



COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

COMMENTAIRE

Art. 5 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: 10.17176/20240217-133039-0

PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 5 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 5 CCC N. XXX.

Art. 5 Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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.

TABLE DES MATIÈRES

I. Généralités	3
II. Bien juridiquement protégé.....	3
III. Éléments constitutifs de base	3
A. Un système informatique.....	3
B. Un comportement punissable	4
1. L'introduction de données.....	4
2. La transmission de données	4
3. L'endommagement, la détérioration et l'altération de données	5
4. La suppression et l'effacement de données	5
5. Le mode de commission	6
C. Une entrave grave au fonctionnement du système informatique	6
D. L'illicéité	7
E. L'intention.....	8
IV. Comparaison avec le droit suisse	8
Bibliographie	9
Travaux législatifs	9

I. GÉNÉRALITÉS

- 1 Au cours des dernières décennies, la société a évolué en profondeur. De nombreux services se sont digitalisés. Les « smartphones » qui n'existaient pas il y a encore vingt ans, sont maintenant omniprésents dans la vie de tous. Conscientes de ce changement, les entreprises ont adapté leurs services à ces nouveaux appareils et proposent pour la grande majorité des **services en ligne**. Cette tendance de fond a encore été accélérée par la pandémie de coronavirus qui a frappé la population mondiale entre 2020 et 2022. Les mesures sanitaires mises en place par les autorités ont en effet sensiblement restreint les contacts entre individus. Le commerce a donc dû trouver de nouvelles façons de poursuivre son activité pour survivre.
- 2 Plus que jamais dans l'histoire de l'humanité, tous les acteurs de la société sont aujourd'hui **interconnectés**. Grâce à leurs *smartphones*, les individus peuvent accéder à leurs comptes « e-banking », faire du commerce en ligne, stocker des données dans les nuages ou visionner des vidéos en « streaming » depuis n'importe quel endroit du globe et en tout temps.
- 3 Cette interconnexion extrême crée cependant une **interdépendance** tout aussi importante. Cette réalité est parfaitement illustrée par la cyberattaque de grande ampleur qui a frappé l'Estonie, pendant plusieurs jours en 2007¹. L'un des pays les plus connectés au monde s'est ainsi retrouvé complètement paralysé. L'administration étatique, le système bancaire, le commerce : plus rien ne fonctionnait, ce qui a causé des dommages considérables à l'ensemble de la société. Aujourd'hui, encore plus qu'au début des années 2000, il est donc indispensable que les systèmes informatiques puissent fonctionner sans entrave.
- 4 Compte tenu des dommages considérables qu'une entrave au bon fonctionnement des systèmes informatiques peut causer, il était indispensable de protéger le bon fonctionnement de ces systèmes au moyen d'une **norme pénale**.

II. BIEN JURIDIQUEMENT PROTÉGÉ

- 5 Le bien juridique protégé par l'art. 5 CCC est le droit de l'exploitant et des usagers d'un système informatique ou d'un système de télécommunications à ce que celui-ci **fonctionne correctement**².

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Un système informatique

- 6 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, ...)
- 7 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.

1. Otis, pp 163-168.

2. Rapport explicatif de la Convention sur la cybercriminalité, n. 65.

B. Un comportement punissable

- 8 L'art. 5 CCC énumère sept comportements punissables : l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques. Cette liste est **exhaustive**. Les comportements qui entravent le bon fonctionnement du système informatique, mais qui ne figurent pas dans cette liste, ne sont donc pas punissables. Tel est par exemple le cas du déplacement de données à l'intérieur du système informatique, bien qu'il soit tout aussi néfaste que l'endommagement ou la détérioration de données.

1. L'introduction de données

- 9 La notion d'**introduction** doit être interprétée dans le sens où l'auteur introduit à l'intérieur du système informatique cible des données qui proviennent de l'extérieur de ce système. Certains auteurs vont même jusqu'à camoufler ces données en leur donnant l'apparence de fichiers tout à fait anodins, pour éviter qu'on ne les repère trop facilement. D'aspect extérieur, ces données semblent donc être des données originales du système.
- 10 L'art. 5 CCC ne s'étend toutefois pas à toutes les données introduites dans le système informatique, mais uniquement à celles **destinées à entraver** son bon fonctionnement. Il s'agit donc de données ou de programmes malveillants qui ralentissent, voire bloquent complètement le fonctionnement du système informatique. Ce résultat peut être atteint soit en activant une fonctionnalité qui ralentit ou bloque le processus de traitement des données, soit en désactivant une fonctionnalité nécessaire au bon fonctionnement du système informatique. A titre d'exemple, on peut citer l'installation d'un cheval de Troie qui permet à l'auteur de prendre le contrôle sur tout ou partie du système informatique ou l'installation d'un virus qui paralyse le processeur ou détruit un secteur de *boot*, empêchant ainsi l'ordinateur de redémarrer.

2. La transmission de données

- 11 Par « transmission de données » il faut comprendre l'**envoi** de données d'un système informatique vers un autre. Le comportement visé ici est l'envoi de données qui entrave le bon fonctionnement du système informatique. Les Parties ont en particulier voulu criminaliser les attaques par déni de service et par déni de service distribué. L'attaque par déni de service consiste à envoyer une quantité si importante de données à un système informatique cible que ce dernier n'arrive plus à les traiter toutes et fini par se bloquer.
- 12 Au fil du temps, les **performances** des systèmes informatiques, en particulier les serveurs, ont considérablement augmenté. Les techniques de répartition de charge³ et de haute disponibilité⁴ ont rendu les attaques par déni de service quasiment impossible à réaliser. Les cybercriminels ont donc fait évoluer l'attaque par déni de service en attaque par déni de service distribué. Cette attaque est similaire à la précédente à la différence près que l'auteur a sous son contrôle une multitude de systèmes informatiques auxquels il donne l'ordre d'envoyer simultanément de très grandes quantités de données au système informatique cible. Vu de la quantité de données qui proviennent de toute part, le système informatique cible ne parvient plus à les traiter toutes et finit par se bloquer. Actuellement ce type d'attaques est relativement répandu. Il est presque toujours lié à des demandes de rançon en échange de la cessation de l'attaque ou à une autre fraude telle que le vol de données.

3. Cette notion désigne le processus de répartition de l'ensemble des demandes sur plusieurs serveurs, dans le but d'en rendre le traitement plus efficace.

4. Ce terme est utilisé en informatique pour désigner des systèmes dont l'architecture en cascade a été conçue pour permettre à un système informatique de poursuivre l'activité effectuée par un autre système informatique si ce dernier venait à être indisponible. Plus les cascades sont nombreuses, plus la haute disponibilité du système est élevée.

Encore aujourd'hui, il n'existe pas de solution pour se défendre efficacement contre les attaques par déni de service distribué. De plus, le préjudice causé aux victimes est particulièrement important, puisqu'elles sont soit privées de l'utilisation de leur système informatique, soit appauvries par le paiement de la rançon.

3. L'endommagement, la détérioration et l'altération de données

- 13 L'intégrité des données est essentielle au bon fonctionnement des systèmes d'information. Son **importance** est telle qu'elle fait même l'objet d'une norme ISO⁵.
- 14 La notion d'**intégrité** des données se rapporte à la fiabilité, l'exactitude et l'exhaustivité des données. Des données dont l'intégrité est garantie sont des données qui n'ont pas été modifiées après leur enregistrement initial. A titre illustratif, on pourrait comparer la notion de garantie de l'intégrité des données à l'envoi d'un colis par la poste dont on certifie qu'il a véritablement été envoyé par l'expéditeur mentionné sur le paquet, que cet envoi a bien eu lieu à la date et à l'endroit indiqués sur le sceau postal, que le paquet n'a pas été ouvert au cours du trajet et que le contenu du paquet n'a pas été modifié après son envoi.
- 15 Il va de soi que le **contenu** des données, c'est-à-dire les informations que les données renferment (par exemple un texte, un code, une image, etc.), est tout aussi important que l'intégrité formelle des données. En plus de garantir l'intégrité formelle des données, il est donc indispensable de garantir aussi que le contenu des données n'a pas été corrompu. Dans l'exemple du paquet évoqué ci-dessus, l'intégrité formelle des données est représentée par l'emballage, alors que l'intégrité du contenu des données correspond à l'objet qui se trouve dans le paquet.
- 16 L'**endommagement** et la **détérioration** de données évoquées à l'art. 5 CCC sont des comportements qui se recoupent en matière informatique. Il s'agit dans les deux cas d'atteintes négatives à l'intégrité ou au contenu des données ou des programmes. Les données endommagées ou détériorées ne sont plus fiables, exactes et exhaustives. L'auteur modifie les données du système informatique cible afin qu'elles ne puissent plus être utilisées correctement lors du traitement de données. Il suffit par exemple de renommer un dossier contenant des fichiers essentiels au bon fonctionnement du système d'exploitation pour que l'ensemble du système informatique se bloque. La modification du code de programmation d'un logiciel permet également de bloquer son bon fonctionnement. Plus récemment, les cybercriminels cryptent les données et monnaient ensuite la clé de cryptage.
- 17 L'**altération** se rapporte à la modification de données existantes dans le système informatique, en tant que conséquence d'un autre acte accompli par l'auteur. Il s'agit d'un terme générique très large qui englobe l'ensemble des modifications apportées aux données, à savoir l'adjonction, le remplacement ou l'effacement de données. Ces modifications peuvent concerner tant l'intégrité formelle que du contenu des données. C'est notamment le cas des données modifiées à la suite de l'introduction d'un cheval de Troie ou l'installation d'un virus.

4. La suppression et l'effacement de données

- 18 Les données informatiques sont sauvegardées sur des supports d'enregistrement (p. ex. disque dur, DVD, clé USB, ...) dans l'ordre dans lequel elles sont créées. Pour pouvoir retrouver des données précises au moment où l'utilisateur en a à nouveau besoin, le système informatique établit une sorte d'**index** qui lui permet de savoir où se trouvent quelles données sur le support⁶.

5. Norme ISO 27001.

- 19 La **suppression** de données consiste à détruire totalement ou partiellement cet index qui permet de retrouver l'emplacement des données. Les données existent encore, mais le système informatique ne peut plus savoir où elles se trouvent sur le support et donc ne peut plus y avoir accès.
- 20 Contrairement à la suppression, l'**effacement** des données est une destruction définitive des données. Les données n'existent plus sur le support d'enregistrement.
- 21 Lorsque l'auteur supprime ou efface des données indispensables au bon fonctionnement du système informatique, telles que celles qui constituent le système d'exploitation, celui-ci devient **inutilisable** et cesse de fonctionner.

5. Le mode de commission

- 22 Les différents comportements qui viennent d'être examinés peuvent évidemment être commis directement par une personne physique. Cela prendrait toutefois beaucoup de temps. En pratique, les cybercriminels utilisent donc plutôt des maliciels ou des bots⁷ pour effectuer ces actes de façon **automatisée**. Le développement très rapide de l'intelligence artificielle va certainement rendre ce type d'agissements encore beaucoup plus simple à réaliser. WormGPT nous donne déjà un aperçu des possibilités fournies par l'intelligence artificielle, puisqu'il permet d'implémenter, dans d'autres systèmes informatiques, des contenus générés par l'intelligence artificielle qui était jusqu'à présent cantonnée à une *sandbox* informatique.
- 23 Se pose également la question de la **commission par omission**. La plupart du temps, les comportements punissables sont des actes commis par des cybercriminels qui cherchent à entraver le bon fonctionnement du système informatique dans le but d'obtenir quelque chose en échange. On peut toutefois aussi imaginer que le système informatique finisse par ne plus fonctionner correctement en raison du fait que son administrateur ne se charge pas de faire les mises à jour nécessaires. A notre avis, l'administrateur du système informatique est dans ce cas punissable, car, de part sa fonction, il a un devoir juridique d'agir et occupe donc une position de garant à l'égard de l'ayant-droit et des utilisateurs du système informatique.
- 24 Selon nous, la solution est identique dans le cas de l'administrateur du système informatique qui n'installe pas de **pare-feu** et/ou d'**antivirus** pour le protéger et laisse ainsi d'innombrables possibilités à des tiers de l'attaquer.

C. Une entrave grave au fonctionnement du système informatique

- 25 Pour se rendre coupable d'atteinte à l'intégrité du système, il ne suffit pas que l'auteur s'en prenne à l'intégrité des données contenues dans le système informatique, car dans ce cas, il s'agirait d'une atteinte à l'intégrité des données au sens de l'art. 4 CCC. Il faut que cet acte entrave gravement le fonctionnement du système informatique.
- 26 Il y a entrave au fonctionnement lorsque le système informatique ne fonctionne plus de manière optimale. Le texte de l'art. 5 CCC a été formulé de façon suffisamment **neutre** pour permettre de protéger de multiples fonctions⁸. Il est ainsi sans importance de savoir quelles fonctions sont entravées. Il est également indifférent que tout le système informatique soit entravé ou que seules certaines fonctions soient entravées.

6. Pour les systèmes formatés en NTFS on parle de « table de fichiers maître » ou MFT (*Master File Table*). Pour les systèmes utilisant l'ancien système de formatage FAT, il s'agissait d'une « table d'allocation de fichiers » ou FAT (*File Allocation Table*).

7. Application programmée pour effectuer une ou plusieurs tâches déterminées de manière automatisée.

8. Rapport explicatif de la Convention sur la cybercriminalité, n. 65.

- 27 Le système informatique est **entravé** dans son bon fonctionnement lorsqu'il est mis hors d'usage. Il est également entravé lorsqu'une application ne peut plus être utilisée. Cela peut se produire notamment parce que le code informatique du programme a été endommagé ou détruit, ou parce que les données que l'utilisateur avait sauvegardées ont été effacées, supprimées ou cryptées. L'entrave du système informatique peut aussi résulter de la diminution de ses performances. Tel est par exemple le cas lorsqu'un cybercriminel prend le contrôle à distance d'un système informatique et l'utilise comme machine-zombie à l'insu de son ayant-droit. Ce faisant, il utilise une partie des performances du système informatique sans l'accord de son ayant-droit, le plus souvent à des fins malveillantes. Enfin, le bon fonctionnement d'un système informatique peut être entravé par de trop fortes sollicitations. C'est le cas des attaques par déni de service ou par déni de service distribué. En soi, le système informatique fonctionne normalement, mais il est assailli de tant de requêtes simultanément qu'il ne peut pas les traiter assez vite et finit par se bloquer.
- 28 Compte tenu de la formulation de la norme, l'entrave doit résulter du comportement punissable. Etant donné que la liste figurant à l'art. 5 CCC est **exhaustive**, l'entrave doit nécessairement découler de l'un des comportements énumérés pour être punissable⁹. L'entrave qui résulterait d'un autre comportement, comme par exemple le déplacement de données à l'intérieur du système informatique, n'est pas punissable.
- 29 Quant au qualificatif « **grave** », il n'a volontairement pas été défini pour permettre à chaque Etat de le définir librement¹⁰. Pour les uns, l'entrave grave pourra se rapporter à un dommage minimum engendré par cette entrave. Pour les autres, il s'agira de l'importance de l'entrave, comme par exemple le blocage de toute connexion vers l'extérieur d'un système informatique. Les auteurs du projet « ont jugé "grave" l'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 (c'est le cas des programmes qui portent atteinte à des systèmes sous la forme d'un "déni de service", des codes malveillants, tels que les virus, qui interdisent ou ralentissent sensiblement le fonctionnement du système, ou des programmes qui envoient un énorme volume de courrier électronique à un destinataire afin de paralyser les fonctions de communication du système) »¹¹.

D. L'illicéité

- 30 Pour être punissable, l'auteur doit avoir agi **sans droit**. C'est l'ayant-droit du système informatique qui détermine qui a le droit d'administrer et d'utiliser le système informatique. Sont ainsi punissables, toutes les personnes qui n'ont pas été autorisées à apporter des modifications au fonctionnement du système informatique. Ne sont en revanche pas punissables, les personnes qui ont été autorisées, expressément ou par acte concluant, par l'ayant-droit, à modifier le fonctionnement du système informatique, ainsi que celles qui y sont autorisées par la loi ou par un contrat.
- 31 Jusqu'au début des années 2000, il était rare que le système d'exploitation ou une application nécessite une mise à jour. Au cours des deux dernières décennies, les **misés à jour** sont cependant devenues de plus en plus courantes. Aujourd'hui, elles constituent même la règle. Lors d'une mise à jour, une nouvelle version du programme est installée à la place de l'ancienne. Les données existantes sont donc effacées et de nouvelles données sont écrites et enregistrées sur le support d'enregistrement. Pour l'essentiel, les mises à jour contiennent des correctifs de l'application, des suppressions de *bugs* ou de nouvelles fonctionnalités. Il n'y a donc a priori aucune forme d'entrave au

9. Rapport explicatif de la Convention sur la cybercriminalité, n. 66.

10. Rapport explicatif de la Convention sur la cybercriminalité, n. 67.

11. Rapport explicatif sur la Convention sur la cybercriminalité, n. 67.

bon fonctionnement du système informatique. Il arrive toutefois que certaines mises à jour nécessitent un espace de stockage sur le disque dur plus important ou accaparent une plus grande partie de la mémoire vive ou des capacités du processeur. Le système informatique s'en trouve par conséquent ralenti. Il est donc entravé dans son bon fonctionnement. Dans la majorité des cas, cela ne pose pas de problèmes car le ralentissement du système informatique est très faible, voire insignifiant. Exceptionnellement, il arrive que des mises à jour bloquent le fonctionnement du système informatique, notamment parce que la version précédente de l'application sollicitait déjà le maximum des ressources disponibles et que la mise à jour exige plus de ressources que celles disponibles. Dans tous les cas, l'utilisateur doit avoir le choix d'installer ou de ne pas installer la mise à jour. Selon nous, l'éditeur de l'application se rend punissable s'il oblige l'utilisateur à installer une nouvelle version de l'application, à défaut de quoi le système informatique est entravé dans son bon fonctionnement, voire que l'application est rendue inutilisable.

- 32 Les comportements énumérés à l'art. 5 CCC ne sont pas non plus illicites lorsqu'ils ont été autorisés **contractuellement**. On pense ici notamment à l'administrateur du système informatique dont la mission est d'assurer la maintenance. Il n'est pas punissable, s'il effectue les mises à jour des programmes installés dans le système informatique. Il se rend en revanche punissable s'il profite de son statut pour porter atteinte au bon fonctionnement du système informatique, par exemple en désinstallant des programmes ou en effaçant des données.

E. L'intention

- 33 L'atteinte à l'intégrité du système est **intentionnelle**. L'intention doit porter sur tous les éléments objectifs de l'infraction. L'auteur doit donc avoir la conscience et la volonté de perturber le bon fonctionnement d'un système informatique sans y être autorisé.

IV. COMPARAISON AVEC LE DROIT SUISSE

- 34 Il n'existe **pas d'équivalent** à l'art. 5 CCC en droit suisse. Les différents comportements pourraient certes donner l'impression d'une similitude avec la détérioration de données (art. 144^{bis} ch. 1 CP). Tel n'est toutefois pas le cas pour trois raisons.
- 35 D'abord, les **biens juridiquement protégés** par les art. 5 CCC et 144^{bis} ch. 1 CP sont totalement différents. Comme expliqué ci-dessus, l'art. 5 CCC protège l'intérêt de l'exploitant et des utilisateurs d'un système informatique ou de télécommunications à ce que celui-ci soit en mesure de fonctionner correctement¹², alors que l'art. 144^{bis} ch. 1 CP assure un droit de disposition sur des données¹³. En d'autres termes, le premier garantit le bon fonctionnement d'un moyen de traitement des données, tandis que le second protège un droit réel particulier.
- 36 Compte tenu du fait que les biens juridiquement protégés ne sont pas les mêmes, les personnes **lésées** par ces deux infractions ne sont pas non plus identiques. La personne lésée par la détérioration de données (art. 144^{bis} ch. 1 CP) est le titulaire des données détériorées. En revanche, l'atteinte à l'intégrité du système (art. 5 CCC) lèse l'ayant-droit du système informatique.
- 37 Ensuite, bien que ces deux infractions partagent de nombreux points communs, elles ne peuvent **pas** être **assimilées**. En effet, l'atteinte à l'intégrité du système (art. 5 CCC) doit en quelque sorte être perçue comme une forme spéciale de la détérioration de données (art. 144^{bis} ch. 1 CP), car elle

12. Rapport explicatif de la Convention sur la cybercriminalité, n. 65.

13. ATF 129 IV 230 consid. 2.1.1 ; Schmid, § 6 n. 14 ; Trechsel / Cramer, n. 2 ad art. 144^{bis} CP ; Weissenberg, n. 6 ad art. 144^{bis} CP.

requiert que l'atteinte à l'intégrité des données cause une entrave grave au fonctionnement du système informatique. Il s'agit d'un élément constitutif supplémentaire qui n'est pas exigé par le droit suisse.

- 38 Enfin, certains **comportements** tombent sous le coup de l'art. 5 CCC alors qu'ils ne sont pas punissables en vertu de l'art. 144^{bis} ch. 1 CP. C'est notamment le 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 »¹⁴. Ces actes ne sont pas non plus correctement réprimés par l'art. 179^{septies} CP (utilisation abusive d'une installation de télécommunication) pour trois raisons. Premièrement, parce que l'art. 179^{septies} CP exige un dessein spécial – à savoir la méchanceté ou l'espièglerie – en plus de l'intention, ce qui n'est pas le cas de l'art. 5 CCC. Ensuite, en raison du fait que l'utilisation abusive d'une installation de télécommunication ne constitue qu'une contravention et n'est donc punie que d'une amende. Or, l'art. 13 § 1 CCC stipule expressément que les infractions réprimées par les art. 2 à 11 CCC doivent être passibles de sanctions comprenant des peines privatives de liberté. Troisièmement, parce la complicité et la tentative d'atteinte à l'intégrité du système sont punissables en vertu de l'art. 11 CCC, alors que la complicité et la tentative d'utilisation abusive d'une installation de télécommunication ne sont pas punissables, étant donné qu'il s'agit d'une contravention (cf. art. 105 al. 2 CP).
- 39 Au vu de ce qui précède, force est de constater que le droit suisse n'est **pas conforme** à l'art. 5 CCC. Il devrait donc être adapté.

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

BIBLIOGRAPHIE

Ottis Rain, Analysis of the 2007 Cyber Attacks against Estonia from the information warfare perspective, in : Proceedings of the 7th European Conference on information warfare and security, Plymouth, 2008, pp 163-168, disponible à <https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/>, visité le 02.11.2023

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

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

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 21.01.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

14. Rapport explicatif de la Convention sur la cybercriminalité, n. 67.