



COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

COMMENTAIRE

Art. 6 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: 10.17176/20240217-133236-0

PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 6 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 6 CCC N. XXX.

Art. 6 Abus de dispositifs

¹ Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux art. 2 à 5 ci-dessus,

ii. d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les art. 2 à 5; et

b. la possession d'un élément visé à la let. a. ch. i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les art. 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

² Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au par. 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux art. 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

³ Chaque Partie peut se réserver le droit de ne pas appliquer le par. 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au par. 1. let. a. ch. ii du présent article.

TABLE DES MATIÈRES

I. Généralités	4
II. Bien juridiquement protégé.....	4
III. Éléments constitutifs de base	4
A. Un objet illicite	4
1. Un dispositif permettant la commission d'une infraction mentionnée aux art. 2 à 5 CCC	4
2. Des données permettant d'accéder à un système informatique dans le but de commettre l'une des infractions mentionnées aux art. 2 à 5 CCC	5
B. Un comportement punissable	5
1. La production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition.....	5
2. La possession.....	6
C. L'illicéité	6
D. L'intention	7
E. Un dessein spécial	7
IV. Les réserves	7
A. Quant aux comportements punissables	7
B. Quant au matériel illicite	9
V. Comparaison avec le droit suisse.....	10
Bibliographie	11
Travaux législatifs	11

I. GÉNÉRALITÉS

- 1 La commission des infractions réprimées aux art. 2 à 5 CCC nécessite en principe l'utilisation d'**outils informatiques**. Tous les cybercriminels ne sont toutefois pas capables de créer ces outils eux-mêmes. Ils cherchent par conséquent à les acquérir auprès de tiers. Au fil du temps, cette demande a conduit à la création d'un véritable marché noir, notamment sur le *dark net*. De nos jours, presque n'importe qui peut acquérir des *malwares* en tout genre, louer des *bots-nets* ou même mandater des cybercriminels pour accomplir des tâches spécifiques. Compte tenu du risque que ce marché noir représente pour l'ensemble des systèmes informatiques et leurs utilisateurs légitimes, les Parties ont décidé de sanctionner pénalement certains actes, potentiellement dangereux, en amont, avant la commission des infractions visées aux art. 2 à 5 CCC¹. L'art. 6 CCC s'appuie sur des instruments adoptés par le Conseil de l'Europe (Convention européenne sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel – STE n° 178) et l'Union européenne (Directive 98/84/EC du Parlement européen et du Conseil en date du 20 novembre 1998 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel), ainsi que sur les dispositions adoptées dans certains pays en la matière².

II. BIEN JURIDIQUEMENT PROTÉGÉ

- 2 En réprimant toutes les formes de commerce ou de possession de matériel destiné à commettre l'une des infractions réprimées par les art. 2 à 5 CCC, les Parties rendent punissables les **actes préparatoires** à la commission de ces infractions. Le but est donc de renforcer la protection des biens juridiques protégés par les art. 2 à 5 CCC, à savoir l'inviolabilité et le bon fonctionnement des systèmes informatiques, ainsi que l'intégrité, la disponibilité et la confidentialité des données.

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Un objet illicite

1. Un dispositif permettant la commission d'une infraction mentionnée aux art. 2 à 5 CCC
- 3 La notion de dispositif n'est définie ni dans le texte de la convention ni dans son rapport explicatif. A notre avis, un **dispositif** au sens de l'art. 6 CCC est un ensemble de pièces, d'éléments ou de données destiné à accomplir une ou plusieurs fonctions précises. On en veut pour preuve que les Parties citent expressément le programme informatique à titre d'exemple de dispositif. Comme il ressort clairement de l'adjonction des termes « y compris », la notion se veut bien plus large que les seuls programmes informatiques. En plus des virus, vers, chevaux de Troie, bombes logiques et autres maliciels qui font indiscutablement partie des programmes visés par cette disposition, on trouve donc aussi des dispositifs matériels tels que les micros, les caméras ou les robots.
- 4 Le **champ d'application** de la norme se limite toutefois aux dispositifs conçus ou adaptés pour commettre l'une des infractions réprimées par les art. 2 à 5 CCC. Il s'agit donc de dispositifs ou de programmes qui sont conçus, par exemple, pour altérer, voire détruire des données, ou pour s'ingérer dans le fonctionnement des systèmes, tels que les programmes-virus, ou bien des programmes conçus ou adaptés pour accéder à des systèmes informatiques³. Les dispositifs qui ne permettent pas

1. Rapport explicatif de la Convention sur la cybercriminalité, n. 71.

2. Rapport explicatif de la Convention sur la cybercriminalité, n. 71.

3. Rapport explicatif de la Convention sur la cybercriminalité, n. 72.

d'accomplir de tels actes ne sont pas concernés par l'art. 6 § 1 let. a ch. 1 CCC. Il en va de même des dispositifs qui permettent de commettre une autre infraction, notamment l'une de celles réprimées par les art. 7 à 10 CCC.

- 5 Au moment de l'élaboration de la convention, une discussion approfondie a eu lieu pour déterminer si les dispositifs visés devaient être ceux qui étaient conçus exclusivement ou spécialement pour permettre la commission d'infractions, ce qui excluait les **dispositifs à double usage**, ou s'il fallait au contraire aussi inclure ces derniers. Les Parties ont finalement conclu qu'il ne fallait pas limiter la poursuite pénale aux seuls dispositifs conçus exclusivement pour commettre des infractions, car cela aurait considérablement réduit le nombre de cas auxquels la norme pourrait s'appliquer. Les Parties ont cependant aussi écarté l'hypothèse consistant à étendre la norme à l'ensemble des dispositifs, y compris licites, qui pourraient permettre la commission des infractions d'une manière ou d'une autre, car la réalisation de l'infraction n'aurait alors reposé plus que sur l'intention de l'auteur. C'est donc une solution intermédiaire qui a été adoptée.
- 6 Sont ainsi visés par l'art. 6 § 1 let. a ch. 1 CCC les dispositifs **principalement** conçus ou adaptés pour permettre la commission de l'une des infractions réprimées par les art. 2 à 5 CCC. Cette formulation exclut les dispositifs à double usage⁴, à moins que l'usage principal soit de commettre une infraction.

2. Des données permettant d'accéder à un système informatique dans le but de commettre l'une des infractions mentionnées aux art. 2 à 5 CCC

- 7 Afin de couvrir l'ensemble des moyens utilisés par les cybercriminels pour commettre l'une des infractions réprimées par les art. 2 à 5 CCC, les Parties ont également rendu punissables les actes visant à mettre à disposition des mots de passe, codes d'accès et données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique (art. 6 § 1 let. a ch. 2 CCC). Le but est d'éliminer toute **lacune**. Cette approche est parfaitement justifiée au regard du grand nombre de mots de passe et autres données d'accès qui ont été dérobés et qui sont proposés à la vente sur le *dark net*.

B. Un comportement punissable

- 8 Les Parties ont voulu réprimer toutes les formes de mise à disposition d'objets illicites, de même que leur possession. En revanche, on constate que la simple fourniture d'**instructions** – par exemple sous forme de textes ou de vidéos – sur la manière de fabriquer des objets illicites n'est pas punissable.

1. La production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition

- 9 L'art. 6 § 1 let. a CCC énumère plusieurs comportements punissables relatifs au commerce. Cette liste est **exhaustive**. Afin de n'oublier aucun comportement, elle se termine néanmoins par une clause générale (« Auffangtatbestand »).
- 10 La « **production** » est la fabrication du matériel illicite en vue de son utilisation pour commettre l'une des infractions figurant aux art. 2 à 5 CCC. Le terme de « production » comprend l'ensemble des étapes nécessaires à la réalisation de l'objet. Cela comprend donc l'écriture du code du maliciel – en langage informatique – ou encore le décryptage d'un mot de passe.
- 11 L'art. 6 § 1 let. a CCC sanctionne ensuite la « **vente** ». Ce terme désigne la remise d'un objet illicite mentionné dans ce paragraphe en échange d'une somme d'argent. La devise dans laquelle la somme

4. Rapport explicatif de la Convention sur la cybercriminalité, n. 73.

est payée n'a pas d'importance. Cette somme peut même être payée en cryptomonnaies. La remise doit toutefois être onéreuse. Il ne peut pas s'agir d'une donation.

- 12 L'« **obtention pour utilisation** » implique un comportement actif de la part de celui qui cherche à se procurer du matériel interdit. Il faut s'être mis en relation avec quelqu'un qui détient le matériel prohibé et l'avoir acquis à titre gratuit ou contre rémunération. La manière dont le matériel est remis est sans importance. Le transfert peut donc se faire par voie électronique, par envoi postal ou même par remise en main propre. Ce qui est déterminant, c'est que l'auteur obtienne le matériel illicite dans le but de l'utiliser pour commettre l'une des infractions réprimées par les art. 2 à 5 CCC. Si l'objectif est de commettre une autre infraction ou simplement de collectionner ce type de matériel, l'auteur n'est pas punissable.
- 13 Le quatrième comportement mentionné dans la liste est l'« **importation** ». Ce terme désigne le fait d'introduire un objet illicite dans le pays qui sanctionne cet acte. L'importation de matériel prohibé crée un risque important qu'il soit par la suite remis à des tiers. Pour réduire ce risque, la simple introduction dans le pays est interdite, même si l'importateur n'est qu'un maillon de la chaîne entre le producteur du matériel et l'utilisateur final.
- 14 L'art. 6 § 1 réprime encore la « **diffusion** ». Il s'agit de la transmission de matériel illicite à un nombre indéterminé de personnes qui n'en ont pas nécessairement fait la demande. L'envoi du matériel peut se faire par n'importe quel mode, que ce soit par voie informatique, par courrier postal ou par remise en main propre.
- 15 Pour éviter toute lacune, la liste se termine par « **d'autres formes** de mise à disposition ». Cette hypothèse permet d'englober tous les cas qui ne correspondent pas exactement aux notions examinées ci-dessus, mais qui permettent néanmoins à l'auteur de fournir des objets illicites à des tiers. Cette expression inclut, par exemple, la création ou la compilation de liens hypertextes qui visent à faciliter l'accès à du matériel illicite⁵.

2. La possession

- 16 L'art. 6 § 1 let. b CCC réprime la **possession** de l'un des objets mentionnés ci-dessus⁶. Tout comme pour les comportements énumérés à l'art. 6 § 1 let. a CCC, l'auteur doit détenir le matériel prohibé dans l'intention de commettre l'une des infractions sanctionnées par les art. 2 à 5 CCC. Si l'auteur détient ce matériel dans le but de commettre une autre infraction ou simplement à des fins de collection, il n'est pas punissable.
- 17 Les Parties ont toutefois laissé une certaine marge de manœuvre à chaque Etat pour déterminer si la possession d'un seul élément suffisait à réaliser l'infraction, ou s'il fallait en posséder un certain **nombre**. Force est toutefois de constater que cette possibilité semble surtout avoir été introduite en faveur des Etats-Unis d'Amérique, lesquels ont été les seuls à en faire usage⁷. Ils n'ont toutefois pas précisé le nombre minimal d'éléments qu'il fallait posséder pour être punissable. Ils se sont simplement référés au nombre prévu dans la loi fédérale des Etats-Unis applicable.

C. L'illicéité

- 18 L'exigence selon laquelle l'auteur doit avoir agi **sans droit** permet aux Parties de créer des exceptions à la répression pénale. Cela leur permet notamment d'exclure du champ d'application de l'art. 6 CCC

5. Rapport explicatif de la Convention sur la cybercriminalité, n. 72.

6. Voir chiffre III. A ci-dessus.

les autorités de poursuite pénale qui détiennent légalement du matériel illicite, sous forme de séquestres, dans le cadre de leurs enquêtes.

- 19 L'art. 6 § 2 réserve expressément l'hypothèse dans laquelle l'auteur n'agit pas sans droit, à savoir que les comportements énumérés à l'art. 6 § 1 let. a ch. 1 CCC ne sont pas punissables s'ils n'ont pas pour but de commettre une infraction réprimée par les art. 2 à 5 CCC. Ainsi, par exemple, les dispositifs d'essai (également appelés « dispositifs de craquage ») et les dispositifs d'analyse de réseaux conçus par les professionnels pour évaluer la fiabilité de leurs produits informatiques ou contrôler la sécurité des systèmes sont fabriqués à des **fins légitimes** et leurs utilisateurs sont donc considérés comme agissant « avec droit »⁸.

D. L'intention

- 20 L'abus de dispositifs est **intentionnel** . L'intention doit porter sur tous les éléments objectifs de l'infraction. Si l'auteur possède ou fournit un programme informatique ordinaire à un tiers sans se douter qu'il pourrait aussi être utilisé pour commettre l'une des infractions réprimées par les articles 2 à 5 CCC, il n'est pas punissable.

E. Un dessein spécial

- 21 En plus de l'intention, l'auteur doit avoir agi dans le **dessein** de commettre l'une des infractions visées aux articles 2 à 5 CCC⁹. Il ne suffit par conséquent pas que l'auteur veuille fabriquer un programme malveillant uniquement pour le défi technique que cela représente ou pour en faire la collection. De même, il ne suffit pas que l'auteur veuille utiliser le programme malveillant ou le mot de passe dans le but de commettre une infraction autre que celles réprimées par les art. 2 à 5 CCC.
- 22 Le but poursuivi par l'auteur doit être la commission, par lui-même ou par un tiers auquel il fournit le matériel prohibé, de l'une des infractions sanctionnées par les art. 2 à 5 CCC. L'art. 6 CCC consacre une infraction de **mise en danger abstraite** . Il n'est donc pas nécessaire que le matériel illicite soit effectivement utilisé ultérieurement pour commettre l'une de ces infractions. Il suffit que l'acte punissable soit commis dans le but d'accomplir l'une des infractions réprimées par les art. 2 à 5 CCC.

IV. LES RESERVES

- 23 Les seuls comportements que les Parties doivent impérativement sanctionner est la vente, la distribution ou toute autre mise à disposition d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique. Elles ont en revanche la possibilité de **limiter** le champ d'application de cette norme en ce qui concerne les autres comportements punissables et/ou les objets illicites.

A. Quant aux comportements punissables

- 24 La convention permet aux Parties de **limiter** la poursuite pénale en refusant de poursuivre la production, l'obtention pour utilisation, l'importation et la possession de matériel illicite.

7. Déclaration 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&code_Pays=USA, visité le 21.1.2024), en lien avec le titre 18 § 1030 du Code des Etats-Unis (Computer Fraud and Abuse Act).

8. Rapport explicatif de la Convention sur la cybercriminalité, n. 77.

9. Rapport explicatif de la Convention sur la cybercriminalité, n. 76.

- 25 La **Géorgie**, la **Suisse**, le **Chili**, le **Japon** et le **Sri-Lanka** ont fait usage de cette possibilité pour limiter au maximum les comportements punissables¹⁰.
- 26 La **Principauté d'Andorre** a indiqué que l'obtention de dispositifs mentionnés à l'art. 6 § 1 let. a CCC destinés à l'utilisation n'était pas punissable dans son droit interne¹¹.
- 27 L'**Azerbaïdjan** a déclaré qu'elle ne poursuivrait les comportements énumérés à l'art. 6 § 1 CCC que si un dommage sérieux survenait¹².
- 28 L'**Ukraine** a expliqué qu'elle ne réprimerait pas l'obtention pour utilisation et d'autres formes de mise à disposition des éléments visés à l'art. 6 § 1 let. a ch. 1 CCC, ainsi que la production et l'obtention pour utilisation des éléments visés à l'art. 6 § 1 let. a ch. 2 CCC¹³.
- 29 Les **Etats-Unis d'Amérique** se sont réservés le droit de ne pas poursuivre la production, l'obtention pour utilisation, l'importation et la possession de matériel illicite conçu ou adapté pour permettre la commission des infractions réprimées par les art. 4 et 5 CCC¹⁴.
- 30 **Israël** a déclaré qu'il ne poursuivrait pas l'obtention pour utilisation ou l'importation de matériel illicite, ni la possession d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique¹⁵.
- 31 L'**Allemagne**, la **Principauté d'Andorre**, l'**Argentine** et le **Pérou** se sont limités à refuser de poursuivre la possession de matériel illicite (art. 6 § 1 let. b CCC)¹⁶.

-
10. Déclaration consignée dans une Déclaration du Ministre des Affaires Etrangères de la Géorgie, datée du 1^{er} juin 2012, déposée avec l'instrument d'approbation le 6 juin 2012 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=GEO>, visité le 21.1.2024), en lien avec l'art. 285 du Code pénal géorgien ; Réserve 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=2&codePays=SWI>, en lien avec les art. 143^{bis} al. 2 et 144^{bis} ch. 2 du Code pénal suisse ; Réserve 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=2&codePays=CHI>, visité le 21.1.2024), en lien avec la Loi chilienne N° 19.223 sur les délits informatiques ; Réserve 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=2&codePays=JAP>, visité le 21.1.2024), en lien avec les art. 168-2 et 168-3 du Code pénal japonais et les art. 4, 5 et 6 de la Loi japonaise sur l'interdiction de l'accès à un système informatique non autorisé ; Réserve consignée dans une Note Verbale de l'Ambassade du Sri Lanka auprès de la Belgique, datée du 26 mai 2015, et dans l'instrument d'adhésion, déposés simultanément le 29 mai 2015 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=LKA>, visité le 21.1.2024), en lien avec l'art. 9 de la Loi sri-lankaise sur les crimes informatiques.
 11. 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>, visité le 21.1.2024), en lien avec l'art. 182 du Code pénal andorran.
 12. Réserve de l'Azerbaïdjan annexée aux pleins pouvoirs remis au Secrétaire Général lors de la signature de l'instrument, le 30 juin 2008, et confirmée dans l'instrument de ratification déposé le 15 mars 2010 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=AZE>, visité le 21.1.2024), en lien avec l'art. 272.1 du Code pénal azerbaïdjanais.
 13. Réserve de l'Ukraine consignée dans l'instrument de ratification déposé le 10 mars 2006 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=U>, visité le 21.1.2024), en lien avec l'art. 361 du Code pénal ukrainien.
 14. Réserve 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=2&codePays=USA>, visité le 21.1.2024), en lien avec la section a chiffre 6 du Computer Fraud and Abuse Act.
 15. Réserve d'Israël consignée dans l'instrument d'adhésion déposé le 9 mai 2016 (disponible <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=ISR>, visité le 21.1.2024), en lien avec la section 6 de la Loi informatique israélienne.

B. Quant au matériel illicite

- 32 La convention permet aussi aux Parties de limiter la poursuite en refusant de considérer comme illicite les **dispositifs**, y compris les programmes informatiques, principalement conçus ou adaptés pour permettre la commission de l'une des infractions réprimées par les art. 2 à 5 CCC.
- 33 La **Géorgie**, la **Norvège**, la **Suisse**, le **Japon** et le **Sri-Lanka** ont également fait usage de cette possibilité pour limiter au maximum le matériel punissable¹⁷.
- 34 Le **Chili** avait initialement émis une réserve identique à celle de la Géorgie, de la Norvège, de la Suisse et du Japon¹⁸. Il a toutefois modifié sa législation en 2022. Dans sa nouvelle version, l'*abuso de los dispositivos* correspond à l'art. 6 CCC¹⁹. La réserve n'est donc plus nécessaire.
- 35 Les **Etats-Unis d'Amérique** se sont réservés le droit de ne pas poursuivre les dispositifs, y compris les programmes informatiques, conçus ou adaptés pour permettre la commission des infractions réprimées par les art. 4 et 5 CCC²⁰.
- 36 L'**Allemagne** a déclaré qu'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission d'une infraction réprimée par les art. 2 à 5 CCC n'était pas du matériel punissable en droit allemand²¹.

-
16. Réserve 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=2&codePays=GER>, visité le 21.1.2024), en lien avec le §202c du Code pénal allemand ; 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>, visité le 21.1.2024), en lien avec l'art. 182 du Code pénal andorran ; Réserve de l'Argentine consignée dans l'instrument d'adhésion reçu et enregistré au Secrétariat Général le 5 juin 2018 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=ARG>, visité le 21.1.2024), en lien avec l'art. 183 du Code pénal argentin ; Réserves 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=2&codePays=PER>, visité le 21.1.2024), en lien avec l'art. 10 de la Loi péruvienne sur les délits informatiques.
 17. Déclaration consignée dans une Déclaration du Ministre des Affaires Etrangères de la Géorgie, datée du 1^{er} juin 2012, déposée avec l'instrument d'approbation le 6 juin 2012 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=GEO>, visité le 21.1.2024), en lien avec l'art. 285 du Code pénal géorgien ; Réserve de la Norvège consignée dans l'instrument de ratification déposé le 30 juin 2006 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=NOR>, visité le 21.1.2024), en lien avec la section 201 du Code pénal norvégien ; Réserve 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=2&codePays=SWI>, en lien avec les art. 143^{bis} al. 2 et 144^{bis} ch. 2 du Code pénal suisse ; Réserve 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=2&codePays=JAP>, visité le 21.1.2024), en lien avec les art. 168-2 et 168-3 du Code pénal japonais et art. 4, 5 et 6 de la Loi japonaise sur l'interdiction de l'accès à un système informatique non autorisé ; Réserve consignée dans une Note Verbale de l'Ambassade du Sri Lanka auprès de la Belgique, datée du 26 mai 2015, et dans l'instrument d'adhésion, déposés simultanément le 29 mai 2015 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=LKA>, visité le 21.1.2024), en lien avec l'art. 9 de la Loi sri-lankaise sur les crimes informatiques.
 18. Réserve 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=2&codePays=CHI>, visité le 21.1.2024).
 19. art. 8 de la Loi chilienne N° 21.459 sur les délits informatiques.
 20. Réserve 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=2&codePays=USA>, visité le 21.1.2024), en lien avec la section a chiffre 6 du Computer Fraud and Abuse Act.

V. COMPARAISON AVEC LE DROIT SUISSE

- 37 Dans son Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, le Conseil fédéral indiquait que l'art. 6 CCC était couvert pour l'essentiel par l'**art. 144^{bis} ch. 2 CP**, ainsi que par l'ajout d'un second alinéa à l'**art. 143^{bis} CP**²².
- 38 Or, même si la Suisse a fait usage de toutes les possibilités données par l'art. 6 § 3 CCC pour **limiter** au maximum les comportements punissable et le matériel illicite, il n'en demeure pas moins que le droit suisse est loin de satisfaire aux exigences minimales posées par l'art. 6 CCC, pour plusieurs raisons.
- 39 Premièrement, l'art. 144^{bis} ch. 2 al. 1 CP ne s'applique qu'aux **logiciels**²³. Il n'est donc pas applicable à d'autres dispositifs, ni aux mots de passe, ni aux code d'accès ou données informatiques similaires. A cela s'ajoute que les logiciels visés par l'art. 144^{bis} ch. 2 al. 1 CP doivent être propres ou destinés à commettre une infraction réprimée par l'art. 144^{bis} ch. 1 al. 1 CP²⁴. Cela pose deux problèmes. D'une part, 144^{bis} ch. 1 al. 1 CP ne satisfait pas entièrement aux conditions minimales de l'art. 4 CCC²⁵. D'autre part, l'art. 144^{bis} ch. 2 al. 1 CP fait complètement abstraction des logiciels propres ou destinés à commettre une infraction correspondant à celles réprimées par les art. 2, 3 ou 5 CCC. Ces logiciels ne sont donc pas punissables en droit suisse.
- 40 L'ajout de l'art. 143^{bis} al. 2 CP ne permet de combler qu'une faible partie de ces **lacunes** très importantes. En effet, cette disposition ne réprime que le fait de mettre en circulation ou de rendre accessible un mot de passe, un programme ou toute autre donnée propres ou destinés à commettre l'infraction réprimée par l'art. 143^{bis} al. 1 CP. Or, d'une part, cette norme ne correspond pas aux exigences minimales de l'art. 2 CCC²⁶. D'autre part, elle ne réprime pas la mise en circulation ou le fait de rendre accessible un mot de passe, un programme ou toute autre donnée propres ou destinés à commettre une autre infraction que celle réprimée par 143^{bis} al. 1 CP.
- 41 En définitive, même à supposer que l'art. 143^{bis} al. 1 CP réponde aux exigences de l'art. 2 CCC et que l'art. 144^{bis} ch. 1 al. 1 CP corresponde aux conditions minimales de l'art. 4 CCC, la **punissabilité** en droit suisse se limiterait à la mise en circulation ou au fait de rendre accessible un mot de passe, un programme ou toute autre donnée propres ou destinés à commettre l'infraction réprimée par l'art. 2 CCC, ainsi qu'à la fabrication, l'importation, la mise en circulation, la promotion, l'offre ou le fait de rendre accessibles d'une quelconque manière des logiciels propres ou destinés à commettre l'infraction réprimée par l'art. 4 CCC.
- 42 Pour correspondre aux exigences minimales de l'art. 6 CCC, il faudrait donc **adapter** les art. 143 al. 1, 143^{bis} al. 1 et 144^{bis} ch. 1 al. 1 CP dans le sens indiqué ci-dessus²⁷ ; créer l'équivalent de l'art. 5 CCC²⁸ et compléter chacune de ces dispositions en y ajoutant un alinéa qui réprimerait la vente, la distribution ou toute autre mise à disposition de mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans le but de commettre l'une de ces quatre infractions.

21. Réserve 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=2&codePays=GER](https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=GER), visité le 21.1.2024)

22. FF 2010 4285

23. Trechsel / Cramer, n. 13 ad art. 144^{bis} CP ; Weissenberg, n. 48 ad art. 144^{bis} CP.

24. Weissenberger, n. 50 ad art. 144^{bis} CP.

25. Voir Art. 4 CCC n. 30ss.

26. Voir Art. 2 CCC n. 39ss.

27. Voir Art. 2 CCC n. 39ss, Art. 3 CCC n. 40ss, Art. 4 CCC n. 30ss.

28. Voir Art. 5 CCC n. 33ss.

BIBLIOGRAPHIE

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

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

TRAVAUX LÉGISLATIFS

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

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, FF 2010 4275, disponible à <https://www.fedlex.admin.ch/eli/fga/2010/813/fr>, visité le 21.1.2024