



COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

COMMENTAIRE

Art. 7 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: 10.17176/20240217-133431-0

PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 7 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 7 CCC N. XXX.

Titre 2: Infractions informatiques

Art. 7 Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

TABLE DES MATIÈRES

I. Généralités	3
II. Bien juridiquement protégé.....	3
III. Éléments constitutifs de base	3
A. Des données informatiques.....	3
B. Des données pertinentes dans les relations juridiques	3
C. Un comportement punissable.....	4
1. L'introduction de données.....	5
2. L'altération, la suppression et l'effacement de données	5
D. L'illicéité	6
E. L'intention.....	6
IV. Éléments constitutif supplémentaire facultatif.....	6
V. Comparaison avec le droit suisse.....	7
Travaux législatifs.....	7

I. GÉNÉRALITÉS

- 1 Compte tenu de l'omniprésence de l'informatique dans la société, un faux dans les titres informatiques est aussi dangereux qu'un faux dans les titres sur papier. Cette disposition a donc pour but d'instituer une infraction qui soit le pendant de la **falsification** des documents sur papier. Elle vise à combler les lacunes du droit pénal liées à la falsification classique, qui requiert la lisibilité visuelle des déclarations contenues dans un document et ne s'applique pas aux données enregistrées sur support électronique. La manipulation de données enregistrées ayant une valeur probante peut entraîner des conséquences aussi graves que les actes traditionnels de contrefaçon s'ils induisent un tiers en erreur. La falsification informatique consiste à créer ou modifier sans autorisation des données enregistrées de manière qu'elles acquièrent une valeur probante différente, de sorte que le déroulement de transactions juridiques, fondé sur l'authenticité des informations fournies par ces données, puisse être entaché de tromperie¹.

II. BIEN JURIDIQUEMENT PROTÉGÉ

- 2 Le bien juridiquement protégé par cette norme est la **sécurité** et la **fiabilité** des données électroniques, susceptibles d'avoir des conséquences sur les relations juridiques².

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Des données informatiques

- 3 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.
- 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 pertinentes dans les relations juridiques

- 5 L'utilisation des termes « **à des fins légales** » signifie que l'art. 7 CCC ne concerne pas toutes les données informatiques, mais uniquement les données qui jouent un rôle dans les relations juridiques. Elles doivent donc permettre de prouver un fait ayant une portée juridique, c'est-à-dire un fait dont dépend la création, la modification ou l'extinction d'un droit. Toutes les données qui ne sont pas pertinentes dans les relations juridiques sont donc exclues du champ d'application de cette norme.
- 6 Pour bénéficier d'un **caractère probant**, l'origine des données doit pouvoir être établie. Dans le monde réel, cette exigence signifie que l'auteur d'un titre doit être identifiable et que ce titre renferme l'expression d'une pensée humaine. Concrètement, cela se traduit par exemple par le fait que l'information ait un sens et que le document soit signé de la main de son auteur. Dans le monde virtuel, la garantie de l'origine des données prend une forme bien différente. Bien entendu, l'équivalent du document papier signé par son auteur existe. Il s'agit alors d'un document informatique

1. Rapport explicatif de la Convention sur la cybercriminalité, n. 81.

2. Rapport explicatif de la Convention sur la cybercriminalité, n. 81.

rédigé par un humain dans lequel la signature manuscrite est remplacée par l'apposition d'une signature électronique qualifiée³. Le monde virtuel offre cependant de nombreuses possibilités supplémentaires de produire des données pertinentes dans les relations juridiques.

- 7 Contrairement aux titres émis dans le monde réel, il n'est pas obligatoire, dans le monde virtuel, que l'auteur des données soit une personne humaine. Certaines données peuvent être **générées automatiquement** par des systèmes informatiques, sans perdre pour autant leur caractère probant. A titre d'exemple, on peut penser à un récépissé de paiement créé par une application d'*e-banking*, un certificat de salaire destiné à l'autorité fiscale généré automatiquement par le système informatique d'une entreprise pour ses employés en fin d'année, ou encore la quittance envoyée automatiquement par une autorité qui atteste du dépôt d'un acte juridique par la voie informatique.
- 8 Comme cela ressort expressément du texte de l'art. 7 CCC, cette disposition s'étend à l'**ensemble des données** pertinentes dans les relations juridiques « qu'elles soient ou non directement lisibles et intelligibles ». Il n'est donc pas non plus indispensable que les données renferment l'expression d'une pensée humaine. Les données peuvent tout à fait avoir été générées par un système informatique. Il faut simplement qu'elles puissent être comprises par un humain ou une machine. Les données peuvent donc tout à fait prendre la forme d'une suite de caractère qui forme un code, un code-barre ou un code-QR. Le meilleur exemple récent de ce type de données est le certificat COVID généré par ordinateur sous forme de code-QR qui atteste qu'une personne est vaccinée contre le COVID et qui permet à son titulaire d'accéder à certains lieux.
- 9 En définitive, dans le monde virtuel, pour que des données bénéficient d'une force probante et puissent être utilisées dans les relations juridiques, il suffit que leur **origine** puisse être établie avec certitude et qu'elles puissent être **comprises** par un humain ou une machine.

C. Un comportement punissable

- 10 La définition du faux dans les titres **varie** considérablement d'un pays à l'autre. Une simple comparaison de la définition qui lui est donnée en Suisse et dans ses pays voisins suffit déjà à s'en convaincre⁴. A travers le monde, on constate que pour certains, la notion de falsification est fondée sur l'authenticité quant à l'auteur du document, tandis que pour d'autres, c'est la véracité des informations contenues dans le document qui est déterminante⁵. Les Parties se sont donc accordées sur le fait que la falsification devait au minimum se rapporter à l'identité de l'émetteur des données, indépendamment de l'exactitude ou de la véracité du contenu de ces données. Elles sont toutefois libres d'étendre le champ d'application de leurs dispositions nationales pour réprimer également la falsification des informations contenues dans le document⁶.
- 11 L'authenticité des données quant à leur **auteur** implique qu'elles proviennent effectivement de la personne dont elles semblent émaner. Dans cette acception, la falsification de données authentiques consiste à faire apparaître un auteur qui n'est pas celui dont émanent véritablement les données. L'auteur réel n'est donc pas le même que l'auteur apparent.
- 12 En ce qui concerne l'authenticité quant au **contenu** des données, elle signifie que les données sont restées dans leur état d'origine. Il y a par conséquent falsification lorsqu'elles ont été modifiées après

3. Procédé technique qui permet de garantir l'authenticité de données et l'identité du signataire dont elles émanent.

4. § 267 du Code pénal allemand ; § 223 du Code pénal autrichien ; art. 485 du Code pénal italien ; art. 441-1 du Code pénal français.

5. Rapport explicatif de la Convention sur la cybercriminalité, n. 82.

6. Rapport explicatif de la Convention sur la cybercriminalité, n. 82.

leur création. La modification visée par l'art. 7 CCC n'est pas la simple correction d'une erreur de plume, mais bel et bien la modification du sens des données.

- 13 L'art. 7 CCC énumère ainsi quatre comportements punissables : l'introduction, l'altération, l'effacement ou la suppression de données informatiques. Cette liste est **exhaustive**. L'introduction de données réprime la création d'un titre faux, alors que l'altération, l'effacement et la suppression se rapportent à la falsification d'un titre vrai.

1. L'introduction de données

- 14 L'**introduction** de données est l'acte par lequel l'auteur introduit à l'intérieur d'un système informatique des données qui proviennent de l'extérieur de ce système. Il peut s'agir de l'introduction non-autorisée de données exactes ou de l'ajout de données inexactes⁷.
- 15 L'art. 7 CCC ne sanctionne que l'introduction de données qui entraîne la création de **données non-authentiques**. Lorsque les données introduites dans le système informatique sont destinées à entraver son bon fonctionnement, c'est l'art. 5 CCC qui s'applique.
- 16 A titre d'**exemple** d'introduction de données non-authentiques, on peut penser au comptable d'une société qui enregistre un paiement par un débiteur dans le programme de comptabilité, alors que le débiteur en question n'a, en réalité, pas payé. On peut aussi penser à l'auteur qui utilise une carte bancaire qu'il a copiée frauduleusement pour payer ses achats, au moyen de la fonction sans contact, faisant ainsi croire au terminal du vendeur que le paiement a été autorisé et effectué par le titulaire légitime de la carte copiée.

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

- 17 L'**altération** de données consiste à porter atteinte à l'intégrité et/ou au contenu des données. L'intégrité des données fait référence à leur fiabilité, leur exactitude et leur exhaustivité. Dans le monde réel, la garantie de l'intégrité des données pourrait être comparée à un colis envoyé 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. Quant à la garantie du contenu, on pourrait la comparer à l'attestation que le contenu du paquet n'a pas été modifié après son envoi. En cas d'altération de données, l'auteur modifie en quelque sorte le contenu du paquet et/ou son emballage dans le but de tromper le destinataire. La modification du contenu des données consiste à remplacer les données originales, par d'autres données. C'est par exemple le cas lorsque l'auteur modifie un texte, change des coordonnées bancaires ou remplace une image par une autre. L'auteur altère en revanche l'intégrité des données lorsqu'il modifie les métadonnées. Tel est notamment le cas de celui qui falsifie l'adresse *e-mail* de l'expéditeur pour faire croire qu'un message provient d'une certaine personne, alors qu'elle provient en réalité d'une autre ou contrefait une signature électronique qualifiée pour faire croire qu'un document a été établi par une certaine personne alors que tel n'est en réalité pas le cas.
- 18 La **suppression** de données consiste à retenir et à cacher des données⁸. L'auteur enlève donc volontairement une partie des données, afin que le destinataire n'ait pas connaissance de l'intégralité des données. Tel est notamment le cas de l'auteur qui supprime une partie des clauses négociées lors de pourparlers transactionnels, dans le but de conclure un contrat qui lui est plus favorable.
- 19 Contrairement à la suppression de données, l'**effacement** de données est une destruction définitive de tout ou partie des données. Les données n'existent plus. On peut ici à celui qui efface des parties

7. Rapport explicatif de la Convention sur la cybercriminalité, n. 83

de conversations électroniques qui ne lui sont pas favorables, puis produit la version expurgée comme moyen de preuve dans un procès, ou à celui qui efface des données contenues dans un dossier médical informatisé pour cacher une erreur médicale qu'il a commise.

D. L'illicéité

- 20 L'auteur doit agir **sans droit**, c'est-à-dire sans y avoir été autorisé par l'ayant-droit. Pour agir de manière licite, une personne doit obtenir l'accord de l'ayant-droit du système informatique pour y introduire les données ou de l'ayant-droit des données pour les modifier.
- 21 Dans la société actuelle de nombreuses entreprises et administrations travaillent avec des systèmes informatiques. La majorité des collaborateurs qui travaillent pour ces entités sont autorisés à y introduire des données ou à les modifier. Toutes ces personnes agissent de manière licite tant qu'elles suivent les **instructions** qui leur ont été données. Leurs actes deviennent en revanche illicites lorsqu'elles introduisent des données ou en modifient en violation des instructions qu'elles ont reçues. Tel est par exemple le cas de la personne qui est responsable de la caisse, qui vole des marchandises, puis qui inscrit des fausses ventes dans le système informatique pour tenter d'effacer les traces de son forfait.

E. L'intention

- 22 La falsification informatique 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 créer de fausses données ou de falsifier des données authentiques dans le but qu'elles soient utilisées dans les relations juridiques.

IV. ÉLÉMENTS CONSTITUTIF SUPPLÉMENTAIRE FACULTATIF

- 23 La dernière phrase de l'art. 7 CCC permet aux Parties d'exiger un **dessein spécial** en plus de l'intention. Ce dessein spécial peut prendre la forme d'une intention frauduleuse ou d'une intention pernicieuse similaire⁹. Le rapport explicatif ne contient pas d'indication sur la manière dont la notion d'intention frauduleuse doit être comprise. A notre avis, l'intention frauduleuse se rapporte à la volonté de l'auteur d'obtenir un avantage indu pour soi-même ou pour autrui. Cet avantage ne doit pas forcément être de nature pécuniaire. Il peut s'agir de tout avantage qui permet d'améliorer sa situation personnelle ou celle d'autrui. L'avantage recherché doit toutefois être indu, c'est-à-dire contraire au droit.
- 24 Les **Etats-Unis d'Amérique** ont fait usage de la possibilité offerte par l'art. 7 in fine CCC et ont indiqué qu'ils ne poursuivraient la falsification informatique que si elle était commise dans une intention frauduleuse¹⁰.
- 25 L'**Allemagne** et le **Pérou** ont repris les deux desseins mentionnés par l'art. 7 in fine CCC, à savoir que la falsification informatique devait être commise avec une intention frauduleuse ou une intention délictueuse similaire¹¹.

8. Rapport explicatif de la Convention sur la cybercriminalité, n. 83.

9. Rapport explicatif de la Convention sur la cybercriminalité, n. 85.

10. Déclaration des Etats-Unis d'Amérique consignée dans l'instrument de ratification déposé le 29 septembre 2006 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=USA>, visité le 21.1.2024), en lien avec le titre 15 §§ 45, 52, 11644 et le titre 18 §§1028, 129, 1030, 1341, 1345 du Code des Etats-Unis.

- 26 La **Belgique** a, quant à elle, déclaré qu'elle n'incriminerait la falsification informatique que lorsqu'elle était commise dans une intention frauduleuse ou à dessein de nuire¹².
- 27 La **Suisse** a décidé qu'elle ne poursuivrait la falsification informatique que si elle était commise dans le dessein de procurer à soi ou à un tiers un avantage ou de causer un dommage¹³.
- 28 Enfin, le **Chili** avait dans un premier temps expliqué qu'il ne poursuivrait la falsification informatique que si elle était commise avec une intention frauduleuse et qu'elle causait un préjudice à des tiers¹⁴. A notre avis cette déclaration n'était pas conforme au texte de l'art. 7 CCC, car une Partie peut uniquement exiger un dessein spécial supplémentaire. Il n'est toutefois pas possible d'exiger la réalisation d'un préjudice, alors que l'art. 7 CCC réprime une infraction de mise en danger. En 2022, le Chili a toutefois modifié sa législation. Dans sa nouvelle version, la *falsificación informática* correspond à l'art. 7 CCC¹⁵. La réserve n'est donc plus nécessaire.

V. COMPARAISON AVEC LE DROIT SUISSE

- 29 L'art. 7 CCC a pour but de sanctionner le faux dans les titres informatique. En droit suisse, ce bien juridique est protégé par le faux dans les titres (**art. 251 CP**) qui a été étendu aux titres informatiques (art. 110 al. 4 CP) depuis le 1^{er} janvier 1995¹⁶.
- 30 Les **comportements** sanctionnés par l'art. 7 CCC consistent à falsifier des données ayant une valeur probante dans le but de tromper autrui. L'introduction de données correspond à la création du titre faux. En revanche, l'altération, l'effacement et la suppression équivalent à la falsification d'un titre dans l'infraction traditionnelle de faux dans les titres.
- 31 Le droit suisse est donc **conforme** aux exigences de l'art. 7 de la convention.

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 concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur

-
11. Déclaration consignée dans une Note verbale de la Représentation Permanente de l'Allemagne déposée avec l'instrument de ratification, le 9 mars 2009 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=GER>, visité le 21.1.2024), en lien avec le § 269 du Code pénal allemand ; Déclarations consignées dans l'instrument d'adhésion et dans une Note Verbale de l'Ambassade du Pérou en France, reçues et enregistrées au Secrétariat Général le 26 août 2019 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=PER>, visité le 21.1.2024), en lien avec l'art. 9 de la Loi péruvienne sur les délits informatiques.
 12. Déclaration communiquée par le Ministre des affaires étrangères de la Belgique au moment du dépôt de l'instrument de ratification, le 20 août 2012 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=BEL>, visité le 21.1.2024), en lien avec l'art. 193 du Code pénal belge.
 13. Déclaration de la Suisse consignée dans l'instrument de ratification déposé le 21 septembre 2011 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=SWI>, visité le 21.1.2024), en lien avec l'art. 251 du Code pénal suisse.
 14. Déclaration du Chili consignée dans l'instrument d'adhésion reçu et enregistré au Secrétariat Général le 20 avril 2017 (disponible sous <https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=CHI>, visité le 21.1.2024), en lien avec l'art. 197 du Code pénal chilien.
 15. Art. 5 de la Loi chilienne N° 21.459 sur les délits informatiques.
 16. FF 1991 II 956ss.

l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991, FF 1991 II 933, disponible à https://www.fedlex.admin.ch/eli/fga/1991/2_969_933_797/fr, visité le 21.1.2024