



COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

COMMENTAIRE

Art. 4 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: 10.17176/20240217-132836-0

PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 4 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 4 CCC N. XXX.

Art. 4 Atteinte à l'intégrité des données

¹ Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

² Une Partie peut se réserver le droit d'exiger que le comportement décrit au par. 1 entraîne des dommages sérieux.

TABLE DES MATIÈRES

I. Généralités	3
II. Bien juridiquement protégé.....	3
III. Éléments constitutifs de base	3
A. Des données informatiques.....	3
B. Un comportement punissable	3
1. La suppression et l'effacement de données	4
2. L'endommagement, la détérioration et l'altération de données	4
3. Le mode de commission	5
C. L'illicéité	5
D. L'intention	6
IV. Élément constitutif supplémentaire facultatif.....	6
V. Comparaison avec le droit suisse.....	7
Bibliographie	8
Travaux législatifs.....	8

I. GÉNÉRALITÉS

- 1 Au cours des vingt dernières années, la société dans son ensemble a effectué une **transition** vers le monde numérique. Une grande partie du commerce se déroule en ligne, les transactions financières se font via *e-banking*, les autorités, les entreprises et les particuliers stockent de grandes quantités d'informations dans des ordinateurs personnels, sur des serveurs ou même dans des *clouds*. Malgré l'ampleur des changements déjà accomplis, cette évolution semble loin d'être terminée. Il est en effet très probable que la société continue à se digitaliser encore davantage dans les décennies à venir.
- 2 Les **documents** numériques remplacent peu à peu les documents papier. Suivant cette même tendance, les documents qui font foi sont de plus en plus ceux au format électronique.
- 3 Au vu de l'importance croissante des données informatiques dans le monde numérique, il se justifiait de les protéger contre des actes malveillants. Alors que les art. 2 et 3 CCC protègent la confidentialité des données, l'art. 4 CCC a pour but d'assurer la protection de l'**intégrité** et la **disponibilité** des données.

II. BIEN JURIDIQUEMENT PROTÉGÉ

- 4 L'art. 4 CCC vise à assurer aux données et programmes informatiques une protection analogue à celle dont bénéficient les biens corporels à l'encontre des dommages occasionnés intentionnellement. Les intérêts juridiques protégés par cette disposition sont, d'une part, l'**intégrité** des données et des programmes informatiques et, d'autre part, le **bon fonctionnement** ou le bon usage des données et des programmes informatiques¹.

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Des données informatiques

- 5 Aux termes de l'art. 1 let. b CCC, « l'expression "données informatiques" désigne toute **représentation** de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ». La notion de données informatiques est donc très large puisqu'elle englobe notamment toutes les lettres, symboles ou codes de programmation qui peuvent être introduits, traités et stockés par un système informatique.
- 6 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 comportement punissable

- 7 Pour qu'un système informatique puisse fonctionner correctement, les données qu'il traite doivent être disponibles et intègres. Afin de garantir ces deux aspects, l'art. 4 CCC énumère cinq comportements punissables. La répression de la suppression et de l'effacement de données vise à protéger la disponibilité des données. La criminalisation de l'endommagement, de la détérioration et de l'altération a quant à elle pour but d'assurer la protection de l'intégrité des données. Cette liste de comportements est **exhaustive**. Elle couvre néanmoins l'ensemble des comportements nuisibles possibles.

1. Rapport explicatif de la Convention sur la cybercriminalité, n. 60.

1. La suppression et l'effacement de données

- 8 Informatiquement, les données se traduisent en **langage binaire** par une succession de « 0 » et de « 1 ». C'est sous cette forme que les données sont traitées et stockées. Lorsque l'utilisateur enregistre des données, le système informatique sauvegarde la série de « 0 » et de « 1 » correspondant à ces données à un espace encore vide du support d'enregistrement (p. ex. disque dur, DVD, clé USB, ...). Afin de retrouver ces données au moment où l'utilisateur en aura à nouveau besoin, le système informatique dispose d'une sorte de plan qui lui permet de savoir où se trouvent quelles données sur le support².
- 9 La **suppression** de données consiste à détruire le moyen de retrouver l'emplacement des données. Les données existent encore, mais l'utilisateur ne peut plus déterminer leur emplacement sur le support et ne peut donc plus y avoir accès. Le système informatique considère que l'espace sur le support est libre et enregistre par conséquent les nouvelles données sur les données supprimées. Le seul moyen pour récupérer les données supprimées est d'utiliser un programme de récupération de données le plus vite possible. Ce programme lit l'intégralité du support et reconstitue un plan du support d'enregistrement pour localiser les données. Cela permet de récupérer les données avant que d'autres ne soient enregistrées par-dessus.
- 10 Contrairement à la suppression, l'**effacement** des données est une destruction définitive des données. Les données n'existent plus sur le support d'enregistrement. Elles ne sont en principe plus récupérables³.

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

- 11 L'intégrité des données est tout aussi essentielle au bon fonctionnement des systèmes d'information que la disponibilité des données. Son importance est si grande qu'elle fait même l'objet d'une norme ISO⁴. La notion d'**intégrité** des données se rapporte à leur fiabilité, leur exactitude et leur exhaustivité. En d'autres termes, des données dont l'intégrité est garantie sont des données qui n'ont pas été modifiées après leur enregistrement initial. La notion d'intégrité des données concerne à la fois le contenu des données et leur forme.
- 12 Dans le monde réel, la notion de garantie de l'intégrité des données peut être comparée à l'envoi d'un **colis** par la poste, dont on certifie qu'il émane véritablement de l'expéditeur indiqué sur le paquet, que l'envoi a bien eu lieu à la date et à l'endroit mentionnés sur le sceau postal, que le paquet n'a pas été ouvert, que son contenu est bien celui qui a été envoyé par l'expéditeur et que rien n'a été enlevé ou rajouté dans le paquet après son envoi.
- 13 Dans ce contexte, l'« **endommagement** » et la « **détérioration** » de données sont des notions qui se recoupent. Elles décrivent des atteintes négatives à la forme ou au contenu des données ou des programmes. Les données endommagées ou détériorées ne sont par conséquent plus fiables, exactes et exhaustives. On ne peut donc plus être sûr qu'elles proviennent de l'expéditeur dont elles semblent émaner, qu'ils s'agit bel et bien des données qui ont été envoyées par l'expéditeur et qu'aucune donnée n'a été supprimée, ajoutée ou modifiée.
- 14 Quant à l'« **altération** », elle se réfère à une modification de données existantes⁵. Cette modification peut concerner tant la forme que le contenu des données. Il s'agit d'un terme très large qui englobe

2. 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).

3. Certains programmes particuliers permettent de reconstituer des données à partir de traces magnétiques qui subsistent sur les disques durs magnétiques, mais les chances de succès sont minces.

4. Norme ISO 27001.

l'ensemble des actions effectuées sur des données par lesquelles on ajoute, remplace ou supprime un ou des éléments.

3. Le mode de commission

- 15 Les différents comportements qui viennent d'être examinés peuvent être commis directement par l'auteur. Il est toutefois aussi possible d'utiliser un *bot*⁶ pour accomplir ces actes. Cela présente l'avantage que l'auteur n'a qu'à donner ses instructions une seule fois au programme, qui répète ensuite automatiquement les actions demandées autant de fois que nécessaire. Il est par ailleurs à craindre que le développement de l'intelligence artificielle rende ce travail encore beaucoup plus simple et efficace à l'avenir. WormGPT est sans doute le précurseur d'une nouvelle forme de commission d'infractions, car il permet d'implémenter dans d'autres systèmes informatiques des contenus générés par l'intelligence artificielle, alors que cette dernière était pour l'instant cantonnée à une *sandbox* informatique.
- 16 Cela étant, même sans recourir à un *bot*, l'**intelligence artificielle** offre déjà actuellement d'innombrables possibilités pour modifier des données. On peut par exemple très facilement lui demander de réécrire un texte en remplaçant une idée par une autre, ou de modifier une image en substituant un élément par un autre. A l'avenir, distinguer les données authentiques des données modifiées deviendra donc de plus en plus difficile.
- 17 Dans la grande majorité des cas, les atteintes à l'intégrité des données sont réalisées par la commission d'un comportement punissable. Des atteintes à l'intégrité des données peuvent toutefois aussi survenir à cause d'une protection insuffisante du système informatique. A notre avis, il peut dans ce genre de cas y avoir une **commission par omission** de la part de l'administrateur du système informatique puisque, de part sa fonction, il a un devoir juridique d'agir et qu'il occupe donc une position de garant à l'égard de l'ayant-droit des données.

C. L'illicéité

- 18 Pour être punissable, l'auteur doit avoir agi **sans droit**. C'est l'ayant-droit des données qui détermine qui est autorisé à les modifier. Sont ainsi punissables toutes les personnes qui n'ont pas été autorisées à modifier ces données. Ne sont en revanche pas punissables les personnes qui ont été autorisées, expressément ou par acte concluant, à modifier ces données par l'ayant-droit ou qui y sont autorisées par la loi ou par un contrat.
- 19 De nos jours, il est courant que des modifications de données se fassent par **acte concluant**. Tel est par exemple le cas à chaque fois que des messages sont échangés par messageries instantanées telles que *WhatsApp*, *Telegram* ou *Threema*. Toutes ces applications cryptent les données avant de les envoyer et les décryptent lors de leur réception. Il s'agit d'une modification de données. Celle-ci est toutefois licite, d'une part, parce qu'elle est acceptée par les utilisateurs par acte concluant et, d'autre part, en raison du fait qu'elle assure la confidentialité des données.
- 20 Un autre cas de modification de données par acte concluant réside dans les **misés à jour** d'applications. 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. Ce processus est licite, pour autant que l'utilisateur ait le choix d'installer ou de ne pas installer la mise à jour. A notre avis, l'éditeur de l'application qui oblige

5. Rapport explicatif de la Convention sur la cybercriminalité, n. 61.

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

l'utilisateur à installer une nouvelle version de l'application, faute de quoi elle devient inutilisable, ou les données illisibles, se rend punissable.

- 21 S'agissant des actes autorisés par la loi, certaines législations nationales contiennent des exceptions à la garantie d'intégrité des données. Elles permettent notamment aux autorités de poursuite pénale ou aux services de renseignements d'installer des *govwares* dans des systèmes informatiques afin de surveiller l'activité des personnes qui les utilisent, par exemple pour découvrir l'auteur d'une infraction ou obtenir des informations utiles à la protection de l'Etat. L'installation de ces programmes espions n'est pas illégale tant qu'elle est effectuée dans le cadre strict posé par la loi. Une surveillance ne peut toutefois être opérée que dans des cas graves et doit être soumise à un contrôle judiciaire postérieur⁷.
- 22 La modification de données n'est pas non plus illicite lorsqu'elle a été autorisée **contractuellement**. On pense ici notamment à l'administrateur du système informatique qui est chargé de 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 effacer ou modifier les données d'un utilisateur sans son autorisation.
- 23 De la même façon, l'informaticien mandaté pour réaliser des **tests d'intrusion** dans un système informatique n'est pas punissable s'il modifie des données pour créer une brèche dans les défenses mises en place pour protéger l'accès au système informatique. En revanche, le *hacker* qui, sans autorisation, agit de la même manière est punissable.

D. L'intention

- 24 L'atteinte à l'intégrité des données est **intentionnelle**. L'intention doit porter sur tous les éléments objectifs de l'infraction. L'auteur doit donc avoir conscience qu'il détériore des données de manière indue et en avoir la volonté. Le dol éventuel suffit.

IV. ÉLÉMENT CONSTITUTIF SUPPLÉMENTAIRE FACULTATIF

- 25 L'art. 4 § 2 CCC autorise les Etats parties à émettre une **réserve** et à ne poursuivre que les comportements ayant entraîné un préjudice grave.
- 26 Le texte ne définit pas la notion de « préjudice grave ». Quant au rapport explicatif, il indique simplement que chaque Etat est libre d'interpréter cette notion comme il le souhaite⁸. Les Parties ont toutefois opté pour la notion de préjudice (*harm*) plutôt que de dommage (« damage »). On comprend donc que le **préjudice** ne se limite pas uniquement à l'aspect économique. Le préjudice peut donc aussi correspondre au temps de travail nécessaire à la récupération ou à la recreation des données, de même qu'aux conséquences de la disparition ou de l'impossibilité d'utiliser les données.
- 27 Les Parties ont aussi précisé que le préjudice devait être **grave**. Cet adjectif, mis en relation avec la notion de préjudice, signifie qu'il doit être d'une certaine ampleur. On peut donc imaginer que le préjudice doit représenter une somme d'argent conséquente, un nombre d'heures de travail important ou avoir de lourdes conséquences.
- 28 L'Azerbaïdjan, la Lituanie, la République slovaque, le Chili et les Etats-Unis d'Amérique ont fait usage de la possibilité donnée par l'art. 4 § 2 CCC. L'**Azerbaïdjan**, la **Lituanie**, la **République slovaque** et les **Etats-Unis d'Amérique** ont précisé que dans leur droit interne, la notion de préjudice grave

7. Arrêt CourEDH Szabó et Vissy contre Hongrie du 12 janvier 2016 (37138/14).

8. Rapport explicatif de la Convention sur la cybercriminalité, n. 64.

devait être interprétée comme ayant causé des dommages sérieux⁹. Le Code pénal slovaque a depuis été modifié. Le § 247 a été remplacé par le § 247b. Dans sa forme simple, la survenance d'un préjudice grave n'est plus exigée (§ 247b par. 1). En revanche, la réalisation d'un préjudice grave est devenue une forme qualifiée de l'infraction (§ 247b par. 2 let. a). Le **Chili** a quant à lui parlé de dommages graves¹⁰. On constate donc que même si la lettre de la convention permettait une interprétation très large, tous les Etats qui ont fait usage de la possibilité offerte par l'art. 4 § 2 CCC ont limité la notion de préjudice au seul aspect économique.

- 29 Il est à cet endroit intéressant de relever la manière originale dont le droit **suisse** a traité la question du préjudice grave. Au lieu de limiter la poursuite pénale aux comportements qui ont causé un préjudice grave, l'art. 144^{bis} ch. 1 al. 2 CP prévoit au contraire une forme qualifiée lorsque le dommage causé par l'auteur est considérable.

V. COMPARAISON AVEC LE DROIT SUISSE

- 30 En droit suisse l'atteinte à l'intégrité des données (art. 4 CCC) trouve son pendant à l'art. 144^{bis} ch. 1 CP. Les **intérêts juridiques protégés** par ces deux normes ne sont toutefois pas strictement identiques puisque l'art. 4 CCC protège l'intégrité et le bon fonctionnement ou le bon usage de données ou programmes informatiques enregistrés, alors que l'art. 144^{bis} ch. 1 CP protège le droit de disposer de données intactes¹¹. Ils sont toutefois très proches et se rejoignent dans leur finalité.
- 31 En ce qui concerne les **comportements** réprimés par l'art. 4 CCC, ils se retrouvent tous à l'art. 144^{bis} ch. 1 CP. Les notions d'« endommagement », de « détérioration » et d'« altération » qui figurent à l'art. 4 CCC sont couvertes par le terme « modifie » qui comprend toutes les formes de transformation¹². La notion d'« effacement » évoquée dans la convention, à savoir la destruction définitive de données, est identique en droit suisse¹³. Enfin, la « suppression » de données qui figure à l'art. 4 CCC est couverte par les termes « met hors d'usage », qui englobe tous les comportements par lesquels l'ayant-droit est empêché d'utiliser correctement ses données¹⁴.
- 32 Enfin, l'art. 144^{bis} ch. 1 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

9. 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. 273.1 du Code pénal arzerbaidjanais ; Réserve 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=2&codePays=LIT>, visité le 21.1.2024), en lien avec l'art. 198² du Code pénal lituanien ; Réserve consignée dans l'instrument de ratification déposé le 8 janvier 2008, retirée dans un instrument du Ministre des Affaires étrangères de la République slovaque transmis par la Représentation Permanente de la République slovaque et enregistrés par le Secrétariat Général le 30 avril 2021 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=SLK>, visité le 21.1.2024), en lien avec le § 247 de l'ancien Code pénal slovaque ; Réserve 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>, visitée le 21.1.2024), en lien avec le titre 18 § 1030 section a chiffre 5 lettre C du Code des Etats-Unis (Computer Fraud and Abuse Act).

10. 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 l'art. 4 de la Loi chilienne N° 21.459 sur les délits informatiques.

11. Schmid, § 6 n. 14 ; Trechsel / Cramer, n. 2 ad art. 144^{bis} CP ; Weissenberg, n. 6 ad art. 144^{bis} CP.

12. Corboz, n. 5 ad art. 144^{bis} CP ; Schmid, § 6 n. 26 ; Trechsel / Cramer, n. 5 ad art. 144^{bis} CP ; Weissenberg, n. 21-22 ad art. 144^{bis} CP.

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 la détérioration de données d'office dans tous les cas¹⁵ ou alors de déposer une déclaration qui limiterait la poursuite aux cas dans lesquels le dommage engendré est considérable.

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

Corboz Bernard, Les infractions en droit suisse, vol. I, 3. éd., Berne 2010

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

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

14. Corboz, n. 5 ad art. 144^{bis} CP ; Schmid, § 6 n. 29 ; Trechsel / Cramer, n. 7 ad art. 144^{bis} CP ; Weissenberg, n. 33 ad art. 144^{bis} CP.

13. Corboz, n. 5 ad art. 144^{bis} CP ; Schmid, § 6 n. 27 ; Trechsel / Cramer, n. 6 ad art. 144^{bis} CP ; Weissenberg, n. 8 ad art. 144^{bis} CP.

15. Schwarzenegger, p. 317.