



COMMENTAIRE EN LIGNE  
LE COMMENTAIRE JURIDIQUE  
EN OPEN ACCESS

COMMENTAIRE

# Art. 3 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: 10.17176/20240217-132639-0

## PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 3 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 3 CCC N. XXX.

### **Art. 3 Interception illégale**

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

## TABLE DES MATIÈRES

|                                                                                     |    |
|-------------------------------------------------------------------------------------|----|
| I. Généralités .....                                                                | 3  |
| II. Bien juridiquement protégé.....                                                 | 3  |
| III. Éléments constitutifs de base .....                                            | 3  |
| A. Des données informatiques.....                                                   | 3  |
| B. Une transmission non publique .....                                              | 3  |
| 1. La notion de transmission .....                                                  | 3  |
| 2. Le caractère non public.....                                                     | 4  |
| C. Le cas particulier des émissions électromagnétiques.....                         | 5  |
| D. L'interception par des moyens techniques .....                                   | 5  |
| E. L'illicéité.....                                                                 | 6  |
| F. L'intention .....                                                                | 7  |
| IV. Éléments constitutifs supplémentaires facultatifs .....                         | 7  |
| A. Le dessein d'obtenir des données informatiques ou un autre dessein spécial ..... | 7  |
| B. Un système informatique connecté à un autre système informatique. ....           | 8  |
| V. Comparaison avec le droit suisse.....                                            | 8  |
| Bibliographie .....                                                                 | 9  |
| Travaux législatifs .....                                                           | 10 |

## I. GÉNÉRALITÉS

- 1 Pour garantir une **protection juridique complète**, l'accès illégal devait être complété par l'interception illégale. Comme nous l'avons vu ci-dessus (cf. Art. 2 N. 9ss), l'accès illégal réprime l'intrusion illicite dans le système informatique et la consultation par des personnes non-autorisées des données qui y sont enregistrées. L'interception illégale, quant à elle, sanctionne la violation de la confidentialité des données qui circulent à l'intérieur du système informatique, ainsi que des données qui sont échangées entre le système informatique et l'extérieur.

## II. BIEN JURIDIQUEMENT PROTÉGÉ

- 2 Cette disposition protège le droit à la **confidentialité des données** transmises. L'infraction représente la même violation du droit au secret des communications que l'écoute et l'enregistrement classiques des conversations téléphoniques entre personnes. L'art. 3 CCC reprend la garantie du droit au respect de la correspondance figurant à l'art. 8 CEDH et l'applique à toutes les formes de transfert électronique des données, que ce transfert s'effectue par téléphone, télécopieur, courrier électronique ou fichier<sup>1</sup>.

## 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 au sujet de l'art. 1 CCC.

### B. Une transmission non publique

#### 1. La notion de transmission

- 5 Contrairement à ce que l'étymologie du terme « **transmission** »<sup>2</sup> pourrait laisser penser, la notion de transmission figurant à l'art. 3 *in initio* CCC ne vise pas que les échanges à distance entre deux appareils. Comme le suggèrent les prépositions « à destination », « en provenance » ou « à l'intérieur » d'un système informatique, elle concerne toutes les données en circulation. Les seules données qui ne sont pas concernées par cette notion sont celles qui sont stockées de manière fixe sur un support, par exemple un disque dur, une clé USB ou un DVD.
- 6 La transmission de données « **à l'intérieur** » d'un système informatique concerne les données qui circulent notamment dans et entre la carte-mère, le processeur, la carte graphique, l'écran d'ordinateur ou l'imprimante. Elle s'étend même aux données qui sont stockées dans la mémoire vive du système informatique, puisque ces données ne sont pas durablement stockées dans cette mémoire,

---

1. Rapport explicatif de la Convention sur la cybercriminalité, n. 51.

2. Du latin "*trans*" et "*mittere*" : envoyer au-delà.

mais n'y sont conservées que quelques instants avant de continuer à circuler dans le système informatique.

- 7 Les transmissions de données « **à destination** » ou « **en provenance** » d'un système informatique supposent que le destinataire ou l'expéditeur des données soit un système informatique, l'autre pouvant être un humain ou un système informatique.
- 8 Dans l'hypothèse, de la transmission de données de l'**être humain** « à destination » d'un **système informatique** on vise l'introduction de données par l'être humain dans le système informatique, par exemple à l'aide d'un clavier, d'une souris ou d'un joystick. A l'inverse, la transmission de données à l'être humain « en provenance » du système informatique s'entend de la restitution des données du système informatique à l'être humain par l'affichage des données sur un écran ou l'impression d'un document par une imprimante.
- 9 Enfin, lorsque la transmission de données se fait entre **deux systèmes informatiques**, elle a lieu tant « à destination » qu'en « en provenance » d'un système informatique. Tel est le cas notamment d'un échange entre un ordinateur et un serveur, entre deux ordinateurs ou encore entre un ordinateur et un *smartphone*. Il importe peu que les deux systèmes informatiques appartiennent à la même personne ou à des personnes différentes. De même, le mode de transmission est sans importance. Les données peuvent être échangées au moyen d'une connexion par fil ou sans fil (Wifi, NFC, Bluetooth, onde radio, ...).
- 10 Les éléments qui précèdent montrent que la notion de transmission est très vaste. Afin de restreindre le champ d'application de cette disposition, l'art. 3 *in fine* CCC permet aux Parties de **limiter** la poursuite pénale à la seule interception illégale de données transmises entre deux systèmes informatiques connectés à distance<sup>3</sup>.

## 2. Le caractère non public

- 11 L'art. 3 CCC ne concerne que les transmissions non publiques. Le caractère non public se rapporte à la transmission et non aux données transmises<sup>4</sup>. Il importe donc peu que les données transmises soient publiques ou privées. Seule la **nature** de la transmission est déterminante.
- 12 A notre avis, une transmission est non publique lorsqu'elle est **limitée** à un certain nombre de personnes ou à des personnes déterminées. Tel est notamment le cas de la transmission d'une présentation par le biais de la vidéoconférence qui ne peut être suivie que par un nombre limité de participants, ou des films mis à la disposition de ses seuls abonnés par une entreprise de « streaming ».
- 13 La notion de transmission non publique ne signifie toutefois pas que la transmission doive se faire au moyen d'un **réseau** qui n'est pas public. La transmission peut s'effectuer en utilisant un réseau public ; il faut simplement que cette transmission soit restreinte à un nombre déterminé de personnes.
- 14 Pour limiter une transmission à un nombre déterminé de personnes, il faut nécessairement mettre en place des **mesures techniques**. Il n'est toutefois pas exigé que ces mesures de sécurité soient particulièrement poussées. Un système permettant de contrôler si la personne qui souhaite accéder à la transmission fait partie des personnes autorisées est suffisant. On peut ainsi imaginer qu'il faille suivre un lien envoyé par courriel, introduire un code fourni préalablement, ou encore s'identifier au moyen d'un identifiant et d'un mot de passe.

---

3. A ce sujet, voir le ch. IV let. B ci-dessous.

4. Rapport explicatif de la Convention sur la cybercriminalité, n. 54.

## C. Le cas particulier des émissions électromagnétiques

- 15 Lorsque la Convention sur la cybercriminalité a été élaborée, entre avril 1997 et décembre 2000, les experts ont voulu anticiper les **évolutions technologiques**. L'interception illégale n'a donc pas été limitée à la seule transmission de données, mais a été étendue aux émissions électromagnétiques.
- 16 Pour comprendre le **fonctionnement** de la captation d'émissions électromagnétiques, il faut se rappeler que les données informatiques correspondent en langage binaire à une succession de « 0 » et de « 1 ». C'est sous cette forme que les systèmes informatiques traitent les données. Du point de vue microtechnique, il faut donc générer des impulsions électriques différentes pour un « 0 » et pour un « 1 ». C'est à cela que servent les transistors. Schématiquement, les systèmes informatiques sont composés d'une multitude de transistors. Ces derniers permettent de faire varier la tension électrique qui traverse les composants électroniques du système informatique passant de basse à élevée selon que le bit traité est un « 0 » ou un « 1 ». Ces innombrables variations de tension créent un champ électromagnétique qui se propage autour du système informatique. Cela permet à une personne située à proximité, équipée d'un appareil adapté, de capter ce flux, le reconvertir en « 0 » et en « 1 » et ainsi reconstituer les données informatiques traitées par le système informatique.
- 17 Pour les experts, l'arsenal juridique semblait **incomplet** si l'on se limitait à sanctionner l'interception de données transmises dans, à destination ou en provenance d'un système informatique, sans réprimer simultanément la captation des ondes électromagnétiques émises par un système informatique. Cela aurait équivalu, dans le monde réel, à sanctionner la mise sur écoute d'une personne dans son appartement au moyen de micro, tout en laissant impunie l'écoute des conversations de cette personne depuis derrière la porte d'entrée de l'appartement.
- 18 Il faut en particulier se rappeler qu'à l'époque de l'élaboration du texte de la convention, l'utilisation du fax était très répandue. Or, cet appareil envoyait des données non-codées, à une fréquence et avec une intensité électrique qui permettaient assez facilement de les capter, puis de les reconstituer dans un langage compréhensible. Les experts y ont certainement identifié une **faille de sécurité** qui pourrait être exploitée par les cybercriminels, ce qui les a conduits à inclure la captation d'ondes électromagnétiques dans la liste des comportements punissables.
- 19 Avec les années, le fax a quasiment complètement disparu. De nos jours, la captation d'ondes électromagnétiques est devenue très **marginale**, voire inexistante, en raison des difficultés techniques pour capter ces signaux. Les câbles électriques utilisés actuellement dans l'informatique sont bien plus isolés qu'à la fin des années 90 et les impulsions électriques sont beaucoup moins fortes. Parallèlement, la quantité de données échangées à chaque seconde a explosé. Il est par conséquent aujourd'hui quasiment impossible de capter les ondes magnétiques provenant d'une seule source et de les reconstituer pour en tirer des données intelligibles.
- 20 Lors de l'élaboration du texte de la convention, les experts ne pouvaient cependant pas anticiper dans quel sens évoluerait la **technologie**. C'est pourquoi ce comportement – même s'il est désormais anecdotique – figure dans la liste des comportements réprimés par l'art. 3 CCC.

## D. L'interception par des moyens techniques

- 21 L'art. 3 CCC ne s'applique qu'aux interceptions de données opérées avec des moyens techniques. La **soustraction physique** de données, notamment le vol d'une clé USB expédiée par la poste ou le vol d'un ordinateur portable allumé et déverrouillé dans un lieu public, ne sont donc pas réprimés par cette disposition.

- 22 L'interception mentionnée à l'art. 3 CCC peut être soit directe, soit indirecte. L'auteur intercepte les données **directement** lorsqu'il accède au système informatique lui-même. La forme la plus simple est l'installation d'un cheval de Troie dans le système informatique, ce qui permet à l'auteur d'obtenir un accès. L'auteur peut aussi utiliser une porte dérobée (*backdoor*) ou exploiter une faille de sécurité. Toutes ces techniques permettent à l'auteur de prendre connaissance des données qui circulent dans le système informatique en temps réel.
- 23 L'interception est dite **indirecte** lorsque l'auteur intercepte le flux de données échangé entre deux appareils. Tel est par exemple le cas du captage du flux de données qui transitent entre un appareil et une borne Wifi à laquelle il est connecté. A l'intérieur d'un réseau local (LAN), l'auteur peut aussi usurper l'adresse MAC d'un système informatique au moment du *broadcasting* pour se faire envoyer les paquets de données qui étaient destinés à celui dont l'adresse a été usurpée. Une autre technique consiste à recourir au *port mirroring*. Initialement, ce système a pour but de contrôler les données échangées au sein d'un réseau. Pour ce faire, une copie de toutes les données qui transitent par un commutateur réseau (*switch*) est envoyée à un système informatique de contrôle. En prenant le contrôle du commutateur réseau, l'auteur peut toutefois rediriger les données copiées vers son propre système informatique, ce qui lui permet de prendre connaissance de toutes les données échangées sur le réseau.
- 24 La notion de « **moyens techniques** » utilisée par les Parties est très vaste et imprécise. Elle n'est pas non plus accompagnée d'une liste exemplative. Ce choix a sans doute pour but de permettre à la norme de s'adapter plus facilement aux innovations technologiques. Quoi qu'il en soit, les appareils concernés sont ceux qui permettent d'écouter, de contrôler ou de surveiller le contenu des communications. Il s'agit donc de dispositifs techniques connectés aux lignes de transmission, ainsi que des dispositifs de collecte et d'enregistrement de communications sans fil. Les moyens techniques dont il est question à l'art. 3 CCC ne se limitent cependant pas aux hardwares. Les logiciels, les mots de passe et autres codes en font aussi partie<sup>5</sup>.

## E. L'illicéité

- 25 Pour être punissable, l'auteur doit avoir agi **sans droit**. C'est l'ayant-droit des données qui détermine qui est autorisé à en prendre connaissance. Sont ainsi punissables toutes les personnes qui n'ont pas été autorisées à consulter ces données. Ne sont en revanche pas punissables les personnes qui ont été autorisées à prendre connaissance de ces données par l'ayant-droit ou qui y sont autorisées en vertu de la loi ou d'un contrat.
- 26 Les législations nationales contiennent en effet des **exceptions** à la garantie de confidentialité des données. Elles permettent notamment aux services de renseignements de prendre connaissance de données qui ne leur sont pas destinées. Elles permettent également aux autorités de poursuite pénale de surveiller en temps réel un flux de données dans le cadre d'une instruction pénale. Ces interceptions ne sont pas illégales tant qu'elles sont opérées dans le strict respect des dispositions légales en vigueur. Une surveillance ne peut toutefois être mise en place que dans des cas graves et doit être soumise à un contrôle judiciaire postérieur<sup>6</sup>.
- 27 L'interception de données n'est pas non plus considérée comme illicite lorsqu'elle est **autorisée contractuellement**. Tel est en particulier le cas de l'administrateur du système informatique qui est chargé de la maintenance. Dans ce cas, il n'est pas punissable s'il intercepte les données dont il a besoin pour effectuer son travail, car il y a été autorisé par l'ayant-droit. De même, la personne

---

5. Rapport explicatif de la Convention sur la cybercriminalité, n. 53.

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

chargée du *monitoring* d'un réseau n'est pas non punissable si elle intercepte les données obtenues grâce à une utilisation conforme, notamment du *port mirroring*. En revanche, lorsque ces personnes profitent des possibilités techniques dont elles disposent pour intercepter des données qui ne sont pas nécessaires à l'exécution de leur travail, elles agissent de manière illicite.

- 28 Dans le contexte des **relations de travail**, une interception licite de données est concevable, mais à des conditions restrictives. De manière générale, la Cour européenne des droits de l'Homme a considéré que les communications privées des employés étaient protégées par l'art. 8 CEDH<sup>7</sup>. Une surveillance par l'employeur n'est donc envisageable que si l'employé a été informé de la surveillance de ses communications, de la nature et de l'étendue de cette surveillance, ainsi que du degré d'intrusion dans sa vie privée et sa correspondance<sup>8</sup>. Si l'employeur respecte ces conditions, l'interception de données de ses employés est licite.
- 29 A l'origine, l'art. 3 CCC n'avait pas pour but de pénaliser les **pratiques commerciales** courantes tendant à obtenir des renseignements sur les utilisateurs. Depuis l'entrée en vigueur de la Convention sur la cybercriminalité, les pratiques commerciales ont considérablement évolué et les renseignements que les entreprises commerciales cherchent à obtenir pour cibler leurs publicités sont de plus en plus importants. En conséquence, les législations nationales ont sensiblement renforcés la protection des données et des consommateurs. Il est donc devenu très fréquent que les sites web doivent obtenir le consentement des internautes avant de collecter des données à leur sujet, notamment à l'aide de « *cookies* ». Sans consentement de l'ayant-droit, la collecte de telles données pourrait constituer une interception illégale.

## F. L'intention

- 30 L'interception illégale est **intentionnelle**. L'intention doit porter sur tous les éléments objectifs de l'infraction. L'auteur doit donc avoir conscience qu'il obtient des données de manière induue et en avoir la volonté. Le dol éventuel suffit. Dans sa forme simple, le but poursuivi par l'auteur est sans importance.

## IV. ÉLÉMENTS CONSTITUTIFS SUPPLÉMENTAIRES FACULTATIFS

- 31 L'art. 3 CCC permet aux Parties de **restreindre** la punissabilité à certains actes particuliers en ajoutant un ou deux éléments constitutifs figurant à la fin de cette disposition.
- 32 Selon la manière dont l'interception illégale est retranscrite en droit national, cette infraction peut être **étroitement liée** à l'accès illégal (art. 2 CCC). Compte tenu du fait que certains Etats ont choisi de limiter la répression de l'accès illégal aux seuls cas commis avec un dessein particulier ou au moyen d'un système informatique connecté à un autre système informatique, il était nécessaire de permettre à ces Etats de restreindre l'interception illégale à ces mêmes cas<sup>9</sup>.

### A. Le dessein d'obtenir des données informatiques ou un autre dessein spécial

- 33 La première possibilité offerte aux Parties consiste à exiger que l'auteur ait agi dans un **dessein spécial**. Plusieurs Etats ont fait usage de cette possibilité.
- 34 Le **Canada**, le **Japon** et le **Pérou** ont indiqué qu'ils ne poursuivraient l'interception illégale que si elle était commise avec une intention délictueuse<sup>10</sup>. Cette dernière notion est particulièrement peut

7. Arrêt CourEDH Halford contre Royaume-Uni du 25 juin 1997 (20605/92) ; arrêt CourEDH Copland contre Royaume-Uni du 3 avril 2007 (62617/00) ; arrêt CourEDH Barbulescu contre Roumanie du 5 septembre 2017 (61496/08).

8. Arrêt CourEDH Barbulescu contre Roumanie du 5 septembre 2017 (61496/08).

précise et crée par conséquent une insécurité du droit considérable. De plus, elle semble se recouper avec la notion d'intention. Elle doit donc selon nous être interprétée restrictivement.

- 35 Le **Chili** avait initialement émis une réserve identique à celle du Canada, du Japon et du Pérou<sup>11</sup>. Il a toutefois modifié sa législation en 2022. Dans sa nouvelle version, l'*interceptación ilícita* ne nécessite plus de dessein spécial<sup>12</sup>.
- 36 La **Suisse**, quant à elle, a déclaré qu'elle ne poursuivrait l'interception illégale que si l'auteur avait agi dans un dessein d'enrichissement illégitime<sup>13</sup>.
- 37 Alors qu'ils avaient déclaré ne poursuivre l'accès illégal qu'à la condition que l'auteur soit animé par un dessein spécial<sup>14</sup>, la **Principauté d'Andorre**, la **Belgique**, les **Etats-Unis d'Amérique** et la **République slovaque** ont renoncé à poser cette même exigence pour l'interception illégale.

## B. Un système informatique connecté à un autre système informatique.

- 38 La Convention sur la cybercriminalité autorise également les Parties de restreindre la punissabilité de l'interception illégale uniquement aux données transmises entre deux systèmes informatiques connectés entre eux. Les seuls Etats qui ont fait usage de cette possibilité sont le **Japon** et le **Pérou**<sup>15</sup>.
- 39 Dans ce cas également, il est surprenant de constater que la **République slovaque** a renoncé à utiliser cette possibilité, alors qu'elle avait expressément indiqué qu'elle ne poursuivrait l'accès illégal que s'il était commis au moyen d'un système informatique connecté à un autre système informatique<sup>16</sup>.

## V. COMPARAISON AVEC LE DROIT SUISSE

- 40 Le Conseil fédéral a reconnu dans son Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité<sup>17</sup> que « le droit pénal suisse ne possède **pas de réglementation** correspondant à l'art. 3 de la Convention, mais plusieurs normes pénales assurent une protection partielle »<sup>18</sup>. Il s'agissait selon lui d'une combinaison des art. 143, 143<sup>bis</sup> et 321<sup>ter</sup> CP. En réalité, tel n'est absolument pas le cas.

---

9. Rapport explicatif de la Convention sur la cybercriminalité, n. 59.

11. Déclaration 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 art. 2 de la Loi chilienne N° 19.223 sur les délits informatiques.

12. Art. 3 de la Loi chilienne N° 21.459 sur les délits informatiques.

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. 143 du Code pénal suisse.

14. Voir Art. 2 CCC nn. 32-34.

15. Déclaration 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=10&codePays=JAP>, visité le 21.1.2024), en lien avec l'art. 109-2 de la Loi japonaise sur la radio ; 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. 7 de la Loi péruvienne sur les délits informatiques.

16. Voir Art. 2 CCC n. 38.

17. FF 2010 4275.

18. FF 2010 4282.

- 41 L'**art. 143<sup>bis</sup> CP** ne réprime que les intrusions dans un système informatique et non l'interception de données<sup>19</sup>.
- 42 En ce qui concerne l'**art. 321<sup>ter</sup> CP**, il réprime un délit propre pur, car l'infraction ne peut être commise que par l'employé d'une entreprise assurant le service des postes ou des télécommunications<sup>20</sup>.
- 43 Quant à l'**art. 143 CP**, il s'agit de la norme qui se rapproche le plus de l'art. 3 CCC. Pour correspondre aux exigences de la convention, cette disposition devrait toutefois faire l'objet de quatre modifications.
- 44 En premier lieu, les **biens juridiques protégés** par ces deux normes sont différents. L'art. 3 CCC protège la confidentialité des données transmises, alors que l'art. 143 CP protège « le droit du bénéficiaire légitime des données d'en disposer librement et conformément à sa volonté »<sup>21</sup>. Le bien juridique protégé par l'art. 143 CP devrait donc être adapté.
- 45 Deuxièmement, l'art. 3 CCC réprime l'interception de transmissions non publiques, peu importe que les données transmises soient ou non publiques. Or, l'art. 143 CP sanctionne uniquement la soustraction des données **spécialement protégées** contre tout accès. La soustraction de données publiques transmises de manière non publique ne tombe donc pas sous le coup de l'art. 143 CP<sup>22</sup>. Or, en pratique, c'est le cas le plus courant, car les données transmises électroniquement ne sont généralement pas spécialement protégées contre tout accès<sup>23</sup>.
- 46 Ensuite, l'art. 143 CP protège uniquement un **droit de disposition** sur des données. Or, les données informatiques n'ont pas toujours une valeur intrinsèque. Exiger un dessein d'enrichissement illégitime revient donc à exclure la protection pénale dans tous les cas où l'auteur soustrait des données sans valeur. Au vu du bien juridiquement protégé, cet élément constitutif devrait être supprimé<sup>24</sup>.
- 47 Enfin, l'art. 3 CCC ne se limite pas uniquement aux transmissions non publiques, mais inclut également les **émissions électromagnétiques**. Celles-ci ne sont toutefois pas protégées par l'art. 143 CP. Elles devraient donc y être ajoutées<sup>25</sup>.
- 48 Pour toutes ces raisons, force est de constater que le droit suisse n'est **pas conforme** à l'art. 3 CCC et devrait dès lors être adapté.

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

## BIBLIOGRAPHIE

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

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

---

19. Weissenberger, n. 17 et 20 ad art. 143<sup>bis</sup> CP.

20. Oberholzer, n. 3 ad art. 321<sup>ter</sup> CP ; Trechsel / Lehmkuhl, n. 3 ad art. 321<sup>ter</sup> CP.

21. FF 1991 II 977 ; SCHMID, § 4 n. 14ss ; Trechsel / Cramer, n. 2 ad art. 143 CP.

22. Treccani, p. 218ss.

23. Schwarzenegger, p. 320.

24. Schwarzenegger, pp. 320-321.

25. Schwarzenegger, p. 321 ; Treccani, p. 233.

Schwarzenegger Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, in : Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zurich 2002

Treccani Jean, Interceptions électroniques, in : Plus de sécurité, moins de liberté, les techniques d'investigation et de preuve en question, Zurich et Coire 2003

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

Trechsel Stefan / Lehmkuhl Marianne Johanna , 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 sous <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 l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991, FF 1991 II 933, disponible sous [https://www.fedlex.admin.ch/eli/fga/1991/2\\_969\\_933\\_797/fr](https://www.fedlex.admin.ch/eli/fga/1991/2_969_933_797/fr), visité le 21.1.2024

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 sous <https://www.fedlex.admin.ch/eli/fga/2010/813/fr>, visité le 21.1.2024