Le droit matériel suisse est-il conforme aux exigences minimales posées par la Convention du Conseil de l'Europe sur la cybercriminalité?

JÉRÉMIE MÜLLER*

Dans une société de plus en plus connectée à Internet et par conséquent de plus en plus dépendante de ce réseau, le législateur se doit de réagir très rapidement pour s'adapter aux nouvelles menaces et de doter ses autorités des moyens nécessaires pour combattre efficacement la cybercriminalité. Cette nouvelle forme de criminalité dont personne n'avait encore entendu parler il y a 30 ans de cela est devenue l'un des fléaux les plus importants de notre époque. Afin de coordonner la lutte contre la cybercriminalité sur le plan international, le Conseil de l'Europe a adopté une convention sur la cybercriminalité le 8 novembre 2001. Une analyse comparative du droit pénal matériel suisse montre cependant que, 14 ans plus tard, notre législation ne satisfait pas aux exigences minimales de cette convention et que des modifications profondes s'imposent de manière pressante.

In einer Gesellschaft, die zunehmend vernetzt ist und deshalb immer abhängiger wird, muss der Gesetzgeber sehr schnell reagieren, um sich an die neuen Bedrohungen anzupassen, und seine Behörden mit den erforderlichen Mitteln ausstatten, um die Computerkriminalität erfolgreich zu bekämpfen. Diese neue Form von Kriminalität, die vor 30 Jahren in der Allgemeinheit noch völlig unbekannt war, ist eine der schlimmsten Geisseln unserer Zeit. Um die Bekämpfung der Computerkriminalität auf internationaler Ebene zu koordinieren, hat der Europarat am 8. November 2001 ein Übereinkommen über Computerkriminalität verabschiedet. Eine Untersuchung des schweizerischen materiellen Strafrechts zeigt, dass unsere Gesetzgebung sogar 14 Jahre später die minimalen Voraussetzungen des Übereinkommens nicht erfüllt und tief greifende Veränderungen dringend notwendig sind.

I. Introduction

Il y a 26 ans, le CERN *(Centre européen de recherche nucléaire)* venait d'inventer le *world wide web*, mais seul quelques scientifiques connaissaient son existence. À cette époque-là, les gens envoyaient leur courrier par la poste, voire par fax. Ils rencontraient leurs amis au café ou à la maison. Ils faisaient leurs courses dans les magasins de la région et allaient payer leurs factures au guichet de la Poste.

En 2015, 3,2 milliards de personnes utilisaient Internet, soit 43,4% de la population mondiale[1]. Durant cette année, le taux d'utilisation d'Internet en Europe était de 77,6%.

* Docteur en droit, titulaire du brevet d'avocat, greffier au Ministère public central du canton de Vaud, Pully.
1 <www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx>.

Les gens s'écrivent désormais des *e-mails* ou des messages *Whatsapp*. Ils rencontrent leurs amis sur Facebook ou sur Twitter. Ils font leurs courses sur *Amazon* ou participent à des ventes aux enchères sur *eBay*. Ils font leur paiement par *e-banking*.

Cette tendance n'a évidemment pas échappé aux criminels qui se sont empressés d'exploiter ce moyen de communication à des fins malveillantes. Il va en effet sans dire que le commerce électronique génère d'importants transferts de fonds, ce qui ne manque pas d'attirer la convoitise de personnes, voire de groupes ou d'organisations, peu scrupuleuses qui rivalisent d'ingéniosité pour s'enrichir aux dépens d'utilisateurs inattentifs ou même naïfs.

Conscient du danger que représente la cybercriminalité et de son caractère transnational, le Conseil de l'Europe a établi une convention sur la cybercriminalité (CCC) dans le but de protéger la société de cette menace par une politique criminelle commune. Pour ce faire, il a été décidé d'harmoniser les éléments constitutifs des infractions informatiques en droit pénal national, de donner aux autorités de poursuite nationales les moyens nécessaires à l'instruction et à la poursuite de ces infractions informatiques, de même que d'autres infractions commises grâce à un système informatique et, enfin, de mettre en place un système de coopération internationale rapide et efficace.

En raison du caractère universel d'Internet, il était important que d'autres États, non-membres du Conseil de l'Europe, mais économiquement et technologiquement importants, soient Parties à cette convention. C'est dans ce but que les États-Unis d'Amérique, le Japon et l'Afrique du Sud ont pris part à l'élaboration de ce texte[2].

Le projet de convention a été adopté par le Comité des Ministres le 8 novembre 2001 et a été ouvert aux signatures le 23 novembre 2001. Ce texte est entré en vigueur le 1er juillet 2004, soit trois mois après que cinq États, dont au moins trois membres du Conseil de l'Europe, l'ont ratifié.

Bien que la Suisse ait signé la convention le 23 novembre 2001, près de 10 ans se sont écoulés avant que les deux Chambres du Parlement fédéral acceptent enfin de ratifier cette convention[3], le 18 mars 2011, et qu'elle entre en vigueur pour la Suisse le 1er janvier 2012.

En février 2016, 48 des 54 États signataires avaient ratifié la convention[4].

II. La convention article par article

1. Art. 1 CCC – Définitions

L'art. 1 de la convention définit les notions de *système informatique*, de *données informatiques*, de *fournisseur de services* et de *données relatives au trafic*, alors que le Code pénal suisse reste muet à ce sujet. Il est vrai que le Message du Conseil fédéral concernant la modification du Code pénal[5] donne quelques indications à propos des termes de *données* et de *système informatique* et qu'avec le temps cette lacune a progressivement été comblée par la doctrine. Il n'en demeure pas moins que, même si ces définitions ne doivent pas obligatoirement être reproduites dans le droit interne[6], il aurait été utile de les ancrer dans le Code pénal, afin d'apporter davantage de clarté au texte légal.

2. Art. 2 CCC – Accès illégal

Il y a accès illégal au sens de l'art. 2 CCC lorsqu'une personne accède intentionnellement et sans droit à tout ou partie d'un système informatique. Cette disposition correspond dans les grandes lignes à l'accès indu à un système informatique au sens de l'art. 143bis al. 1 CP. Cependant, malgré la récente reformulation de cet article[7], ainsi que la réserve émise par la Suisse s'agissant du droit de ne

[2] En février 2016, l'Allemagne, l'Autriche, l'Italie, la France, la Grande-Bretagne, les États-Unis d'Amérique et le Canada avaient ratifié la convention. En revanche, la Grèce, l'Irlande et la Suède l'avaient signée mais pas encore ratifiée. La Russie, bien que membre du Conseil de l'Europe n'a pas ratifié, ni même signé la convention (<conventions.coe.int/Treaty/Commun/ChercheSig.asp? NT=189&CM=8&DF=20/12/2011&CL= FRE>).

[3] Bulletin officiel du Conseil national 2011, 559; Bulletin officiel du Conseil des États 2011, 340; FF 2011, 2587 ss.

[4] <conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL =FRE>.

[5] RO 1994 2290 2309; FF 1991 II 933 (en particulier 951), Message concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991.

[6] Rapport explicatif de la Convention sur la cybercriminalité, n. 22 (peut être trouvé sous: <conventions.coe.int/Treaty/fr/Reports/Html/185.htm>).

[7] Modification entrée en vigueur le 1er janvier 2012 (RO 2011 6293; FF 2010, 4275).

poursuivre l'accès illégal que s'il a été commis en violation des mesures de sécurité, cette disposition ne satisfait pas à toutes les conditions posées par l'art. 2 CCC[8].

D'une part, l'art. 143bis al. 1 CP incrimine uniquement l'accès indu au système informatique d'autrui, alors que la convention protège l'intégrité de tous les systèmes informatiques. La notion de système informatique appartenant à autrui se rapporte nécessairement au droit d'accéder à ce système[9]. Cet élément n'est pas dénué d'importance dans la mesure où un système informatique peut être partagé par de nombreux utilisateurs. C'est notamment le cas dans les entreprises ou dans les familles. Dans l'hypothèse où un employé accéderait indûment au compte d'un collègue, il ne serait pas punissable puisqu'il a un droit d'accéder au système informatique[10]. Le terme *autrui* restreint donc exagérément le champ d'application de cette disposition et devrait donc être supprimé pour être conforme aux exigences de l'art. 2 CCC.

D'autre part, l'art. 143bis al. 1 CP exige que l'auteur se soit introduit dans le système informatique à l'aide d'un dispositif de transmission de données. Cela a pour conséquence que l'auteur qui profite de l'absence de sa victime pour entrer dans son bureau et s'introduire dans son ordinateur ne se rend pas coupable d'accès indu à un système informatique puisqu'il n'utilise pas un dispositif de transmission de données[11], alors que la convention prévoit clairement que ce type d'actes rentre dans le champ d'application de l'art. 2 CCC[12]. Cet élément constitutif devrait donc également être supprimé.

3. Art. 3 CCC – Interception illégale

L'art. 3 CCC réprime l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques.

Le droit suisse ne connaît pas de disposition équivalente. Bien que l'art. 143 CP – voire éventuellement l'art. 179novies CP – s'en rapproche, cette disposition devrait faire à tout le moins l'objet de trois modifications pour répondre aux exigences de l'art. 3 CCC.

S'agissant tout d'abord du champ d'application de l'art. 3 CCC, il s'étend non seulement aux transmissions non publiques, mais également aux émissions électromagnétiques. Or, tel n'est pas le cas de l'art. 143 al. 1 CP qui ne comprend que les données enregistrées ou transmises électroniquement ou selon un mode similaire. Le champ d'application de l'art. 143 al. 1 CP devrait donc être étendu aux émissions électromagnétiques[13].

Il sied ensuite de relever que les biens juridiques protégés par les art. 143 al. 1 CP et 3 CCC sont différents puisque le premier garantit le droit du bénéficiaire légitime des données d'en disposer librement et conformément à sa volonté[14], alors que le second protège le droit au respect des données transmises – c'est-à-dire leur confidentialité – en application de l'art. 8 CEDH[15]. Pour se conformer aux exigences de la Convention sur la cybercriminalité, la solution la plus simple consisterait donc à créer une nouvelle norme, bien qu'il soit également possible d'étendre la protection conférée par l'art. 143 CP à la confidentialité des données transmises électroniquement.

---

[8] Contra: P. WEISSENBERGER, Basler Kommentar, Strafrecht II, 3e éd., Bâle 2013, CP 143bis N 3.
[9] B. CORBOZ, Les infractions en droit suisse, 3e éd., Berne 2010, CP 143bis N 2; A. DONATSCH, Strafrecht III, Delikte gegen den Einzelnen, 10e éd., Zurich 2013, 200; G. STRATENWERTH/G. JENNY/F. BOMMER, Schweizerisches Strafrecht, Besonderer Teil I, 7e éd., Berne 2010, § 14 n. 39; S. TRECHSEL, Schweizerisches Strafgesetzbuch, Praxiskommentar, 2e éd., Zurich 2012, CP 143bis N 4; WEISSENBERGER (n. 8), CP 143bis N 11 s.
[10] N. SCHMID, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994, § 5 n. 17.
[11] FF 1991 II 979.
[12] Rapport explicatif de la Convention sur la cybercriminalité, n. 46 et 50.
[13] C. SCHWARZENEGGER, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, in: Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zurich 2002, 321; J. TRECCANI, Interceptions électroniques, in: Plus de sécurité, moins de liberté, les techniques d'investigation et de preuve en question, Zurich 2003, 233.
[14] FF 1991 II 977; SCHMID (n. 10), § 4 n. 14 ss; TRECHSEL (n. 9), CP 143 N 2.
[15] Rapport explicatif de la Convention sur la cybercriminalité, n. 51.

Enfin, les données transmises ne sont, la plupart du temps, pas protégées, ce qui a pour conséquence que l'art. 143 CP est inapplicable[16], alors que l'art. 3 CCC exige que les données non protégées bénéficient également de la protection de la loi pénale[17].

4. Art. 4 CCC – Atteinte à l'intégrité des données

L'atteinte à l'intégrité des données au sens de l'art. 4 CCC consiste à endommager, effacer, détériorer, altérer ou supprimer des données informatiques intentionnellement et sans droit. Les États Parties peuvent se réserver le droit d'exiger que ces comportements entraînent des dommages sérieux, ce que la Suisse a cependant renoncé à faire.

La disposition de droit suisse qui se rapproche le plus de l'art. 4 CCC est l'art. 144bis ch. 1 al. 1 CP. Même si les biens juridiques protégés par l'art. 4 CCC, à savoir l'intégrité et le bon fonctionnement ou le bon usage de données ou de programmes informatiques enregistrés, ne sont pas parfaitement identiques à celui de l'art. 144bis ch. 1 al. 1 CP, soit le droit de disposer de données (intactes)[18], il n'en demeure pas moins qu'ils se rejoignent. Il n'y a donc pas de modification à envisager de ce point de vue-là.

En ce qui concerne les comportements réprimés par l'art. 4 CCC, on constate qu'ils ont tous leur équivalent en droit suisse (art. 144bis ch. 1 al. 1 CP). Les notions d'*endommagement* et de *détérioration*, qui impliquent une altération négative de l'intégrité ou du contenu informatif de données et de programmes[19], sont couvertes par le terme *modifie*[20]. L'*effacement* est repris tel quel en droit suisse. L'*altération*, c'est-à-dire la modification de données existantes[21], est couverte par le terme *modifie*[22]. Quant à la *suppression* de données, qui signifie qu'elles ne sont pas ou plus accessibles à la personne ayant accès à l'ordinateur ou au support sur lequel les données étaient stockées[23], elle est reprise par la notion de *mise hors d'usage*[24]. Sous cet angle également le droit suisse ne prête donc pas le flanc à la critique.

5. Art. 5 CCC – Atteinte à l'intégrité du système

L'art. 5 CCC réprime l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Contrairement à l'opinion défendue par les auteurs du rapport explicatif de l'avant-projet d'Arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité de 2009, selon laquelle l'art. 144bis ch. 1 al. 1 CP incriminerait les comportements réprimés par l'art. 5 CCC[25], force est de constater qu'il n'existe en réalité aucun équivalent à cette disposition en droit suisse[26].

Le premier problème se pose déjà au stade de la comparaison des biens juridiques protégés par ces deux normes. Ils sont à ce point différents que cette seule dissemblance suffit à justifier la création d'une norme distincte. En effet, l'art. 5 CCC protège l'intérêt des exploitants et des usagers d'un sys-

[16] SCHWARZENEGGER (n. 13), 320, TRECCANI (n. 13), 218 ss .
[17] SCHWARZENEGGER (n. 13), 320.
[18] SCHMID (n. 10), § 6 n. 14; STRATENWERTH/ JENNY/BOMMER (n. 9), § 14 n. 59; TRECHSEL (n. 9), CP 144bis N 2; WEISSENBERGER (n. 8), CP 144bis N 6.
[19] Rapport explicatif de la Convention sur la cybercriminalité, n. 61.
[20] CORBOZ (n. 9), CP 144bis N 5; SCHMID (n. 10), § 6 n. 26; STRATENWERTH/JENNY/BOMMER (n. 9), § 14 n. 60; TRECHSEL (n. 9), CP 144bis N 5; WEISSENBERGER (n. 8), CP 144bis N 21 s.
[21] Rapport explicatif de la Convention sur la cybercriminalité, n. 61.
[22] CORBOZ (n. 9), CP 144bis N 5; SCHMID (n. 10), § 6 n. 26; STRATENWERTH/JENNY/BOMMER (n. 9), § 14 n. 60; TRECHSEL (n. 9), CP 144bis N 5; WEISSENBERGER (n. 8), CP 144bis N 21 s.
[23] Rapport explicatif de la Convention sur la cybercriminalité, n. 61.
[24] CORBOZ (n. 9), CP 144bis N 5; DONATSCH (n. 9), 212; SCHMID (n. 10), § 6 n. 29; STRATENWERTH/JENNY/BOMMER (n. 9), § 14 n. 60; TRECHSEL (n. 9), CP 144bis N 7.
[25] <www.admin.ch/ch/f/gg/pc/documents/1722/Vorlage_Bericht.pdf>.
[26] Contra: WEISSENBERGER (n. 8), CP 144bis N 5.

tème informatique ou d'un système de télécommunications à ce que celui-ci soit en mesure de fonctionner correctement[27], alors que l'art. 144bis ch. 1 al. 1 CP assure un droit de disposition sur des données[28].

S'agissant ensuite des comportements réprimés par l'art. 5 CCC, le rapport explicatif du Conseil de l'Europe mentionne qu'il y a notamment entrave grave en cas d'*envoi à un système informatique de données dont la forme, le volume ou la fréquence porte un préjudice important à la capacité du propriétaire ou de l'exploitant d'utiliser le système en question ou de communiquer avec d'autres systèmes*[29]. Or, bon nombre de ces comportements ne sont pas punissables en vertu de l'art. 144bis ch. 1 al. 1 CP, car cette disposition ne vise que les cas de modification ou d'altération de données, le législateur ayant volontairement renoncé à incriminer d'autres formes de sabotage informatique[30]. L'atteinte qui peut être portée à l'intégrité d'un système informatique, notamment par l'*e-bombing*, le *spamming* ou encore une attaque de type déni de service distribué (attaque DDoS) ne tombe donc pas sous le coup de l'art. 144bis ch. 1 CP[31].

Compte tenu de ces éléments, il est indispensable qu'un nouvel article réprimant l'atteinte à l'intégrité des systèmes informatiques soit créé pour rendre le droit matériel suisse conforme aux exigences de la convention.

6. Art. 6 CCC – Abus de dispositifs

L'abus de dispositifs au sens de l'art. 6 CCC se caractérise par la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'outils de piratage tels que des codes d'accès ou des programmes permettant de commettre une des infractions réprimées par les art. 2 à 5 CCC.

Les États Parties peuvent se réserver le droit de ne pas appliquer l'art. 6 § 1 CCC, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés à l'art. 6 § 1 let. a ch. ii CCC, faculté que la Suisse a utilisé.

Malgré cette réserve, le droit suisse n'est pas entièrement conforme aux exigences minimales posées par la convention[32]. L'art. 6 § 1 CCC exige en effet que l'auteur agisse avec l'intention de faire utiliser les éléments qu'il fournit par des tiers, dans le but de commettre l'une ou l'autre des infractions visées par les art. 2 à 5 CCC. Or, seuls les art. 143bis et 144bis CP – correspondant respectivement aux art. 2 et 4 CCC – répriment cette forme d'actes préparatoires (art. 143bis al. 2 et 144bis ch. 2 CP). Quant à la remise d'éléments destinés à commettre une interception illégale (art. 3 CCC) ou une atteinte à l'intégrité du système (art. 5 CCC), elle n'est tout simplement pas punissable en droit suisse puisque l'art. 143 CP reste muet sur cette question et que comme indiqué ci-dessus, il n'existe aucune norme réprimant l'atteinte à l'intégrité du système.

Plutôt que d'ajouter un second alinéa à chaque article topique – ce qui a l'inconvénient d'alourdir inutilement le texte légal – une solution consisterait à créer un nouvel article s'appliquant à toutes les infractions informatiques, comme le sont en comparaison l'art. 172ter CP avec les infractions contre le patrimoine ou l'art. 200 CP avec les infractions contre l'intégrité sexuelle.

7. Art. 7 CCC – Falsification informatique

L'art. 7 CCC réprime l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles.

Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée. La Suisse a fait usage de cette possibilité pour n'appliquer l'art. 7

[27] Rapport explicatif de la Convention sur la cybercriminalité, n. 65.
[28] SCHMID (n. 10), § 6 n. 14; STRATENWERTH/ JENNY/BOMMER (n. 9), § 14 n. 59; TRECHSEL (n. 9), CP 144bis N 2; WEISSENBERGER (n. 8), CP 144bis N 6.
[29] Rapport explicatif de la Convention sur la cybercriminalité, n. 67.
[30] FF 1991 II 982 s.; SCHMID (n. 10), 1994, § 6 n. 15; C. SCHWARZENEGGER, E-Commerce – Die Strafrechtliche Dimension, in: O. Arter/F.S. Jörg (éds), Internet-Recht und Electronic Commerce Law, 1re éd., Lachen 2001, 366 s.
[31] L. MOREILLON, Nouveaux délits informatiques sur Internet, medialex 2001, 22 ss.
[32] WEISSENBERGER (n. 8), CP 144bis N 6.

CCC que dans la mesure où l'infraction est commise dans le dessein de se procurer ou de procurer à un tiers un avantage ou de causer un dommage.

Les intérêts juridiquement protégés par cette norme sont la sécurité et la fiabilité des données électroniques qui peuvent avoir des conséquences pour les relations juridiques[33]. En droit suisse, ce bien juridique est protégé par le faux dans les titres (art. 251 CP) qui a été étendu aux titres informatiques (art. 110 al. 4 CP) depuis le 1er janvier 1995[34]. Le droit suisse est donc conforme aux exigences de l'art. 7 CCC.

8. Art. 8 CCC – Fraude informatique

La fraude informatique au sens de l'art. 8 CCC sanctionne le fait de causer un préjudice patrimonial à autrui par toute introduction, altération, effacement ou suppression de données informatiques, mais également par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui. Cet article réprime donc toute manipulation abusive au cours d'un traitement de données en vue d'effectuer un transfert illicite de propriété[35].

En droit suisse, cette disposition figure à l'art. 147 al. 1 CP. Les notions d'*introduction*, d'*altération*, d'*effacement* ou de *suppression* de données informatiques sont comprises dans les termes *utilisation incorrecte* et *utilisation incomplète*[36]. Les autres formes d'atteinte au fonctionnement d'un système informatique (art. 8 let. b CCC) sont quant à elles englobées dans la formulation *en recourant à un procédé analogue*[37]. Le droit suisse est donc conforme aux exigences de l'art. 8 CCC[38].

9. Art. 9 CCC – Infractions se rapportant à la pornographie enfantine

L'art. 9 § 1 CCC réprime une série de comportements, tels que la production en vue de sa diffusion, l'offre, la mise à disposition, la diffusion, la transmission, la possession de matériel de pornographie enfantine, commis par le biais d'un système informatique. Aux termes de la convention, la notion de pornographie enfantine s'entend de représentations visuelles de mineurs – ou de personnes se faisant passer pour tels – se livrant à un comportement sexuellement explicite et d'images réalistes représentant des mineurs se livrant à un comportement sexuellement explicite (art. 9 § 2 CCC).

L'art. 197 CP a récemment été modifié[39] pour correspondre aux exigences de la Convention de Lanzarote. Que ce soit dans son ancienne ou dans sa nouvelle teneur, la liste des comportements réprimés par l'art. 197 CP est plus large que celle figurant à l'art. 9 § 1 CCC, puisqu'elle mentionne encore l'importation, la prise en dépôt, la promotion, l'exposition, l'acquisition ou l'obtention par voie électronique de pornographie enfantine.

S'agissant de la notion de mineur, l'art. 9 § 3 CCC la définit comme toute personne de moins de 18 ans. Une Partie peut toutefois fixer une limite d'âge inférieure à 18 ans, ce que la Suisse a fait en limitant l'âge d'un mineur à 16 ans. Le but de cette réserve était de faire correspondre l'âge fixé à l'art. 197 ch. 3 et 3bis aCP[40] aux exigences de la convention. Depuis le 1er juillet 2014, l'art. 197 al. 4 et 5 CP ne mentionne plus la notion d'*enfants*, mais celle de *mineurs*[41], si bien que la réserve émise par la Suisse a perdu une grande partie de son utilité. La seule situation pour laquelle cette réserve a encore du sens est celle visée par l'art. 197 al. 8 CP, à savoir si un mineur âgé de 16 ans ou plus produit, possède ou consomme, avec le consentement d'un autre mineur âgé de 16 ans ou plus, des objets ou des représentations au sens de l'art. 197 al. 1 CP qui les impliquent.

Aux termes de l'art. 9 § 4 CCC, une Partie peut également se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1 let. d et e, et 2 let. b et c de l'art. 9 CCC. La Suisse a aussi utilisé

[33] Rapport explicatif de la Convention sur la cybercriminalité, n. 81.
[34] FF 1991 II 956 ss.
[35] Rapport explicatif de la Convention sur la cybercriminalité, n. 86.
[36] CORBOZ (n. 9), CP 147 N 4 s.; DONATSCH (n. 9), 249; SCHMID (n. 10), § 7 n. 45 ss; STRATENWERTH/JENNY/BOMMER (n. 9), § 16 n. 6; TRECHSEL (n. 9), CP 147 N 4 s.; G. FIOLKA, Basler Kommentar, Strafrecht II, 3e éd., Bâle 2013, CP 147 N 9 s.
[37] CORBOZ (n. 9), CP 147 N 7; DONATSCH (n. 9), 250; SCHMID (n. 10), § 7 n. 77; STRATENWERTH/JENNY/BOMMER (n. 9), § 16 n. 9; TRECHSEL (n. 9), CP 147 N 7; FIOLKA (n. 36), CP 147 N 18.
[38] FIOLKA (n. 36), CP 147 N 1.
[39] Nouvelle teneur depuis le 1er juillet 2014 (FF 2012, 7051; RO 2014, 1159).
[40] CORBOZ (n. 9), CP 197 N 57; DONATSCH (n. 9), 550. Autre opinion: K. MENG, Basler Kommentar, Strafrecht II, 3e éd., Bâle 2013, CP 197 N 23.
[41] FF 2012, 7095.

cette possibilité pour ne pas appliquer l'art. 9 § 2 let. b CCC, soit la répression de représentations visuelles mettant en scène une personne majeure qui apparaît comme un mineur se livrant à un comportement sexuellement explicite. Émettre une telle réserve était de peu d'utilité, puisque l'art. 197 CP, que ce soit dans son ancienne ou dans sa nouvelle formulation, permet de réprimer ce type de représentation[42].

La Suisse a en revanche, à juste titre, renoncé à faire usage de la possibilité de ne pas appliquer l'art. 9 § 2 let. c CCC concernant les images réalistes représentant un mineur se livrant à un comportement sexuellement explicite (p. ex. comics ou mangas), puisque l'art. 197 al. 4 et 5 CP (anciennement art. 197 ch. 3 et 3bis CP) englobe ce type de représentations[43].

10. Art. 10 CCC – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

L'art. 10 § 1 CCC érige en infraction les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

La Suisse a ratifié toutes ces conventions et a modifié son droit interne dans ce sens. Le droit suisse est donc conforme aux exigences de la convention.

L'art. 10 § 2 CCC réprime les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

La Suisse a ratifié toutes ces conventions et a adapté son droit interne en conséquence. Sous cet angle également le droit suisse est conforme aux exigences de la convention.

11. Art. 11 CCC – Tentative et complicité

L'art. 11 CCC impose aux États Parties de réprimer toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des art. 2 à 10 CCC. Il exige également de sanctionner pénalement toute tentative intentionnelle de commettre l'une des infractions établies en application des art. 3 à 5, 7, 8, 9 ch. 1 let. a et c CCC.

Les normes suisses actuelles qui correspondent aux art. 2 à 10 CCC sanctionnent toutes au moins des délits. Partant, les art. 22, 23 et 25 CP, qui traitent des différentes formes de tentatives et de la complicité, leur sont applicables sans aucune restriction. Pour autant que les nouvelles dispositions qui devraient être créées[44] constituent également – à tout le moins – des délits, le droit suisse serait conforme à l'art. 11 CCC.

12. Art. 12 CCC – Responsabilité des personnes morales

L'art. 12 § 1 CCC impose aux États Parties d'adopter toutes les mesures nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé sur un pouvoir de représentation de la personne morale,

[42] Du même avis concernant l'ancienne formulation de l'art. 197 CP: MENG (n. 40), CP 197 N 22; L.-A. TIRELLI, La répression pénale des consommateurs de pédopornographie à l'heure d'Internet, Genève 2008. D'un autre avis: STRATENWERTH/JENNY/BOMMER (n. 9), § 10 n. 6.

[43] CORBOZ (n. 9), CP 197 N 57; DONATSCH (n. 9), 516; STRATENWERTH/JENNY/BOMMER (n. 9), § 10 n. 7; MENG (n. 40), CP 197 N 37 .

[44] Cf. remarques formulées au sujet des dispositions précédentes.

sur une autorité pour prendre des décisions au nom de la personne morale ou sur une autorité pour exercer un contrôle au sein de la personne morale.

L'art. 12 § 2 CCC prévoit en outre que chaque Partie adopte les mesures nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée à l'art. 12 § 1 CCC a rendu possible la commission d'une infraction figurant aux art. 2 à 10 CCC pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

Le droit pénal suisse ne connaît que deux règles concernant la responsabilité pénale des personnes morales, à savoir les alinéas 1 et 2 de l'art. 102 CP.

Aux termes de l'art. 102 al. 1 CP, un crime ou un délit qui est commis au sein d'une entreprise dans l'exercice d'activités commerciales conformes à ses buts est imputé à l'entreprise s'il ne peut être imputé à aucune personne physique déterminée en raison du manque d'organisation de l'entreprise.

Cette disposition ne répond pas aux exigences minimales de la convention pour trois raisons. D'abord, elle prévoit une responsabilité pénale subsidiaire de l'entreprise[45], alors que la convention exige une responsabilité primaire. Ensuite, la responsabilité de l'entreprise ne peut être engagée que si l'on n'arrive pas à déterminer, en raison d'un manque d'organisation, quelle personne physique au sein de la personne morale a commis l'infraction[46], alors que la convention ne limite pas la responsabilité de l'entreprise à ce seul motif. Enfin, même si ces deux premières conditions sont réalisées, la loi exige encore que l'infraction ait été commise dans le cadre des activités commerciales et conformément aux buts de la personne morale[47], restrictions qui n'existent pas dans la convention.

L'art. 102 al. 2 CP, quant à lui, crée une responsabilité primaire de la personne morale pour certaines infractions particulières s'il doit lui être reproché de ne pas avoir pris toutes les mesures d'organisation raisonnables et nécessaires pour empêcher la commission d'une telle infraction[48].

Cette disposition n'est pas non plus conforme à la convention pour deux raisons. D'une part, les infractions informatiques ne font pas partie du catalogue d'infractions auxquelles l'art. 102 al. 2 CP est susceptible de s'appliquer. D'autre part, il faut que l'insuffisance de mesures d'organisation puisse être reprochée à la personne morale, ce qui restreint beaucoup trop le champ d'application de cette norme.

Force est ainsi de constater que sur ce point également le droit pénal suisse n'est pas conforme aux exigences minimales posées par la convention. L'art. 12 § 3 CCC autorise certes les États Parties à instituer une responsabilité de la personne morale qui soit administrative ou civile plutôt que pénale pour atteindre les but fixés par la convention, on peine cependant à déceler quelle disposition de l'ordre juridique suisse permettrait d'atteindre ces buts.

En conséquence, pour être conforme à la convention, le droit suisse devrait subir plusieurs modifications. D'une part, pour répondre aux exigences posées par l'art. 12 § 1 CCC, il devrait s'enrichir d'une nouvelle norme instituant une responsabilité pénale des personnes morales lorsqu'une personne physique mentionnée à l'art. 12 § 1 CCC a commis, pour le compte de la personne morale, une infraction correspondant aux comportements réprimés par les art. 2 à 10 CCC. D'autre part, pour satisfaire aux conditions de l'art. 12 § 2 CCC, il conviendrait de créer une seconde norme instituant une responsabilité pénale des personnes morales lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée à l'art. 12 § 1 CCC a rendu possible la commission d'une infraction réprimée par les art. 2 à 11 CCC pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

---

[45] M. DUPUIS/B. GELLER/G. MONNIER/ L. MOREILLON/C. PIGUET/C. BETTEX/ D. STOLL, Code pénal, Petit commentaire, 2012, CP 102 N 14 ss; M. A. NIGGLI/D. GFELLER, Basler Kommentar, Strafrecht II, 3e éd., Bâle 2013, CP 102 N 52; TRECHSEL (n. 9), CP 102 N 15.

[46] DUPUIS/GELLER/MONNIER/MOREILLON/PIGUET/BETTEX/STOLL (n. 45), CP 102 N 17 ss; NIGGLI/GFELLER (n. 44), CP 102 N 64 et 107; TRECHSEL (n. 9), CP 102 N 14.

[47] DUPUIS/GELLER/MONNIER/MOREILLON/PIGUET/BETTEX/STOLL (n. 45), CP 102 N 13; NIGGLI/GFELLER (n. 44), CP 102 N 78 ss et 91 ss; TRECHSEL (n. 9), CP 102 N 10.

[48] DUPUIS/GELLER/MONNIER/MOREILLON/PIGUET/BETTEX/STOLL (n. 45), CP 102 N 19 ss; NIGGLI/GFELLER (n. 44), CP 102 N 242 ss; TRECHSEL (n. 9), CP 102 N 19.

13. Art. 13 CCC – Sanctions et mesures

Aux termes de l'art. 13 CCC, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des art. 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

Cette disposition oblige également les Parties à sanctionner, pénalement ou non, les personnes morales tenues pour responsables en application de l'art. 12 CCC, de manière effective, proportionnée et dissuasive, ce qui implique des sanctions pécuniaires.

Pour autant qu'il soit modifié dans le sens proposé ci-dessus, le droit pénal suisse serait conforme à ces exigences.

III. Conclusion

À ce jour, le droit suisse est loin de satisfaire aux exigences de la Convention sur la cybercriminalité. Les dispositions actuelles du droit de fond ont été imaginées par des experts il y a plus de 30 ans et sont entrées en vigueur il y a 21 ans. Or, déjà à l'époque ces dispositions relevaient davantage du rapiéçage normatif que d'une véritable systématique législative destinée à combattre efficacement la criminalité informatique. À cela s'ajoute que, les années passant, l'informatique – et la cybercriminalité avec elle – a subi de telles transformations que ces normes, hier inadaptées, sont devenues aujourd'hui inutilisables puisqu'elles ne correspondent plus aux activités criminelles actuelles.

Dans un monde dans lequel les technologies se développent extrêmement rapidement, la Suisse ne peut pas se permettre de prendre du retard, faute de quoi elle deviendrait un paradis pour les cybercriminels du monde entier. Elle doit donc au plus vite adapter son droit de fond.

Au vu des différentes corrections nécessaires, il serait souhaitable de regrouper les infractions informatiques par exemple dans un nouveau titre 3bis intitulé «Infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques», voire même en faire une loi spéciale séparée.

Il y a une vingtaine d'années, les principaux auteurs d'infractions informatiques étaient des informaticiens qui agissaient essentiellement pour relever de nouveaux défis. Avec le temps, la criminalité organisée a toutefois également commencé à s'intéresser de plus près à ce type d'infractions en raison de l'important potentiel lucratif que ces agissements pouvaient procurer. Le temps a d'ailleurs montré à quel point ce domaine est intéressant, puisque la cybercriminalité est devenue pour la première fois en 2011 l'activité criminelle la plus rentable au monde, devant la vente d'armes au noir et le trafic de drogue[49].

Un autre phénomène important est celui de la professionnalisation de ce genre d'activités. Les cybercriminels se répartissent les tâches et se perfectionnent dans leur branche, ce qui permet d'augmenter l'ampleur de l'activité criminelle et donc des gains.

Pour ces raisons, il est indispensable de prévoir des formes qualifiées pour chaque infraction, lorsque l'activité criminelle revêt une certaine ampleur, que l'auteur agit par métier ou lorsqu'il agit en qualité d'affilié à une bande.

Résumé

À l'heure actuelle, le droit suisse ne satisfait pas aux exigences minimales de la Convention sur la cybercriminalité. Pire encore, il est totalement inadapté au monde virtuel qui nous entoure. Pour pouvoir lutter efficacement contre la cybercriminalité qui, à n'en pas douter, va continuer à évoluer et à se propager à tous les domaines liés à l'informatique, il est indispensable que le législateur modifie rapidement et en profondeur notre droit.

[49] <www.zdnet.com/blog/btl/cybercrime-costs- 338bn-to-global-economy-more-lucrative-than-drugs-trade/57503>.

Zusammenfassung

Zurzeit erfüllt das schweizerische Recht die Mindestvoraussetzungen des Übereinkommens über Computerkriminalität nicht. Schlimmer noch, es ist der virtuellen Welt, die uns umgibt, völlig unangemessen. Damit die Computerkriminalität, die sich zweifellos entwickeln und sich in allen Bereichen mit Bezug zur Informatik verbreiten wird, wirksam bekämpft werden kann, muss der Gesetzgeber unbedingt unser Recht schnell und tief greifend ändern.