



COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

COMMENTAIRE

Art. 2 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jérémie Müller
Edité par Damian K. Graf

État du traitement : 17.02.2024

PDF créé le : 06.10.2026

DOI: 10.17176/20240217-132351-0

PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 2 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 2 CCC N. XXX.

Chapitre II: Mesures à prendre au niveau national

Section 1: Droit pénal matériel

Titre 1: Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Art. 2 Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

TABLE DES MATIÈRES

I. Généralités	3
II. Bien Juridiquement protégé	3
III. Éléments constitutifs fondamentaux	4
A. Un système informatique	4
B. Un accès au système informatique	4
C. L'illicéité	5
D. L'intention	6
IV. Éléments constitutifs supplémentaires facultatifs	6
A. Accès en violation des mesures de sécurité	6
B. Le dessein d'obtenir des données informatiques ou un autre dessein spécial	7
C. Un système informatique connecté à un autre système informatique	9
V. Comparaison avec le droit suisse	9
Bibliographie	10
Travaux législatifs	11

I. GÉNÉRALITÉS

- 1 L'accès illégal à un système informatique constitue l'**infraction de base** dans le domaine de la cybercriminalité. Il s'agit souvent du comportement délictueux préalable nécessaire à la commission d'une autre infraction informatique, telle que l'atteinte à l'intégrité de données (art. 4 CCC), l'atteinte à l'intégrité du système (art. 5 CCC), la falsification informatique (art. 7 CCC) ou la fraude informatique (art. 8 CCC). Toutefois, certains cybercriminels se contentent d'accéder sans droit à un système informatique, par bravade ou pour le seul défi technique que cela représente, sans commettre d'infraction subséquente. Il est donc justifié d'ériger en infraction ce comportement en tant que tel, plutôt qu'il soit absorbé par les infractions réprimées par les articles suivants. Ainsi, l'auteur se rend coupable d'accès illégal du seul fait qu'il se fraie un accès vers un système informatique. Il n'est pas nécessaire qu'il vole ou modifie des données dans le système informatique.
- 2 D'aucuns pourraient voir dans le *hacking* une activité ludique, relativement inoffensive, à laquelle s'adonnent quelques *geeks* en quête de nouveaux défis. La réalité est toutefois tout autre. Ce comportement est bien plus **répandu** qu'on pourrait le croire au premier abord et ses auteurs poursuivent des buts bien moins honorables que le simple divertissement.
- 3 Naturellement, la mise en place de mesures de sécurité fortes est le moyen le plus efficace pour protéger un système informatique contre des accès non-autorisés. Compte tenu de la menace ou de l'atteinte à la sécurité des systèmes et des données informatiques que le *hacking* représente, les mesures techniques doivent être accompagnées de **mesures législatives** destinées à dissuader les cybercriminels de passer à l'acte ou à les sanctionner en cas de commission d'actes malveillants¹. De cette manière, l'intérêt des organisations et des particuliers à pouvoir diriger, exploiter et contrôler leurs systèmes informatiques sans perturbation ni entrave d'aucune sorte est protégé au mieux².

II. BIEN JURIDIQUEMENT PROTÉGÉ

- 4 L'art. 2 CCC protège l'**inviolabilité** des systèmes informatiques. Cette protection par le droit pénal s'impose pour au moins deux raisons.
- 5 D'une part, l'accès illégal à un système informatique peut engendrer des **coûts** de remise en état importants chez l'ayant-droit. Les auteurs modifient en effet souvent des données pour s'introduire à l'intérieur du système. De plus, les victimes ne se rendent souvent compte de l'intrusion que quelque temps après qu'elle a eu lieu. Il est dès lors particulièrement difficile de retrouver ce qui a été modifié par les auteurs, ainsi que les nouvelles données générées par le système informatique à la suite de cette modification. Une fois identifiées, ces données doivent être remises dans leur état d'origine. Ces opérations peuvent nécessiter beaucoup de temps travail et peuvent donc être très onéreuses³.
- 6 D'autre part, l'accès illégal permet aux auteurs de **consulter** des informations auxquelles ils ne devraient pas avoir accès (p. ex. rapports confidentiels, secrets commerciaux, listes de clients, pièces comptables, numéros de carte de crédit, données personnelles, ...). Ces informations peuvent ensuite être revendues au marché noir, ce qui peut engendrer un dommage encore bien plus important pour l'ayant-droit que la seule remise en état de la protection du système⁴.

1. Rapport explicatif de la Convention sur la cybercriminalité, n. 45.

2. Rapport explicatif de la Convention sur la cybercriminalité, n. 44.

3. Rapport explicatif de la Convention sur la cybercriminalité, n. 44.

4. Rapport explicatif de la Convention sur la cybercriminalité, n. 44.

III. ÉLÉMENTS CONSTITUTIFS FONDAMENTAUX

A. Un système informatique

- 7 Aux termes de l'art. 1 let. a CCC, « l'expression "système informatique" désigne tout **dispositif** isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ». La notion de système informatique comprend ainsi l'ensemble des hardwares (carte mère, processeur, disque dur, écran, clavier, imprimante, ...) et des softwares (BIOS, système d'exploitation, logiciels, mises à jour, ...), ainsi que les dispositifs qui permettent la connexion de ces différents éléments les uns aux autres (câbles, routeur, borne wifi, ...).
- 8 Pour davantage de détails au sujet de cette notion, il est renvoyé à ce qui a été écrit à l'art. 1 CCC ci-dessus.

B. Un accès au système informatique

- 9 On pourrait être tenté de comparer l'accès illégal à un système informatique à l'infraction de violation de domicile. L'accès au système informatique serait ainsi l'équivalent numérique de l'introduction dans le logement. Cette **analogie** a ceci de rassurant que l'on peut très bien se représenter intellectuellement la situation. Le monde virtuel est toutefois plus complexe que cela et les contours des notions juridiques nécessairement plus flous.
- 10 Il est compliqué de faire une analogie avec le monde réel. S'il fallait néanmoins en faire une, l'accès à un système informatique pourrait être comparé au fait d'entrer dans un **château-fort** du Moyen-Âge. L'accès au château est limité par un mur d'enceinte et des douves. La porte d'entrée principale est généralement surveillée par des gardes. Ceux-ci contrôlent que les personnes qui entrent dans la forteresse y sont bien autorisées. Une fois à l'intérieur, les individus peuvent accéder à certaines parties du château et pas à d'autres, en fonction de leur rang. Le rang est défini par le seigneur auquel le château appartient. Dans chaque partie du château se trouvent des objets qui peuvent être regardés, touchés, modifiés ou même détruits. Pour ces objets également, c'est le seigneur du château qui détermine qui peut faire quoi avec quel objet. Le seigneur est le seul à pouvoir accéder à toutes les pièces du château et à pouvoir agir comme bon lui semble avec tous les objets du château.
- 11 Dans un système informatique le fonctionnement est **similaire** à celui du château-fort. Pour pouvoir accéder au système informatique l'utilisateur doit généralement entrer un identifiant et un mot de passe. Une fois connecté, l'utilisateur peut accéder à tout ou partie du système informatique en fonction de son niveau d'accréditation, qui est déterminé par l'administrateur du système informatique. Ce niveau d'accréditation détermine également ce que l'utilisateur peut faire ou non dans les parties du système informatique auxquelles il a accès, à savoir uniquement voir le titre des documents contenus dans un dossier, les ouvrir pour les lire, les éditer ou les supprimer. L'administrateur est le seul à pouvoir accéder à tout le système informatique et à disposer des droits qui lui permettent d'effectuer toutes les actions qu'il souhaite avec les données qui s'y trouvent.
- 12 L'analogie avec le monde réel s'arrête cependant là. En effet, la notion d'« accès » dans le monde virtuel ne peut pas être comparée à celle de « pénétrer », dans le monde réel. En informatique, la notion d'« accès » signifie que l'auteur parvient à établir une **connexion** avec tout ou partie d'un système informatique. Il n'y a donc pas à proprement parler de déplacement physique de l'auteur d'un endroit vers un autre.

- 13 Dans la forme simple de l'infraction, le **moyen** utilisé par l'auteur pour se connecter au système informatique est sans importance. L'auteur peut donc établir une connexion au moyen d'un accès local ou d'un accès à distance. Si l'auteur établit une connexion locale avec un système informatique auquel il a physiquement accès, celle-ci se fera au moyen d'un clavier – matériel ou virtuel – et d'une souris, voire simplement avec les doigts pour les tablettes et les *smartphones*. Il peut aussi utiliser un terminal pour se connecter à un système informatique central. Si l'auteur décide au contraire d'établir une connexion à distance, il peut passer par n'importe quel réseau de télécommunication. Le type de réseau (local, public, privé, ...), ainsi que le type de connexion (avec ou sans fil) sont sans importance.
- 14 **L'étendue** de l'accès n'est pas non plus décisif pour la réalisation de l'infraction. L'accès peut être total, auquel cas il s'étend à l'ensemble du système informatique. Il peut aussi n'être que partiel. Dans ce cas il ne concerne qu'une partie du système informatique. Tel est par exemple le cas lorsque l'auteur n'accède qu'à la session d'un utilisateur ou à une partie des données stockées sur un serveur.
- 15 L'infraction est **consommée** dès que la connexion avec le système informatique est établie. Plus rien n'empêche alors l'auteur de prendre connaissance des données informatiques contenues dans le système informatique. Il n'est cependant pas nécessaire que l'auteur en prenne connaissance pour que l'infraction soit consommée. En pratique, ces deux événements coïncident néanmoins le plus souvent, car au moment où l'accès est établi, les données s'affichent à l'écran.
- 16 La notion d'accès au sens de l'art. 2 CCC doit clairement être **distinguée** de l'atteinte à l'intégrité des données qui figure à l'art. 4 CCC. Pour réaliser l'infraction, il suffit que l'auteur se ménage un accès vers un système informatique. Même si, en pratique, l'établissement d'un accès illégal entraîne régulièrement la modification de données, de telles détériorations ne sont pas nécessaires à la commission de l'infraction.
- 17 Enfin, seul l'établissement d'un accès illégal est punissable. Le **maintien** d'un accès, établi de manière licite, après que l'ayant-droit du système informatique a informé l'utilisateur qu'il n'était plus autorisé à y accéder, n'est pas punissable. On peut notamment penser à l'employé qui, au cours de son activité professionnelle, utilise son ordinateur privé pour se connecter au réseau de l'entreprise et qui, une fois licencié, continue à consulter des fichiers de la société. L'absence de punissabilité ne dure toutefois que le temps de la connexion. S'il interrompt la connexion et en établit une nouvelle, il se rend alors coupable de l'infraction. Cette absence de punissabilité constitue à notre avis clairement une lacune improprement dite, les Parties n'ayant sans doute tout simplement pas envisagé cette possibilité lors de l'élaboration du texte.

C. L'illicéité

- 18 Pour être punissable, l'auteur doit avoir agi sans droit. Cela implique de déterminer dans un premier temps si le système informatique est public – c'est-à-dire ouvert à tous – ou si son **accès** est **limité**, voire une combinaison des deux. Si le système informatique est public, l'accès ne peut en aucun cas être illicite et toute infraction est exclue. En revanche, si l'accès à tout ou partie du système informatique est restreint, celui qui y accède sans autorisation est punissable.
- 19 C'est l'ayant droit du système informatique qui détermine qui est **autorisé** à accéder à quelle partie du système informatique. Sont ainsi punissables non seulement les personnes qui n'ont pas été autorisées à accéder au système informatique, mais également celles qui ont été autorisées à accéder à une partie du système informatique, mais qui accèdent à une autre partie du système informatique à laquelle l'accès ne leur a pas été accordé. Ne sont en revanche pas punissables les personnes qui ont été autorisées à accéder au système informatique par son ayant-droit et qui se conforment aux limites de cet accès.

- 20 L'ayant droit du système informatique n'en est pas toujours l'administrateur. C'est en particulier le cas des systèmes informatiques de taille moyenne et grande. Dans ces situations, la gestion du système informatique est déléguée par son ayant-droit à un administrateur tiers. Cet **administrateur** peut être soit une personne physique, soit une personne morale. Dans les deux cas, l'ayant-droit du système informatique autorise l'administrateur à y accéder pour accomplir sa mission. L'administrateur n'accède donc pas sans droit au système informatique tant qu'il le fait dans le but d'accomplir sa mission. En revanche, l'accès est non-autorisé lorsqu'il s'effectue dans un autre but, comme par exemple consulter des informations privées ou confidentielles qui ne lui sont pas destinées.
- 21 Lorsque la gestion du système informatique est déléguée à une **entreprise**, toutes les personnes physiques chargées de cette mission au sein de cette société sont autorisées à y accéder. Tel n'est en revanche pas le cas des personnes physiques au sein de cette personne morale auxquelles cette tâche n'a pas été attribuée. Si ces personnes accèdent au système informatique, elles le font sans droit, car elles ne le font pas pour accomplir la mission qui a été confiée à la personne morale.
- 22 La personne spécifiquement mandatée pour **tester** la sécurité du système informatique, qui réussit à accéder au système informatique en déjouant les mesures de protection mises en place, n'agit pas de manière illicite, car elle y a été autorisée par son ayant-droit.

D. L'intention

- 23 L'accès illégal est **intentionnel**. L'intention doit porter sur tous les éléments objectifs de l'infraction. L'auteur doit donc avoir conscience qu'il accède sans droit à un système informatique et en avoir la volonté. Le dol éventuel suffit. Si l'auteur se doute qu'il accède à tout ou partie d'un système informatique auquel il ne devrait pas avoir accès, mais établit une connexion malgré tout, il se rend coupable d'accès illégal. En revanche, si l'auteur commet une erreur de manipulation et établit une connexion non-autorisée, malgré lui, l'intention fait défaut et l'infraction n'est pas réalisée.
- 24 La norme ne réprime que l'établissement de l'accès illégal et non le fait de **maintenir** l'accès contre la volonté de l'ayant-droit. Partant, celui qui accède à un système informatique par inadvertance, mais qui, une fois connecté, en explore le contenu, n'est pas punissable.
- 25 Lorsque l'auteur pense à tort que le système informatique auquel il accède est public ou qu'il pense à tort être en droit d'y accéder pour une autre raison, il commet une **erreur** sur les faits.

IV. ÉLÉMENTS CONSTITUTIFS SUPPLÉMENTAIRES FACULTATIFS

- 26 Au moment de l'élaboration de la Convention sur la cybercriminalité, une majorité des Parties voulaient ériger en infraction le **piratage** pur et simple. D'autres étaient en revanche opposés à une pénalisation générale du *hacking*, au motif que la simple intrusion ne cause pas forcément des dommages et que, dans certains cas, les actes de *hacking* permettent même de découvrir des failles de sécurité et de les combler⁵. Pour tenir compte de ces considérations et comme les législations nationales de nombreux pays contenaient déjà des dispositions qui réprimaient le piratage sous des formes diverses, il a été donné la possibilité aux Parties de limiter la punissabilité de l'accès illégal en exigeant la réalisation d'un ou plusieurs éléments constitutifs supplémentaires.

A. Accès en violation des mesures de sécurité

- 27 La Convention sur la cybercriminalité donne tout d'abord la possibilité aux Parties de ne sanctionner l'accès illégal que lorsqu'il est commis en violation de mesures de sécurité. L'**Allemagne**, la **Finlande**,

le **Japon**, la **Lituanie**, le **Pérou**, la **République slovaque**, la **République tchèque** et la **Suisse** ont fait usage de cette faculté⁶.

- 28 Cette exigence supplémentaire signifie que le système informatique doit être **protégé** contre un accès non-autorisé. En d'autres termes, si l'auteur accède sans droit à un système informatique qui n'est pas protégé, il n'est pas punissable.
- 29 La notion de **mesures de sécurité** doit être comprise de manière large. Elle englobe tant les mesures de sécurité physiques que virtuelles. En ce qui concerne les mesures de sécurité physiques, le système informatique peut par exemple se trouver dans une pièce fermée à laquelle on ne peut accéder qu'avec une clé, un badge magnétique, une empreinte digitale, rétinienne ou vocale. Sur le plan virtuel, les mesures de sécurité peuvent notamment consister en une protection par pare-feu, code PIN, mot-de-passe, ou encore une double, voire même triple authentification.
- 30 Si l'auteur ne parvient pas à déjouer les mesures de sécurité ou s'il décide spontanément de mettre un terme à son activité avant de les avoir franchies, seule une **tentative** est envisageable. Cela pose toutefois problème puisqu'à la lecture de l'art. 11 § 2 CCC, on constate qu'il n'est pas exigé des Parties qu'elles répriment la tentative d'accès illégal. Chaque Etat est donc libre de traiter cet aspect comme il le souhaite, de sorte que ce comportement pourrait, selon la législation nationale des Etats Parties, ne pas être punissable du tout.

B. Le dessein d'obtenir des données informatiques ou un autre dessein spécial

- 31 Une autre possibilité donnée aux Parties est d'exiger que l'auteur ait agi dans un **dessein spécial**. Plusieurs Etats ont fait usage de cette possibilité.
- 32 Les **Etats-Unis d'Amérique** ont décidé d'exiger que l'auteur ait agi dans le but d'obtenir des données⁷. Bien que cette possibilité ait été donnée aux Parties, son utilisation est regrettable car elle vide la norme d'une grande partie de sa substance. Cette disposition a en effet spécifiquement été

5. Rapport explicatif de la Convention sur la cybercriminalité, n. 49.

6. Déclaration consignée dans une Note verbale de la Représentation Permanente de l'Allemagne déposée avec l'instrument de ratification, le 9 mars 2009 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=GER>, visité le 21.1.2024), en lien avec le § 202a du Code pénal allemand ; Déclaration de la Finlande consignée dans l'instrument de ratification déposé le 24 mai 2007 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=FIN>, visité le 21.1.2024), en lien avec le chapitre 38, section 8 du Code pénal finlandais ; Déclaration consignée dans une lettre du Consul Général du Japon déposée avec l'instrument d'acceptation le 3 juillet 2012 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=JAP>, visité le 21.1.2024), en lien avec l'art. 2 et 3 de la Loi japonaise sur l'interdiction de l'accès à un système informatique non autorisé ; Déclaration consignée dans l'instrument de ratification déposé le 18 mars 2004 et confirmée par une Note Verbale du Ministère des Affaires Etrangères de Lituanie, en date du 26 avril 2004, enregistrée au Secrétariat Général le 10 mai 2004 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=LIT>, visité le 21.1.2024), en lien avec l'art. 198¹ du Code pénal lituanien ; Déclarations consignées dans l'instrument d'adhésion et dans une Note Verbale de l'Ambassade du Pérou en France, reçues et enregistrées au Secrétariat Général le 26 août 2019 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=PER>, visité le 21.1.2024), en lien avec l'art. 2 de la Loi péruvienne sur les délits informatiques ; Déclaration de la République slovaque consignée dans l'instrument de ratification déposé le 8 janvier 2008 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=SLK>, visité le 21.1.2024), en lien avec le § 247 du Code pénal slovaque ; Déclaration de la République tchèque consignée dans l'instrument de ratification déposé le 22 août 2013 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=CZE>, visité le 21.1.2024), en lien avec le § 230 du Code pénal tchèque ; Déclaration de la Suisse consignée dans l'instrument de ratification déposé le 21 septembre 2011 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=SWI>, visité le 21.1.2024), en lien avec l'art. 143^{bis} CP.

élaborée pour réprimer les actes des hackers qui accèdent à des systèmes informatiques par bravade, sans toutefois s'intéresser aux données qu'ils contiennent. Exiger ce dessein spécial précis semble donc contraire à l'esprit de la norme.

- 33 La **Belgique**, quant à elle, a déclaré n'incriminer l'accès illégal que lorsqu'il est commis dans une intention frauduleuse ou à dessein de nuire⁸. L'intention frauduleuse semble se rapporter à la volonté d'obtenir un avantage indu pour soi-même ou pour autrui. Quant au dessein de nuire, il s'agit vraisemblablement de la volonté de causer un préjudice à autrui sous quelque forme que ce soit.
- 34 La **Principauté d'Andorre** et la **République slovaque** ont décidé de ne poursuivre l'accès illégal que s'il était commis dans le but d'obtenir des données sans droit, de les détériorer (en ce qui concerne la Principauté d'Andorre uniquement) ou dans un autre dessein délictueux⁹. Cette formulation vise à éviter que des auteurs échappent à la condamnation en raison du fait qu'ils poursuivaient un autre dessein que l'obtention ou la détérioration de données. A notre avis, elle doit toutefois être interprétée à la lumière des desseins spéciaux énumérés à l'art. 2 CCC et s'y apparenter à la fois en ce qui concerne le but poursuivi par l'auteur et son intensité délictuelle. Le 1^{er} janvier 2021, le Code pénal slovaque a été modifié et la réserve de la République slovaque adaptée¹⁰. Le § 247 a été remanié. Dans sa forme simple, cette disposition n'exige plus aucun dessein spécial (§ 247 par. 1). Le § 247 par. 2 prévoit en revanche une forme qualifiée lorsque l'auteur cause un préjudice considérable.
- 35 Enfin, le **Canada** a indiqué qu'il ne poursuivrait l'accès illégal que s'il était commis avec une intention délictueuse¹¹. Cette dernière notion est particulièrement peu précise et crée par conséquent une insécurité du droit considérable. De plus, elle semble se recouper avec la notion d'intention. Elle doit donc selon nous être interprétée restrictivement.
- 36 Le **Chili** avait initialement émis une réserve identique à celle du Canada¹². Il a toutefois modifié sa législation en 2022. Dans sa nouvelle version, l'*accesso ilícito* est punissable lorsqu'il est commis

-
7. Déclaration des Etats-Unis d'Amérique consignée dans l'instrument de ratification déposé le 29 septembre 2006 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=USA>, visité le 21.1.2024), en lien avec le titre 18 § 1030 section a chiffre 1 à 3 du Code des Etats-Unis (Computer Fraud and Abuse Act).
8. Déclaration communiquée par le Ministre des affaires étrangères de la Belgique au moment du dépôt de l'instrument de ratification, le 20 août 2012 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=BEL>, visité le 21.1.2024), en lien avec l'art. 550bis § 2 du Code pénal belge.
9. Réserve consignée dans une Note Verbale du Ministère des Affaires étrangères d'Andorre, datée du 14 octobre 2016, déposée avec l'instrument de ratification le 16 novembre 2016 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=AND>), en lien avec les art. 182 et 225 du Code pénal andorran ; Déclaration de la République slovaque consignée dans l'instrument de ratification déposé le 8 janvier 2008, (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=SLK>, visité le 21.1.2024), en lien avec l'ancien § 247 du Code pénal slovaque.
10. Déclaration consignée dans l'instrument de ratification déposé le 8 janvier 2008, amendée dans une Note verbale de la Représentation Permanente de la République slovaque, datée du 30 avril 2021, enregistrée au Secrétariat Général le 30 avril 2021 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=SLK>, visité le 21.1.2024), en lien avec le nouveau § 247 du Code pénal slovaque.
11. Déclaration consignée dans une Note Verbale de la Mission du Canada auprès de l'Union européenne, déposée avec l'instrument de ratification le 8 juillet 2015 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=CAN>, visité le 21.1.2024), en lien avec l'art. art. 342.1 du Code pénal canadien.
12. Déclaration du Chili consignée dans l'instrument d'adhésion reçu et enregistré au Secrétariat Général le 20 avril 2017 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=CHI>, visité le 21.1.2024), en lien avec l'art. 2 de la Loi chilienne N° 19.223 sur les délits informatiques.

intentionnellement¹³. Un dessein spécial n'est plus exigé. Cependant, lorsque l'accès illégal est commis dans le but d'obtenir ou d'utiliser les données contenues dans le système informatique, la peine est augmentée¹⁴.

C. Un système informatique connecté à un autre système informatique

- 37 La Convention sur la cybercriminalité permet enfin aux Parties de limiter la punissabilité de l'accès illégal aux **connexions** établies sans droit avec un système informatique par l'intermédiaire d'un autre système informatique. En faisant usage de cette possibilité, les Parties peuvent exclure les cas dans lesquels l'auteur accède physiquement au système informatique qu'il vise, sans passer par un réseau.
- 38 Les seuls Etats à avoir fait usage de cette possibilité sont la **République slovaque** et le **Japon**¹⁵. Le Code pénal slovaque a depuis été modifié. La nouvelle teneur du § 247, entrée en vigueur le 1^{er} janvier 2021, ne prévoit plus cette exigence dans sa version actuelle, de sorte que la réserve de la République slovaque a été adaptée¹⁶.

V. COMPARAISON AVEC LE DROIT SUISSE

- 39 En droit suisse, le *hacking* est réprimé par l'**art. 143^{bis} CP**. Cette disposition sanctionne l'accès indu au système informatique d'autrui, spécialement protégé contre tout accès, au moyen d'un dispositif de transmission de données. Cette norme ne correspond toutefois pas aux exigences de l'art. 2 CCC à trois égards.
- 40 Premièrement, la convention n'effectue pas de distinction entre les systèmes informatiques. Elle protège l'intégrité de tous les systèmes informatique, indépendamment de leur appartenance. L'art. 143^{bis} al. 1 CP, en revanche, incrimine uniquement l'accès indu au système informatique « **appartenant à autrui** ». Compte tenu du fait que cette disposition se trouve dans le titre 2 du Code pénal, soit des infractions contre le patrimoine, cette formulation doit être interprétée au regard des droits réels¹⁷. Le système informatique doit donc appartenir à une personne autre que l'auteur. Si l'auteur est le propriétaire ou le copropriétaire du système informatique, cet élément constitutif n'est pas réalisé puisqu'il n'appartient pas à autrui. Ainsi, si plusieurs sessions ont été ouvertes dans le même système informatique, l'auteur, (co)propriétaire du système informatique, qui accède à une autre session que la sienne n'est pas punissable¹⁸. La doctrine majoritaire estime au contraire qu'il faut comprendre par « appartenant à autrui » qu'une personne autre que l'auteur est autorisée à accéder et à disposer du système informatique ou d'un sous-système informatique¹⁹. Une telle interprétation rendrait toutefois la notion « appartenant à autrui » redondante avec l'élément constitutif de l'illicéité

13. Art. 2 al. 1 de la Loi chilienne N° 21.459 sur les délits informatiques.

14. Art. 2 al. 2 de la Loi chilienne N° 21.459 sur les délits informatiques.

15. Déclaration de la République slovaque consignée dans l'instrument de ratification déposé le 8 janvier 2008 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=SLK>, visité le 21.1.2024), en lien avec l'ancien § 247 du Code pénal slovaque ; Déclaration consignée dans une lettre du Consul Général du Japon déposée avec l'instrument d'acceptation le 3 juillet 2012 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=JAP>, visité le 21.1.2024), en lien avec l'art. 2 et 3 de la Loi japonaise sur l'interdiction de l'accès à un système informatique non autorisé.

16. Déclaration consignée dans l'instrument de ratification déposé le 8 janvier 2008, amendée dans une Note verbale de la Représentation Permanente de la République slovaque, datée du 30 avril 2021, enregistrée au Secrétariat Général le 30 avril 2021 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=SLK>, visité le 21.1.2024), en lien avec le nouveau § 247 du Code pénal slovaque.

17. Schmid, § 5 n. 17. Contra : Weissenberger, n. 12 ad art. 143bis CP.

18. Schmid, § 5 n. 17.

de l'accès. Si le législateur a mentionné ces deux éléments de manière distincte, c'est qu'il s'agit de deux notions qui doivent être analysées indépendamment l'une de l'autre. Pour être conforme à la convention, le terme « autrui » figurant à l'art. 143^{bis} al. 1 CP devrait donc être supprimé.

- 41 L'art. 143^{bis} al. 1 CP exige que l'auteur ait accédé au système informatique à l'aide d'un **dispositif de transmission de données**²⁰. Cela a par exemple pour conséquence que l'auteur qui profite de l'absence de sa victime pour entrer dans son bureau et se connecter directement à son ordinateur ne se rend pas coupable d'accès indu à un système informatique puisqu'il n'utilise pas un dispositif de transmission de données²¹. L'art. 2 § 2 CCC permet aux Parties de limiter la poursuite pénale à l'accès illégal commis au moyen d'un système informatique connecté à un autre système informatique. La Suisse n'a toutefois pas déclaré faire usage de cette possibilité. En conséquence, l'élément constitutif de l'accès au moyen d'un dispositif de transmission de données devrait être supprimé.
- 42 Enfin, l'art. 143^{bis} CP consacre une infraction poursuivie sur **plainte** uniquement. Or, lorsqu'une infraction n'est poursuivie que sur plainte, une autorité pénale ne peut se saisir elle-même. Etant donné qu'il existe un conflit de doctrine sur le fait qu'une plainte déposée dans l'Etat requérant suffise à mettre en œuvre la coopération internationale, il serait prudent de poursuivre l'accès indu à un système informatique d'office²².
- 43 Au vu de ce qui précède, force est de constater que le droit suisse n'est **pas conforme** à l'art. 2 CCC. L'art. 143^{bis} CP devrait par conséquent être modifié.

Les notions techniques d'informatique figurant dans la présente contribution ont été rédigées avec l'aide de Monsieur Yannick Jacquety, ICT Manager avec diplôme fédéral. Il en est ici chaleureusement remercié.

BIBLIOGRAPHIE

Dupuis Michel / Geller Bernard / Monnier Gilles / Moreillon Laurent / Piguet Christophe / Bettex Christian / Stoll Daniel (éditeurs), Code pénal - Petit commentaire, 2. éd., Bâle 2017

Pfister Christa, Hacking in der Schweiz, Diss., Zürich, 2008

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994

Schwarzenegger Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, in : Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zurich 2002

Stratenwerth Günter / Bommer Felix, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 8. éd., Berne, 2022

Trechsel Stefan / Cramer Dean, in : Trechsel Stefan / Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Weissenberg Philippe, in : Niggli Marcel Alexander / Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

19. Dupuis et al., n. 10 ad art. 143^{bis} CP ; Pfister, pp. 105-106; Stratenwerth / Bommer, § 14 n. 39 ; Trechsel / Cramer, n. 4 ad art. 143^{bis} CP ; Weissenberger, n. 13 ad art. 143^{bis} CP.

20. Dupuis et al., n. 17 ad art. 143^{bis} CP ; Trechsel / Cramer, n. 7 ad art. 143^{bis} CP ; Weissenberger, n. 17 ad art. 143^{bis} CP.

21. FF 1991 II 979 ; Pfister, p. 115 ; Trechsel / Cramer, n. 7 ad art. 143^{bis} CP ; Weissenberger, n. 18 ad art. 143^{bis} CP.

22. Schwarzenegger, p. 317 et les références citées.

TRAVAUX LÉGISLATIFS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible sous <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

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, FF 1991 II 933, disponible sous https://www.fedlex.admin.ch/eli/fga/1991/2_969_933_797/fr, visité le 21.1.2024