



COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

COMMENTAIRE

Art. 8 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: 10.17176/20240217-133626-0

PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 8 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 8 CCC N. XXX.

Art. 8 Fraude informatique

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 de causer un préjudice patrimonial à autrui:

- a. par toute introduction, altération, effacement ou suppression de données informatiques;
- b. par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

TABLE DES MATIÈRES

I. Généralités	3
II. Bien juridiquement protégé.....	3
III. Éléments constitutifs de base	3
A. Un système informatique	3
B. Des données informatiques.....	3
C. Un comportement punissable.....	3
1. Une manipulation de données	4
a. L'introduction de données	4
b. L'altération, la suppression et l'effacement de données	4
2. Une atteinte au fonctionnement du système informatique	4
D. Un préjudice patrimonial.....	5
E. L'illicéité.....	5
F. L'intention	5
G. Un dessin spécial.....	5
IV. Comparaison avec le droit suisse	6
Bibliographie	7
Travaux législatifs	7

I. GÉNÉRALITÉS

- 1 L'évolution de l'informatique et son implantation dans **tous les domaines**, spécialement celui du transfert d'argent, ont transformé ce secteur en véritable paradis pour la criminalité économique. La facilité avec laquelle les infractions peuvent être commises et la quasi-absence de risque d'être poursuivi pénalement ont favorisé le transfert d'infractions économiques « traditionnelles » vers Internet. Afin de lutter contre cette forme de délinquance, l'art. 8 CCC érige en infraction « toute manipulation abusive au cours d'un traitement de données en vue d'effectuer un transfert illicite de propriété »¹.

II. BIEN JURIDIQUEMENT PROTÉGÉ

- 2 Cette disposition protège les systèmes informatiques contre des **manipulations frauduleuses** effectuées dans le but de créer un préjudice patrimonial à autrui et d'en retirer un profit.

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Un système informatique

- 3 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, ...).
- 4 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. 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.

C. Un comportement punissable

- 7 L'art. 8 CCC énumère plusieurs comportements punissables et les subdivise en **deux catégories**. La première concerne la manipulation de données, tandis que la seconde se rapporte à l'atteinte au fonctionnement du système informatique.

1. Rapport explicatif sur la Convention sur la cybercriminalité, n. 86.

1. Une manipulation de données

a. L'introduction de données

- 8 L'**introduction** de données a le même sens qu'aux art. 4, 5 et 7 CCC². Il s'agit donc de l'acte par lequel l'auteur introduit à l'intérieur d'un système informatique des données qui proviennent de l'extérieur de ce système. L'art. 8 CCC ne sanctionne toutefois pas l'introduction de n'importe quelles données, mais uniquement celles qui sont de nature à causer un préjudice patrimonial.
- 9 Il y a notamment introduction de données lorsque l'auteur, sans y être autorisé, insère une **carte de débit** dans un *bancomat* et entre le numéro d'identification personnel en vue de procéder à un retrait d'argent, ou lorsque l'auteur se connecte à un portail de *e-banking*, à la place d'un tiers, au moyen d'un identifiant et d'un mot de passe qu'il a dérobé et qu'il procède indument à un transfert d'argent.

b. L'altération, la suppression et l'effacement de données

- 10 Les notions d'altération, de suppression et d'effacement de données sont **identiques** à celles des art. 4, 5 et 7 CCC³.
- 11 Il y a altération de données lorsque l'auteur porte atteinte à l'**intégrité** des données, c'est-à-dire à leur fiabilité, leur exactitude et leur exhaustivité. Tel est par exemple le cas lorsque l'auteur modifie les métadonnées d'un paiement lors d'une transaction en ligne, ce qui a pour conséquence de faire rediriger les fonds par le système informatique de la banque vers un compte appartenant à l'auteur plutôt que vers le compte du destinataire initial.
- 12 Les données sont aussi altérées lorsque l'auteur s'en prend à leur **contenu**. On peut par exemple penser au cas dans lequel l'auteur modifie en arrière-plan les coordonnées bancaires ou le montant d'un ordre de paiement sur une plateforme d'« e-banking » sans que l'utilisateur ne s'en aperçoive, de sorte que le paiement est plus élevé que prévu et/ou n'est pas crédité sur le compte prévu.
- 13 L'auteur **supprime** des données lorsqu'il en entrave le libre accès. L'auteur empêche le système informatique d'avoir un accès complet à toutes les données auxquelles il devrait avoir accès. C'est le cas de l'auteur qui, disposant d'une limite de crédit auprès d'un organisme de carte de crédit, supprime les données relatives à cette limite dans le système informatique de cet organisme, afin de lui permettre de continuer à effectuer des paiements à crédit, tout en sachant qu'il n'aura pas les moyens de les rembourser.
- 14 L'**effacement** de données enfin est une destruction définitive des données. Elles n'existent donc plus. On peut ici penser à l'auteur qui accède au système informatique de son créancier et qui efface toutes les données en lien avec la somme qu'il doit, ou à celui qui, au cours d'enchères en ligne, efface les offres les plus élevées et les remplace par sa propre offre à un prix bien moindre.

2. Une atteinte au fonctionnement du système informatique

- 15 Pour s'assurer de n'oublier aucun comportement frauduleux, l'art. 8 let. b CCC envisage également, de façon générale, « **toute forme d'atteinte** au fonctionnement d'un système informatique ». Cette formulation se rapporte à des actes tels que les manipulations de matériel, les actions empêchant les sorties sur imprimante et les actes affectant les enregistrements ou les flux de données, ainsi que l'ordre dans lequel les programmes sont exécutés⁴.

2. Rapport explicatif de la Convention sur la cybercriminalité, n. 87.

3. Rapport explicatif de la Convention sur la cybercriminalité, n. 87.

4. Rapport explicatif de la Convention sur la cybercriminalité, n. 87.

- 16 Contrairement aux comportements réprimés par l'art. 5 CCC l'atteinte au fonctionnement du système informatique ne doit pas nécessairement être **grave**. Elle doit en revanche être destinée à causer un préjudice patrimonial.
- 17 A titre d'**exemple**, on peut citer la manipulation d'un terminal de paiement par carte bancaire qui confirmerait un paiement au vendeur, alors que celui-ci n'a en réalité pas été opéré sur le compte à débiter.

D. Un préjudice patrimonial

- 18 Les comportements qui viennent d'être évoqués ne sont punissables que s'ils engendrent un **préjudice patrimonial** à autrui. Ce préjudice peut être économique ou matériel il s'agit donc d'une notion très large qui englobe à la fois les liquidités et les immobilisations corporelles ou incorporelles ayant une valeur économique⁵. Plus généralement, on peut le définir comme toute lésion du patrimoine sous la forme d'une diminution de l'actif, d'une augmentation du passif, d'une non-augmentation de l'actif ou d'une non-diminution du passif.
- 19 Le texte de l'art. 8 CCC ne fixe pas de **montant minimal** quant au préjudice patrimonial causé. Un préjudice, même minime, suffit.
- 20 Il n'est pas non plus exigé que le préjudice soit définitif. Un **préjudice temporaire** ou provisoire peut suffire. Une transaction bancaire opérée frauduleusement qui crée un préjudice financier au titulaire du compte qui a été débité, mais qui, par la suite, est corrigé lorsque la fraude est révélée, réalise l'infraction.

E. L'illicéité

- 21 L'auteur doit agir **sans droit**, c'est-à-dire sans y avoir été autorisé par l'ayant-droit, par la loi ou par un contrat.
- 22 La personne à laquelle l'ayant-droit **confie** son identifiant et son mot de passe afin qu'elle procède à un versement par « e-banking » n'agit pas sans droit, tant qu'elle ne fait qu'exécuter strictement les instructions qu'elle a reçues. Si elle profite de ses accès pour augmenter le montant du virement ou modifier l'identité du bénéficiaire, elle agit en revanche sans droit.
- 23 L'administrateur d'un portail de « e-banking » ou d'un magasin en ligne qui a pour mission d'en effectuer la **maintenance** n'est pas punissable, s'il modifie des données ou empêche temporairement le site web de fonctionner. En revanche, s'il profite de ses accès, par exemple pour modifier les données dans le compte d'un client, il se rend coupable de fraude informatique.

F. L'intention

- 24 La fraude informatique est **intentionnelle**. L'intention doit porter sur tous les éléments constitutifs objectifs, c'est-à-dire à la fois sur le comportement punissable et sur la survenance d'un préjudice patrimonial.

G. Un dessin spécial

- 25 En plus de l'intention, l'art. 8 CCC exige que l'auteur agisse dans un dessin de se procurer ou de procurer un tiers un bénéfice économique. La notion de **bénéfice économique** ne doit selon nous pas être comprise dans le sens étroit qui lui est donné en comptabilité. Elle englobe au contraire

5. Rapport explicatif de la Convention sur la cybercriminalité, n. 88.

l'ensemble des avantages économiques qui permettent un enrichissement. En d'autres termes, il s'agit de toute amélioration de la situation patrimoniale.

- 26 On pense avant toute chose à une augmentation de l'actif, une diminution du passif, une non-diminution de l'actif ou une non-augmentation du passif. Dans ces hypothèses, l'**enrichissement** correspond par exemple au prix de la marchandise livrée mais non payée, à la somme détournée d'un compte bancaire ou encore au montant de la prestation obtenue aux frais d'autrui.
- 27 La notion de bénéfice économique est à notre avis encore plus large et s'étend également à **tout avantage patrimonial**. Tel est le cas de l'auteur qui peut utiliser une plateforme de « streaming » payante sans bourse délier, de celui qui, lors d'une réservation en ligne, fournit à titre de garantie le numéro de carte de crédit d'un tiers pour ne pas avoir à supporter lui-même le risque de voir la sienne être débitée en cas d'annulation tardive ou encore de la personne qui utilise les coordonnées d'un tiers, comme par exemple un étudiant ou un retraité, pour obtenir – à prix réduit – des prestations qu'il aurait dû payer au prix plein.
- 28 Le bénéfice économique visé par l'auteur doit aussi être obtenu **sans droit**. Si l'auteur a ou croit avoir une prétention patrimoniale correspondant à l'enrichissement obtenu, il n'agit pas sans droit et n'est donc pas punissable. De même, les activités commerciales concurrentes qui peuvent causer un préjudice économique à une personne et apporter un bénéfice à une autre, mais qui ne sont pas pratiquées dans une intention frauduleuse ou malhonnête, telle que l'utilisation de programmes de collecte d'informations pour faire jouer la concurrence sur Internet, ne constituent pas une fraude informatique⁶.

IV. COMPARAISON AVEC LE DROIT SUISSE

- 29 En droit suisse, la norme qui se rapproche le plus de l'art. 8 CCC est l'**art. 147 CP**. Cette disposition ne correspond toutefois pas aux exigences de l'art. 8 CCC sur plusieurs points.
- 30 En premier lieu, les **biens juridiques protégés** par ces deux normes sont différents. L'art. 8 CCC protège les systèmes informatiques contre des manipulations frauduleuses effectuées dans le but de créer un préjudice patrimonial à autrui et d'en retirer un profit. L'art. 147 CP protège, au contraire, uniquement le patrimoine, à l'exclusion de l'intérêt de l'exploitant d'un système informatique à ce que ce dernier soit utilisé correctement⁷.
- 31 En ce qui concerne les **comportements** punissables, l'art. 147 CP réprime l'utilisation de données incorrecte⁸, incomplète⁹ ou induite¹⁰. Ceux-ci se recoupent en grande partie avec les notions d'introduction, d'altération, d'effacement ou de suppression de données informatiques mentionnées à l'art. 8 CCC. L'art. 147 CP laisse toutefois une importante brèche ouverte puisqu'elle ne sanctionne pas la suppression de données qui auraient dû se trouver dans le système informatique¹¹.
- 32 Enfin, l'art. 147 CP ne sanctionne que la fraude informatique causée par une **manipulation de données**¹². Le comportement mentionné à l'art. 8 let. b CCC ne tombe donc pas sous le coup de l'art.

6. Rapport explicatif de la Convention sur la cybercriminalité, n. 90.

7. ATF 129 IV 22 consid. 4.2.

8. ATF 129 IV 315, consid. 2.1 ; Corboz, n. 4 ad art. 147 CP ; Fiolka, n. 9 ad art. 147 CP ; Schmid, § 7 nn. 45ss ; Stratenwerth / Bommer, BT I, § 16 n. 6 ; Trechsel / Cramer, 2008, n. 4 ad art. 147 CP.

9. Corboz, 2010, n. 5 ad art. 147 CP ; Fiolka, n. 10 ad art. 147 CP ; Schmid, § 7 nn. 54ss ; Stratenwerth / Bommer, BT I, § 16 n. 6 ; Trechsel / Cramer, 2008, n. 5 ad art. 147 CP.

10. ATF 129 IV 315, consid. 2.1 ; Corboz, 2010, n. 6 ad art. 147 CP ; Fiolka, n. 11 ad art. 147 CP ; Schmid, § 7 nn. 61ss ; Stratenwerth / Bommer, BT I, § 16 n. 7 ; Trechsel / Cramer, 2008, n. 6 ad art. 147 CP.

11. Fiolka, n. 10 ad art. 147 CP.

147 CP. Ce point est particulièrement problématique, car de nombreux actes échappent à la répression, alors que la Suisse s'est engagée à les poursuivre.

- 33 Force est de constater que le droit suisse n'est **pas conforme** à l'art. 8 CCC et devrait dès lors être adapté.

BIBLIOGRAPHIE

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

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

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

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

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)