Collection lausannoise
CEDIDAC

Camille Perrier Depeursinge / Sylvain Métille /
Joëlle Vuille (éditeurs)

Lutter contre la cybercriminalité en Suisse

Stämpfli
Éditions

Plusieurs approches pour lutter contre la cybercriminalité

SYLVAIN MÉTILLE
Professeur associé, Faculté de droit, des sciences criminelles et d'administration publique, Université de Lausanne
Avocat associé, Étude HDC

PAULINE MEYER
Doctorante FNS, Faculté de droit, des sciences criminelles et d'administration publique, Université de Lausanne

Table des matières

I. Introduction

La cybercriminalité désigne les infractions pénales commises à l'encontre ou au moyen d'un système d'information et de communication. C'est donc le droit pénal qui sert à dissuader de commettre ces infractions et à

sanctionner celles qui ont été commises, dans la mesure où leurs auteurs sont identifiés et les conditions de leur poursuite réunies (II).

En pratique, cette approche unique ne suffit pas à appréhender l'ensemble des enjeux liés aux comportements délictuels dans le cyberespace. En effet, si l'effet dissuasif du droit pénal suffisait à empêcher la réalisation de tout comportement délictuel, aucune infraction n'aurait lieu. Ce serait évidemment très satisfaisant, mais cela ne correspond pas à la réalité du terrain.

Il est important de s'intéresser à l'ensemble des personnes concernées par la réalisation d'une infraction : celles susceptibles de passer à l'acte et les auteurs d'infractions, mais également les potentielles lésées d'actes de cybercriminalité. Ces dernières peuvent aussi agir pour rendre la commission d'infractions plus difficiles ou en réduire le caractère attrayant. Elles diminuent ainsi leur probabilité d'être lésées à titre individuel, mais participent en même temps à un effort collectif de lutte simple et efficace contre la cybercriminalité.

Ce n'est pas le droit pénal qui permet aux victimes de mieux s'armer contre la cybercriminalité, mais la cybersécurité. La cybersécurité contribue à une protection contre la cybercriminalité, en réduisant le risque de faire l'objet d'une attaque réussie (III.B). Comme nous le verrons, certaines lois poussent les organisations à augmenter leur cybersécurité. Les exigences de cybersécurité permettent de diminuer l'attrait que peuvent présenter les personnes physiques et morales pour des délinquants. La cybersécurité permet également de rendre plus difficile la réalisation d'actes de cybercriminalité.

Certains domaines du droit, plus transversaux encore, apportent des considérations de cybersécurité et participent à rendre plus difficile, ou moins intéressante, la commission d'infractions. C'est par exemple le cas de la protection des données personnelles, avec ses obligations de sécurité (III.C).

Finalement, le droit n'étant pas l'unique réponse face à la cybercriminalité, d'autres incitations doivent permettre une augmentation de la cybersécurité au sein de la société, parmi lesquelles en particulier l'éducation et la sensibilisation (III.D).

II. La répression et la prévention générale

Le droit pénal est un mode de contrôle social qui permet à l'État d'incriminer et de pénaliser certains comportements[1]. Il a une fonction réactive et sanctionnatrice, mais également préventive (dans une moindre mesure).

1 HURTADO POZO/GODEL, N 3.

En termes de dissuasion ou de prévention primaire, le droit pénal sert typiquement à la prévention des dangers collectifs, à l'intimidation d'auteurs potentiels et à l'encouragement à toute personne de veiller au respect des normes. Le droit pénal comporte également des dimensions de prévention secondaire et tertiaire, dont font partie la neutralisation des personnes à l'origine d'actes délictuels ou les mesures tendant à diminuer la probabilité de récidive[2].

Le droit pénal est prévu dans le CP[3] et le CPP[4], lois centrales consacrant les infractions applicables à une majorité des actes de cybercriminalité et les compétences des autorités de poursuite pénale[5]. Ce cadre légal produit un effet dissuasif sur la population comme sur les délinquants. La Cyberstratégie (CSN) publiée en 2023 par le Conseil fédéral compte par ailleurs parmi ses objectifs un renforcement des ressources pour la lutte contre la cybercriminalité. Le cadre légal et son application devraient donc encore être renforcés ces années à venir[6].

De nombreux éléments peuvent être utilisés pour expliquer pourquoi le droit pénal n'a pas un effet dissuasif suffisant en matière de cybercriminalité. Premièrement, les auteurs ont souvent un sentiment d'impunité, étant cachés derrière leur ordinateur. Cela est renforcé lorsqu'ils agissent depuis l'étranger, étant très loin de la victime et des autorités de poursuite pénale qui risquent en priorité de s'intéresser à eux[7]. Les difficultés pratiques auxquelles ces autorités font face dans les enquêtes internationales leur donnent également l'impression d'être à l'abri[8]. Même dans le cas d'auteurs présents en Suisse, les efforts mis dans la poursuite des infractions commises en ligne restent souvent inférieurs à ceux concernant des infractions commises dans la vie réelle[9].

Deuxièmement, le gain possible peut être très important. Dans le cas d'escroqueries ou de chantage, les montants demandés ne sont parfois pas très élevés pour les victimes en Suisse[10]. Ils peuvent néanmoins déjà constituer une motivation très intéressante selon le coût de la vie et les revenus possibles dans le pays où se trouve l'auteur[11]. À l'inverse, comme ces montants ne sont pas

2 QUELOZ, p. 7, 11, 13 et 15.
3 Code pénal suisse du 21 décembre 1937 (CP), RS 311.0.
4 Code de procédure pénale suisse du 1er janvier 2011 (CPP), RS 312.0.
5 HURTADO POZO/GODEL, N 10 s.
6 Conseil fédéral, SN, p. 28 à 31.
7 GHERNAOUTI, p. 20.
8 NICOLET/PEISSARD, p. 165 ss.
9 IRL (*in real life*), même si toutes les infractions commises en ligne un évidemment un impact sur la vie réelle des personnes concernées.
10 Cela ne signifie pas pour autant qu'il n'y a pas de cas où les montants demandés sont importants, l'un n'empêchant pas l'autre. Les montants moins importants appellent généralement moins de vigilance et peuvent être commis plus facilement.
11 De plus, la criminalité sérielle permet à ses auteurs de s'enrichir en commettant une série d'infractions portant sur des montants relativement faibles.

toujours très importants en Suisse, ils peuvent décourager les victimes à déposer plainte et à engager une procédure civile ou pénale. Ainsi tant la prévention que la répression s'en trouvent diminuées.

Troisièmement, l'automatisation et la reproductibilité de certaines infractions les rendent aussi très intéressantes. L'auteur peut valoriser beaucoup plus facilement son investissement dans le monde virtuel que dans le cas d'un cambriolage par exemple. Une fois qu'il a développé un logiciel malveillant, il lui suffit de le diffuser[12]. L'effort pour atteindre une ou plusieurs cibles est assez similaire.

Quatrièmement, les auteurs vont souvent s'appuyer sur des erreurs ou incompétences des victimes[13], les rendant parfois honteuses et peu enclines à engager des poursuites pénales. Les victimes ne disposent souvent pas des mesures appropriées pour prévenir des actes de cybercriminalité, alors qu'il est nécessaire qu'elles soient incitées à se prémunir contre des cyberattaques.

Tant que des infractions continuent d'être réalisées quotidiennement avec des conséquences importantes, il faut reconnaître que le droit pénal n'a pas un effet dissuasif suffisant. Il est donc nécessaire d'utiliser d'autres moyens tendant à rendre la commission d'infractions plus difficile, ainsi qu'à diminuer d'une part l'attrait des victimes potentielles et d'autre part la probabilité d'être la cible d'une attaque réussie. Pour ce faire, la cybersécurité doit permettre de renforcer les mesures de protection.

III. La diminution de l'intérêt à commettre des infractions

A. Le principe

Plusieurs moyens existent pour rendre la commission d'une infraction plus compliquée et pour en diminuer l'attrait. Plus le niveau de sécurité est élevé, moins les auteurs seront tentés de commettre des infractions[14]. Un effort plus important sera en effet attendu de leur part, ce qui rend le coût de l'opération plus élevée sans pour autant en augmenter le bénéfice. Les chances de succès de la cyberattaque sont aussi moindres.

Par exemple, plus les individus au sein d'une entreprise sont informés et sensibilisés sur des pratiques de cyberhygiène, moins ils sont susceptibles de tomber dans un piège tendu par un délinquant. De la même manière, la mise en place

12 NCSC, Rapport semestriel 2021/1, p. 15 ; TEICHMANN/GERBER, N 1.
13 NCSC, Rapport semestriel 2022/1, p. 35.
14 Sur la prévention situationnelle, voir MARKWALDER, Internet et facilitation du passage à l'acte, p. 3 .

de correctifs sur des vulnérabilités permet de limiter les risques que des personnes mal intentionnées exploitent ces dernières, pour compromettre des moyens informatiques et altérer les informations qui y sont traitées.

B. La cybersécurité

1. Les objectifs de la cybersécurité

La cybersécurité est étroitement liée à la poursuite pénale de la cybercriminalité. Elle comprend les mesures permettant de prévenir et de gérer les cyberincidents ainsi qu'à améliorer la résilience face aux cybermenaces[15]. Les cyberincidents sont des évènements « *survenant lors de l'utilisation de moyens informatiques et ayant pour conséquence une atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'informations ou à la traçabilité de leur traitement* » (art. 5 lit. d LSI2[16]). Les cyberattaques sont un type particulier de cyberincidents, soit des cyberincidents provoqués intentionnellement[17].

La cybersécurité vise à permettre aux personnes susceptibles de faire l'objet d'un cyberincident de prévenir, détecter et réagir à de tels incidents. Il s'agit de responsabiliser les personnes physiques et morales, pour qu'elles puissent diminuer la probabilité d'être victimes d'actes de cybercriminalité ou d'être utilisées comme vecteur par des délinquants afin de causer du tort à d'autres personnes. En cas d'attaques abouties, la cybersécurité permet aux lésées de rétablir au plus vite une situation sûre.

2. Un cadre légal disparate

Il n'existe pas en Suisse une loi générale sur la cybersécurité applicable à l'ensemble de la population, à l'image du Code pénal. Le cadre légal fonctionne d'une façon radicalement différente. Les bases légales en vigueur ne s'appliquent pas à tout individu, mais à des cercles limités d'assujettis. L'autoréglementation et la réglementation sectorielle sont privilégiées par l'État et le fédéralisme implique une certaine réserve de la Confédération, qui souhaite conserver un rôle partenarial et subsidiaire[18].

---

15 Conseil fédéral, CSN, p. 9.

16 Modification du 29 septembre 2023 de la Loi fédérale sur la sécurité de l'information au sein de la Confédération (FF 2023 2296, LSI2). Lorsque la loi n'est pas modifiée, nous continuons à utiliser l'abréviation LSI.

17 Voir art. 5 lit. e LSI2.

18 Conseil fédéral, CSN, p. 12 et 21.

Certains secteurs élaborent des réglementations (contraignantes et non contraignantes) de cybersécurité. Les actes législatifs adoptés dans ce contexte s'appliquent régulièrement à certaines « infrastructures critiques », soit des organisations essentielles à l'économie nationale, au bien-être de la population ou au fonctionnement de la société[19]. Les infrastructures critiques sont définies à l'art. 5 lit. c LSI[20] comme « *l'approvisionnement en eau potable et en énergie, les infrastructures d'information, de communication et de transports ainsi que d'autres installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population* ». Cette définition très générale renvoie implicitement aux organisations actives dans les secteurs critiques reconnus en Suisse dont les secteurs des autorités, de l'approvisionnement en énergie, des transports ou encore de la santé[21].

Parmi les secteurs réglementés, les autorités et les organisations de la Confédération sont aujourd'hui soumises à la LSI. La LSI doit permettre aux autorités et organisations assujetties de se protéger de la cybercriminalité, de l'empêcher et de remédier à ses conséquences. La LSI adopte une approche globale des mesures techniques et organisationnelles permettant d'une part d'assurer la sécurité de l'information et d'autre part la sécurité des moyens informatiques[22]. Cette loi est en voie de révision pour introduire une obligation de signaler les cyberattaques visant les infrastructures critiques[23], à savoir à un cercle d'organisations plus étendu que celui des autorités et organisations de la Confédération[24].

19 Les sous-secteurs critiques regroupent « *tout système de services ou d'approvisionnement qui englobe l'ensemble d'un processus d'approvisionnement et couvre tous les domaines pertinents pour le fonctionnement du système en question* », voir FF 2023 1659, p. 7. Les secteurs critiques regroupent des domaines tels que la santé, les autorités, les finances ou encore les transports, voir FF 2023 1569, p. 6.

20 Loi fédérale du 1er mai 2022 sur la sécurité de l'information au sein de la Confédération (LSI), RS 128.

21 Il existe neufs secteurs critiques en Suisse : les autorités, l'énergie, l'élimination, les finances, la santé, l'information et la communication, l'alimentation, la sécurité publique et les transports, voir FF 2023 1659, p. 6 s.

22 La LSI distingue la sécurité de l'information et la sécurité des moyens informatiques, HUSI-STÄMPFLI, N 21 ss et 30. Les notions de sécurité de l'information et de sécurité des moyens informatiques se recoupent avec la notion de cybersécurité ; elles impliquent souvent des mesures similaires.

23 Sur la notion d'infrastructure critique, voir FF 2023 1659, p. 7.

24 La révision a été acceptée par les deux chambres du Parlement.

D'autres réglementations sectorielles existent, par exemple pour l'approvisionnement en électricité ou pour d'autres secteurs liés à l'approvisionnement économique du pays[25].

3. La Loi fédérale sur la sécurité de l'information

a) La portée de la loi

La LSI actuellement en vigueur a été adoptée parce que la Confédération a estimé que le cadre légal helvétique pour la sécurité de l'information était lacunaire et manquait de coordination[26]. La LSI visait initialement à assurer une plus grande sécurité des informations traitées par la Confédération et des moyens informatiques exploités pour ce faire (art. 1 al. 1 LSI ; art. 1 al. 1 lit. a LSI2)[27]. Les autorités et organisations de la Confédération traitent en effet beaucoup d'informations, souvent sensibles.

La LSI a fait l'objet d'une révision en 2023 afin d'introduire une nouvelle obligation de signaler les cyberattaques visant les infrastructures critiques[28]. Cette révision, qui n'est pas encore entrée en vigueur, vient soutenir un autre objectif jusque-là sous-jacent de la loi qui est l'amélioration de la capacité de résilience de la Suisse face aux cybermenaces (art. 1 al. 1 lit. b LSI2), par le renforcement des compétences dans le domaine de la cybersécurité et l'introduction de l'obligation de signaler les cyberattaques ciblant les infrastructures critiques[29].

Pour atteindre ses objectifs, la LSI instaure deux approches différenciées entre différents cercles d'assujettis. La première, applicable principalement aux autorités et organisations de la Confédération, dresse un catalogue d'exigences pour garantir la sécurité de l'information et la sécurité des moyens informatiques. La seconde impose à un cercle plus étendu d'autorités et d'organisations une obligation de signaler certaines cyberattaques.

---

25 Voir par exemple *infra* III.B.4 pour l'approvisionnement en électricité. Pour d'autres exemples, voir les normes minimales des différents secteurs de l'approvisionnement économique du pays, disponible sous : <https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html> (*consulté le 24.2.2024*).

26 FF 2017 2765, p. 2777.

27 DZAMKO-LOCHER, p. 113 s. ; HARASGAMA *et al.*, p. 42 ; HUSI-STÄMPFLI, N 29.

28 FF 2023 2296.

29 FF 2023 84, p. 20 s. ; MEYER/MÉTILLE, N 2.

b) Les exigences de sécurité

Le premier volet d'exigences posé par la LSI date de la première version de la loi et n'a pas été substantiellement modifié lors de la révision. Il impose des obligations aux autorités et organisations de la Confédération pour garantir la sécurité de l'information et la sécurité des moyens informatiques.

Les exigences s'appliquent dans tous les cas à l'Assemblée fédérale, au Conseil fédéral, aux tribunaux de la Confédération, au Ministère public de la Confédération et à son autorité de surveillance ainsi qu'à la Banque Nationale Suisse[30]. Certaines mesures attendues par la loi doivent être mises en place également par des organisations telles que les Services du Parlement, l'administration fédérale, les services administratifs des tribunaux de la Confédération, l'armée et les organisations de l'art. 2 al. 4 LOGA[31] Les cantons sont susceptibles d'être soumis à quelques dispositions de la loi[32].

La LSI adopte une approche fondée sur les besoins de protection et sur les risques[33]. Les exigences figurent aux art. 6 ss LSI et sont concrétisées dans l'OSI[34]. L'approche suivie est majoritairement préventive. En d'autres termes, l'on peut voir que de nombreuses mesures de prévention sont attendues des assujettis, en comparaison avec le nombre de mesures détectives ou réactives prévues par la loi. La LSI et son ordonnance imposent l'implémentation de mesures techniques et organisationnelles à l'instar de l'analyse de risques[35], de la formation des collaborateurs[36], de l'établissement d'un plan pour faire face aux « *graves violations de la sécurité de l'information susceptibles de menacer l'accomplissement de tâches indispensables de la Confédération* »[37] ou encore la réalisation d'entraînements en vue de tels incidents[38]. Elle impose également des obligations générales de détection et de réaction aux violations de la sécurité de l'information[39] ou encore la sécurité des moyens informatiques

30 Voir l'art. 2 al. 1 LSI.

31 Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA), RS 172.010. Le Conseil fédéral peut restreindre le champ d'application de la loi aux organisations de l'art. 2 al. 3 et 4 LOGA à celles exerçant des activités sensibles ou recourant et accédant aux moyens informatiques de la Confédération (art. 2 al. 3 LSI).

32 Art. 3 LSI ; FF 2017 2823 à 2825 ; HUSI-STÄMPFLI, N 26 à 28 ; MEYER/MÉTILLE, N 5 à 9.

33 Art. 6 à 8 LSI.

34 Ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI), RS 128.1.

35 Art. 8 al. 1 LSI, 8 al. 1 OSI.

36 Art. 11 OSI.

37 Art. 12 al. 2 LSI.

38 Voir art. 12 al. 2 LSI ; FF 2017 2765, p. 2828 ss ; SG-DDPS, Législation d'exécution relative à la loi sur la sécurité de l'information, Rapport explicatif, p. 13 ss ; ECKERT/GLAUS, p. 12 ; HUSI-STÄMPFLI, N 33 ss ; MEYER/MÉTILLE, N 16 ss.

39 Art. 12 al. 1 LSI.

exploités[40]. Le respect de ces exigences permet aux autorités et organisations assujetties de diminuer la probabilité d'être la cible d'actes de cybercriminalité ou que des délinquants utilisent leurs moyens informatiques ou les informations qu'elles traitent pour porter préjudice à des tiers.

c) L'obligation de signaler les cyberattaques

La modification de la LSI a principalement permis l'introduction de l'obligation de signaler les cyberattaques visant les infrastructures critiques[41]. Cette obligation devrait participer à l'amélioration de la résilience de la Suisse contre les cyberattaques.

L'art. 74*b* LSI liste les exploitants d'infrastructures critiques soumis à l'obligation en limitant les assujettis aux exploitants d'infrastructures critiques les plus importantes sur le plan national[42]. Par exemple, l'approvisionnement en biens d'usage quotidien indispensables (notamment en denrées alimentaires) compte de nombreux opérateurs plus ou moins importants dans la chaîne d'approvisionnement. Seules les organisations dont la défaillance partielle ou complète entraînerait de graves difficultés d'approvisionnement sont soumises à l'obligation de signaler les cyberattaques[43].

Les cyberattaques doivent être signalées lorsqu'elles mettent en péril le fonctionnement de l'infrastructure critique concernée, lorsqu'elles entraînent une manipulation ou une fuite d'informations, lorsqu'elles n'ont pas été détectées durant une période prolongée (particulièrement s'il y a des indices supposant qu'elles ont été exécutées en vue de préparer d'autres attaques) ou lorsqu'elles s'accompagnent d'actes de chantage, de menaces ou de contrainte[44].

Le signalement doit être effectué auprès de l'OFCS[45] dans les 24h suivant la détection de la cyberattaque. Il doit contenir des informations relatives

---

40 Art. 19 LSI ; voir notamment FF 2017 2831 ; MEYER/MÉTILLE, N 23 à 25.

41 Voir les art. 74*a* ss LSI2.

42 FF 2023 84, p. 34 ss ; ROESLE, p. 2 ; MEYER/MÉTILLE, N 49 s. Par ailleurs, pour éviter que les cyberattaques ayant un effet limité doivent être signalées, le Conseil fédéral peut exempter les assujetties à l'obligation lorsque les perturbations provoquées par les cyberattaques n'ont qu'un effet limité sur le fonctionnement de l'économie ou sur le bien-être de la population (art. 74*c* LSI2).

43 FF 2023 84, p. 39 s.

44 Voir art. 74*d* LSI2 ; FF 2023 84, p. 43.

45 Office fédéral de la cybersécurité, anciennement Centre national pour la cybersécurité (NCSC), voir SG-DDPS, Législation d'exécution relative à la loi sur la sécurité de l'information, Explications, p. 5 s.

notamment à l'entité ciblée, au mode opératoire de l'attaque ou encore aux effets et aux mesures envisagées et prises (art. 74*e* LSI2)[46].

Les signalements de cyberattaques effectués dans le cadre des art. 74*a* ss LSI2 permettent à l'OFCS de disposer d'une vue d'ensemble des cybermenaces[47]. Avec les informations que l'office obtient sur la base des signalements[48], il apporte un soutien technique à certaines autorités, dont celles chargées de la poursuite pénale. Les informations pouvant être transmises concernent l'identité ou le mode opératoire d'auteurs de cyberattaques en vertu de l'art. 76*a* LSI2[49]. L'accès à ces informations aide naturellement les autorités de poursuite pénale à exécuter leurs tâches.

L'obligation de signaler permet d'apporter une plus-value à la protection contre la cybercriminalité également dans la mesure où les exploitants d'infrastructures critiques ont droit au soutien de l'OFCS lorsqu'ils signalent une cyberattaque[50]. Il peut conseiller et soutenir les exploitants d'infrastructures critiques pour que ces derniers puissent limiter les dommages. L'on pourrait même se risquer à espérer que ce soutien passe par des recommandations en vue de prévenir de nouvelles cyberattaques, en tous cas similaires.

4. Les autres instruments réglementaires

La LSI n'est pas l'unique loi régissant des aspects de cybersécurité en Suisse. Certains secteurs se sont pourvus de bases légales pour imposer des exigences de cybersécurité à d'autres cercles de destinataires. À titre d'exemple, les fournisseurs de télécommunication sont maintenant soumis à certaines obligations de sécurité. Les art. 96*a* ss OST[51], concrétisant l'art. 48*a* LTC[52], imposent aux fournisseurs de télécommunication de prendre des mesures de sécurité pour lutter contre toute manipulation non autorisée d'installations de télécommunication. L'art. 96*a* al. 2 OST prévoit par exemple concrètement que les fournisseurs d'accès à Internet doivent lutter par des moyens techniques appropriés contre les attaques de déni de service distribué.

46 FF 2023 84, p. 44 s.
47 Art. 74*a* al. 4 LSI2 ; FF 2023 84, p. 33.
48 L'OFCS acquiert des informations sur la base des signalements obligatoires de cyberattaques comme sur la base des signalements d'autres cybermenaces (art. 73*b* LSI2).
49 FF 2023 84, p. 51.
50 Art. 74 al. 1, 74*a* al. 4 LSI2 ; FF 2023 84, p. 33.
51 Ordonnance du 1er avril 2007 sur les services de télécommunication (OST), RS 784.101.1.
52 Loi du 20 octobre 1997 sur les télécommunications (LTC), RS 784.10.

Un autre exemple est celui du sous-secteur critique de l'approvisionnement en électricité. Un nouvel art. 8*a* LApEl[53] est adopté dans le contexte de la nouvelle obligation de signaler les cyberattaques. Il imposera aux gestionnaires de réseau, aux producteurs et aux agents de stockage de prendre des mesures pour protéger adéquatement leurs installations contre les cybermenaces. Il en va particulièrement de mesures permettant de prévenir et de régler au plus vite les cyberincidents visant les installations concernées[54]. L'art. 8*a* LApEl sera concrétisé dans l'ordonnance, qui rendra contraignante la norme minimale pour la sécurité des TIC de l'OFAE[55].

C. La Loi fédérale sur la protection des données

Certaines réglementations n'ayant pas comme vocation « principale » à appréhender des considérations de cybersécurité présentes néanmoins un lien étroit avec ces dernières Il en va de la sorte pour les lois de protection des données personnelles, dont la LPD[56] au niveau fédéral.

La LPD consacre une importance particulière au principe de la sécurité des données[57]. C'est aussi une obligation pour le responsable du traitement et le sous-traitant de prendre des mesures techniques et organisationnelles pour assurer la sécurité des données (confidentialité, intégrité, disponibilité, traçabilité)[58]. Elles doivent être adaptées au risque pour la personne concernée et en tenant compte des possibilités et du coût des différentes mesures pouvant être mises en place[59].

Le but de la protection des données est d'assurer la protection de la personnalité en lien avec le traitement de ces données. La sécurité des données impose le cadre technique et organisationnel minimal dans lequel peuvent avoir lieu les traitements de données personnelles[60]. En évitant qu'elles ne soient accessibles à des personnes qui ne sont pas censées pouvoir les consulter, les lois de protection des données incitent les responsables du traitement et les sous-traitants

53 Loi du 15 juillet 2007 sur l'approvisionnement en électricité (LApEl), RS 734.7.
54 FF 2023 84, p. 56.
55 Rapport explicatif concernant l'avant-projet relatif à la révision de l'ordonnance sur l'approvisionnement en électricité, p. 1.
56 Loi fédérale du 25 septembre 2020 sur la protection des données (LPD), RS 235.1.
57 Voir art. 8 LPD.
58 Voir art. 2 Ordonnance du 31 août 2022 sur la protection des données (OPDo), RS 235.11 ; Ordonnance sur la protection des données (OPDo), Rapport explicatif, p. 23 ; CR LPD-FANTI/STAEGER, art. 8, N 11.
59 Ordonnance sur la protection des données (OPDo), Rapport explicatif, p. 21. Pour plus d'information à ce sujet, voir notamment CR LPD-FANTI/STAEGER, art. 8, N 87 ss ; MEYER/DAVIES, N 16 ss.
60 FF 2017 6565, p. 6650.

à protéger les données des individus. La mise en œuvre du principe de sécurité évite également que des tiers ne puissent les utiliser pour commettre des infractions, notamment des usurpations d'identité.

La LPD a introduit, lors de sa révision totale du 25 septembre 2020, l'obligation d'annoncer certaines violations de la sécurité des données à l'autorité nationale de surveillance (PFPDT) et aux personnes concernées[61]. Les personnes concernées doivent désormais être informées directement lorsque des données les concernant ont été exposées et qu'elles peuvent prendre des mesures utiles à leur protection. C'est notamment le cas si des identifiants et mots de passe ont par exemple été rendus accessibles. Dans une telle situation, les personnes concernées peuvent prendre des mesures pour se protéger en modifiant leurs mots de passe et leurs données d'accès[62]. Ainsi les personnes concernées peuvent prendre, conjointement aux responsables du traitement et aux sous-traitants, des mesures pour rendre la commission d'une infraction plus difficile[63].

La LPD contient également une obligation de protection des données dès la conception[64] et de protection des données par défaut[65]. Ces mesures techniques et organisationnelles ainsi que ces préréglages appropriés participent aussi à limiter les accès indus aux données, et sont donc une pierre à l'édifice de la cybersécurité.

D. L'éducation et la sensibilisation

En matière de cybersécurité, le point faible est tantôt l'infrastructure, tantôt l'être humain. Dans les cas d'attaques par rançongiciel par exemple, l'expérience a montré le plus souvent que soit l'infrastructure n'était pas suffisamment mise à jour (faille *zero day* par exemple) ou que des mesures élémentaires de protection manquaient (absence de double authentification ou mot de passe insuffisant par exemple), soit l'humain était le maillon faible et avait pu être piégé (en lui faisant par exemple croire qu'il était contacté par une autre personne que l'attaquant).

Pour anticiper les situations dans lesquelles l'être humain est exploitable par les délinquants, l'éducation et la sensibilisation sont cruciales. Elles doivent se faire à tous les échelons[66]. Des programmes doivent exister pour sensibiliser la

61 Art. 24 LPD.
62 FF 2017 6565, p. 6682.
63 Pour plus d'informations sur la nouvelle obligation d'annoncer les violations de la sécurité des données, voir CR LPD-MÉTILLE/MEYER, art. 24, N 28 ss.
64 Art. 7 al. 1 et 2 LPD.
65 Art. 7 al. 3 LPD.
66 Au sujet de l'objectif stratégique de la Suisse en la matière, voir Conseil fédéral, CSN, p. 15.

population en général quant aux mesures que tout individu peut mettre en place pour une utilisation sécurisée des moyens informatiques[67]. Les entreprises et les autorités doivent également sensibiliser leurs collaborateurs et peuvent par exemple mener des campagnes internes d'hameçonnage[68]. Il existe par ailleurs certaines exigences légales en rapport avec la formation des collaborateurs[69].

En améliorant la sensibilisation et l'éducation, il serait possible, avec des coûts assez limités, de rendre bien mieux informées les potentielles personnes lésées. Elles pourraient ensuite détecter plus efficacement les cas les plus évidents de cybercriminalité, et ainsi d'éviter de tomber dans un piège[70].

La sensibilisation et l'éducation sont susceptibles de couvrir une multitude de situations. Il ne faut effectivement pas se limiter aux risques financiers ou économiques liés aux cyberattaques pouvant être perpétrées sur les moyens informatiques d'une entreprise. L'éducation et la sensibilisation doivent aussi porter sur des sujets tels que les risques liés à la pornodivulgation, au surpartage parental (*sharenting)*, *etc*.

IV. Conclusion

Le droit pénal et la poursuite de la cybercriminalité sont indéniablement des instruments nécessaires pour la prévention générale de la cybercriminalité et pour la poursuite pénale des auteurs d'infraction. En revanche et comme nous avons pu le voir, le droit pénal ne suffit pas à lui seul pour empêcher la cybercriminalité. D'autres instruments légaux doivent être utilisés pour inciter les personnes susceptibles d'être lésées à mieux se protéger. Une meilleure protection permet de rendre la commission d'infractions plus difficile et moins attrayante pour les auteurs.

Le domaine juridique de la cybersécurité est récent en Suisse et est en plein développement. Certaines lois ont été adoptées ou révisées pour permettre d'inciter certaines organisations à mettre en place des mesures appropriées pour prévenir, détecter les cyberincidents (et donc les cyberattaques) ainsi qu'y réagir correctement. La LSI impose à ce titre un catalogue d'exigences à différents cercles d'assujettis. Alors que les autorités et organisations de la Confédération doivent mettre en place des mesures techniques et organisationnelles permettant d'assurer leur cyberrésilience, un cercle plus important d'infrastructures

67 Voir la campagne S-U-P-E-R du NCSC, disponible sous : <https://www.s-u-p-e-r.ch/fr/> (*consulté le 24.2.2024*).

68 NCSC, Rapport semestriel 2022/II, p. 7.

69 Voir art. 11 OSI qui impose aux unités administratives de la Confédération de former et de sensibiliser leurs collaborateurs à leur entrée en fonction et périodiquement.

70 NCSC, Rapport semestriel 2022/II, p. 7 s.

critiques est soumis à une obligation de signaler les cyberattaques. Des lois sectorielles se développent dans un esprit similaire à celui de la LSI, comme la LApEl qui imposera une obligation aux organisations actives dans l'approvisionnement en électricité d'assurer leur protection contre les cybermenaces.

D'autres lois prévoient des considérations connexes à la cybersécurité, comme la LPD. La sécurité des données personnelles est nécessaire pour qu'un responsable du traitement ou un sous-traitant garantissent la protection de la personnalité et des droits fondamentaux des personnes concernées. Par conséquent, elles doivent mettre en œuvre les mesures techniques et organisationnelles adaptées au besoin de protection de leurs traitements, aux risques et ainsi de suite.

Bien que certaines considérations de cybersécurité disposent d'un réel point d'ancrage dans la loi et que l'on assiste à des avancées législatives, la situation n'est pas totalement satisfaisante. La CSN de 2023 prévoit d'analyser en tout temps où des lacunes persistent et comment les combler, mais toujours selon une approche sectorielle[71]. On pourrait se demander si une autre approche, éventuellement avec des exigences minimales transversales, permettrait au moins aux organisations et infrastructures les plus importantes pour la Suisse d'être mieux protégées face à la cybercriminalité. Dans tous les cas, les efforts législatifs ne doivent pas se limiter au droit pénal.

Cela étant, le droit ne constitue qu'une partie de la réponse au besoin de cybersécurité. Parmi les mesures à prendre pour se protéger des cyberattaques, les infrastructures critiques, les entreprises, la population doivent être sensibilisées et formées. Comme cela, toutes les personnes potentiellement lésées par une infraction peuvent être plus amplement et clairement informées, ce qui leur permet d'éviter de tomber dans des pièges, de détecter des cybermenaces ainsi que de réagir en cas de cyberattaques de façon plus efficace.

V. Bibliographie

Doctrine

Daniel DZAMKO-LOCHER, Überlegungen zu Recht und Risiko bei behördlicher Cloudnutzung, L'informatique en nuage, Berne 2022 ; **Martin ECKERT/Noëlle GLAUS**, Das neue Informationssicherheitsgesetz (ISG), RR.COMP 3/2023, p. 12 ; **Rehana C. HARASGAMA/Jan KLEINER/Viviane BERGER**, Cyberangriffe beim Bund – Was gilt es aus rechtlicher Sicht zu beachten ?, Sécurité & Droit 1/2022, p. 40 ss (cité : HARASGAMA *et al.*) ; **José HURTADO POZO/Thierry GODEL**, Droit pénal général, 3e éd., Genève/Zurich/Bâle 2019 ; **Sandra HUSI-STÄMPFLI**, Informationssicherheits- und Datenschutzgesetz : Chance auf ein neues Zeitalter, Jusletter 25 septembre 2023 ; **Philippe MEIER/Sylvain MÉTILLE** (éds), Loi

[71] Conseil fédéral, CSN, p. 21.

fédérale sur la protection des données, Commentaire Romand, Bâle 2023 (cité : CR LPD-AUTEUR/E, art. X, N Y) ; **Pauline MEYER/Ryan DAVIES**, Portée pratique du caractère approprié des mesures de sécurité des données sous la LPD, Jusletter 25 septembre 2023 ; **Pauline MEYER/Sylvain MÉTILLE**, Loi fédérale sur la sécurité de l'information : version 2.0, Jusletter 5 septembre 2022 ; **Yves NICOLET/Jean-Philippe PEISSARD**, Cybercriminalité : difficultés et enjeux de la poursuite pénale, Criminalité économique et cybercriminalité – Mélanges en l'honneur de la professeure Isabelle Ausburger-Bucheli, p. 103 ss ; **Nicolas QUELOZ**, Droit pénal suisse, partie générale, 2e éd., Genève/Zurich/Bâle 2016 ; **Eugen ROESLE**, Meldung von Data B-reaches, RRCOMP 2/2022, p. 2 ss ; **Fabian TEICHMANN/ Léonard GERBER**, La qualification des attaques DDoS en droit suisse, Jusletter 27 septembre 2021.

Documents officiels

Centre national pour la cybersécurité (NCSC), Rapport semestriel 2021/1 du 2 novembre 2021 (cité: NCSC, Rapport semestriel 2021/1) ; **Centre national pour la cybersécurité (NCSC)**, Rapport semestriel 2022/I du 3 novembre 2022 (cité : NCSC, Rapport semestriel 2022/I) ; **Centre national pour la cybersécurité (NCSC)**, Rapport semestriel 2022/II du 11 mai 2023 (cité : NCSC, Rapport semestriel 2022/II) ; **Conseil fédéral**, Cyberstratégie (CSN), avril 2023 (cité : Conseil fédéral, CSN) ; **Conseil fédéral**, Message du 2 décembre 2022 relatif à la modification de la loi sur la sécurité de l'information (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), FF 2023 84 (cité : FF 2023 84) ; **Conseil fédéral**, Stratégie nationale de protection des infrastructures critiques du 16 juin 2023, Approche globale pour garantir l'approvisionnement en biens et prestations essentiels, FF 2023 1659 ; **Département fédéral de l'environnement, des transports, de l'énergie et de la communication**, Rapport explicatif du 21 septembre 2023 concernant l'avant-projet relatif à la révision de mai 2004 de l'ordonnance sur l'approvisionnement en électricité (protection contre les cybermenaces) (cité : Rapport explicatif concernant l'avant-projet relatif à la révision de l'ordonnance sur l'approvisionnement en électricité) ; **Global Cyber Security Capacity Centre**, Cybersecurity Capacity Review, Switzerland, juin 2020 (cité : Cybersecurity Capacity Review) ; **Office fédéral de la justice**, Ordonnance sur la protection des données (OPDo), Rapport explicatif du 31 août 2022 (cité : Ordonnance sur la protection des données (OPDo), Rapport explicatif) ; **Secrétariat général du DDPS (SG-DDPS)**, Législation d'exécution relative à la loi sur la sécurité de l'information, Explications du 8 novembre 2023 (cité : SG-DDPS, Législation d'exécution relative à la loi sur la sécurité de l'information, Explications) ; **Secrétariat général du DDPS**, Législation d'exécution relative à la loi sur la sécurité de l'information, Rapport explicatif du 24 août 2022 (cité : SG-DDPS, Législation d'exécution relative à la loi sur la sécurité de l'information, Rapport explicatif).