nous approuvons de manière générale le projet qui nous semble être un moyen approprié afin d'atteindre le but visé, dans la mesure où les cyberattaques sont devenues l'une des principales menaces pour la sécurité et l'économie suisse. Leur signalement permettrait une meilleure vue d'ensemble de la situation en Suisse, d'aider les victimes à gérer les cyberattaques et d'avertir à temps les autres exploitants d'infrastructures critiques. Nous nous permettons les 4 commentaires suivants :

1. Délai

Nous estimons qu'il serait **utile de préciser le délai de signalement** prévu pour l'instant de façon indéterminée (*cf.* art. 74a al. 1 P-LSI « *le plus rapidement possible après leur découverte* »), sans remettre en cause la possibilité d'un signalement en deux temps (*cf.* art. 74e al. 2 P-LSI).

Nous comprenons que les entreprises ignorent souvent à quel point l'attaque est grave et ce qui s'est passé précisément (AP-LSI, p. 21), ce qui pourrait expliquer pourquoi ne pas préciser de délai. Or, la précision d'un délai renforcerait la sécurité juridique, d'autant que la possibilité d'un signalement en deux temps permet précisément de tenir compte du fait que les entreprises ignorent souvent l'étendue de l'attaque. A titre de comparaison, les obligations FINMA sont plus précises, puisqu'il est prévu aussi un signalement en deux temps mais de façon précise, soit une obligation de signalement dans les 24h après une première évaluation de la gravité de la cyberattaque critique et, dans les 72 heures, via la plate-forme de saisie (Communication FINMA sur la surveillance 05/2020, p. 4). Les réglementations étrangères sont souvent aussi plus précises. Par exemple, en Europe il est prévu un délai de 24h à 72h suivant l'impact/la gravité de l'incident et un délai de 1 mois pour soumettre le rapport final (art. 20 directive SRI). Aux Etats-Unis, il est prévu un délai de 72h et, exceptionnellement, 24h en cas de paiement d'une rançon (CISA sec. 2242(a)(1)(A).

2. Définition de cyberattaques et cyberincidents

Nous estimons qu'il serait **utile de préciser la définition de cyberattaques et cyberincidents** (*cf.* art. 5 let. d et e), soit que ces événements peuvent aussi survenir et être qualifiés comme tels **même en l'absence de toute violation de la sécurité des données** ou d'autres dispositions légales ou réglementaires.

Cette précision renforcerait selon nous la sécurité juridique. A titre de comparaison, la LPD du 25 septembre 2020 (nLPD) (et le RGPD) prévoit une obligation d'annonce en cas de "*violation de la sécurité des données entraînant vraisemblablement un risque élevé*" (art. 24 nLPD ; art. 33 RGPD), ce qui rend incertain d'annoncer en cas de cyberincident malgré le respect de toutes les mesures de sécurité des données.

3. Liste des secteurs

Nous saluons le fait que la liste des secteurs critiques est large et inclut des secteurs, tels que les hautes écoles, contrairement à d'autres législations, notamment européennes. Nous partageons votre avis selon lequel les **hautes écoles sont d'une grande importance** pour la formation et l'économie en Suisse, leurs activités de recherche en particulier, constituant un moteur de l'innovation, ce qui fait ainsi d'elles une cible privilégiée pour les cyberattaques, comme nous le montre encore l'actualité récente.

Nous considérons en revanche important **d'assouplir la possibilité de mettre à jour et de préciser** les secteurs critiques, par exemple à travers une autorité délégatrice et/ou un mécanisme souple d'adaptation. A titre de comparaison, aux Etats-Unis, les 16 secteurs d'infrastructures identifiés comme critiques peuvent être définis plus clairement par la Cybersecurity and Infrastructure Security Agency (CISA sec. 2242(b)(1)). En Chine, les entités concernées sont aussi identifiées et précisées par les régulateurs sectoriels (Règlement sur la protection de la sécurité des infrastructures d'information critiques, art. 8 ss).

4. Mesures complémentaires

Nous tenons finalement à souligner le fait que l'objet de cette consultation, notamment l'introduction de l'obligation de **signalement des cyberattaques, ne représente qu'un pan de la lutte** contre la cybercriminalité. Il est également important que tout un travail en amont soit fait, par des mesures de sensibilisation, de prévention et de formation des acteurs des milieux concernés ainsi que de la population de manière générale, au niveau fédéral et cantonal.

A la lumière de ce qui précède, nous réitérons notre soutien au projet.

Nous vous remercions de l'attention que pour porterez à la présente et vous prions de croire, Monsieur le Conseiller fédéral, à l'expression de notre haute considération.

* * *

Prof. Yaniv Benhamou
Prof. Jacques de Werra
Mme Louise Wang

Pour le Digital Law Center