Dernière modification : 29.07.2026

PDF créé le : 07.10.2026

COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

TABLE DES MATIÈRES

Art. 1 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 5
Art. 2 CCC (Convention sur la cybercriminalité [Cybercrime Convention])... 31
Art. 3 CCC (Convention sur la cybercriminalité [Cybercrime Convention]).. 47
Art. 4 CCC (Convention sur la cybercriminalité [Cybercrime Convention]).. 63
Art. 5 CCC (Convention sur la cybercriminalité [Cybercrime Convention]).. 75
Art. 6 CCC (Convention sur la cybercriminalité [Cybercrime Convention]).. 89
Art. 7 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 105
Art. 8 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 117
Art. 9 CCC (Convention sur la cybercriminalité [Cybercrime Convention]). 127
Art. 11 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 145
Art. 12 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 151
Art. 16 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 167
Art. 18 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 181
Art. 25 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 199
Art. 27 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 211
Art. 28 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 231
Art. 29 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 239
Art. 32 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 259
Art. 33 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 303
Art. 34 CCC (Convention sur la cybercriminalité [Cybercrime Convention]) 321

COMMENTAIRE

Art. 1 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jérémie Müller

PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 2 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 1 CCC N. XXX.

Chapitre I Terminologie
Art. 1 Définitions

Aux fins de la présente Convention:

a. 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;

b. 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;

c. l'expression «fournisseur de services» désigne:

i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs;

d. «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

TABLE DES MATIÈRES

I. Généralités 8
II. Système informatique (Let. A) 8
A. Un dispositif 9
B. Un programme 11
C. Un traitement des données automatique 12
D. Perspectives 13
1. La dématérialisation des systèmes informatiques 13
2. L'Internet des objets (IoT) 14
3. L'intelligence artificielle 15
III. Données informatiques (let. b) 16
A. La forme des données 16
B. Les types de données 17
C. Les programmes 18
D. Perspectives 19
E. Excursus : la distinction entre données relatives à l'abonné, données relatives au trafic et données de contenu en droit pénal suisse 19
1. Les données relatives à l'abonné 19
2. Les données relatives au trafic (ou données secondaires) 20
3. Les données de contenu 21
IV. Fournisseur de Services (let. c) 22
A. Les fournisseurs d'accès 22
B. Les fournisseurs de stockage ou de contenu 24
C. Perspectives 26
V. Données relatives au trafic (let. d) 26
Bibliographie 29
Travaux législatifs 29

I. GÉNÉRALITÉS

1 La Convention sur la cybercriminalité commence par fournir, à son article 1, quatre définitions des notions centrales auxquelles se réfèrent les différents articles qui suivent. Les rédacteurs de la convention ont certes précisé dans leur Rapport explicatif que les Parties ne seraient pas tenues de reproduire mot pour mot, dans leurs lois internes, les quatre notions définies à l'art. 1 CCC. Ils ont toutefois précisé qu'il fallait que les lois nationales couvrent ces notions d'une façon qui soit compatible avec les principes de la Convention et offrent un cadre équivalent pour sa mise en œuvre.[1] L'intérêt de ces définitions apparaît donc clairement : mettre l'ensemble des Parties sur un pied d'égalité afin de s'assurer qu'elles se réfèrent aux mêmes concepts. Cela permet notamment d'**éviter des litiges**, par exemple qu'une Partie refuse d'exécuter certaines dispositions au motif qu'elle interprète une notion différemment d'une autre Partie.

2 Les rédacteurs de la Convention étaient manifestement **conscients de l'évolution rapide** de l'informatique.[2] C'est sans doute pour cette raison qu'ils ont décidé de formuler les définitions de l'art. 1 CCC de manière aussi neutre que possible du point de vue technologique, en se limitant à la description fonctionnelle de chaque notion. Cette stratégie a porté ses fruits, puisque, vingt-cinq ans plus tard, ces définitions demeurent pertinentes malgré l'évolution technologique considérable qui a eu lieu au cours de cette période.

II. SYSTÈME INFORMATIQUE (LET. A)

3 La définition retenue par les auteurs de la Convention sur la cybercriminalité se compose de **trois aspects**. Elle suppose, en premier lieu, l'existence d'un dispositif. Celui-ci peut être isolé ou en réseau. La définition englobe donc aussi bien l'ordinateur personnel que les environnements informatiques interconnectés. Le deuxième élément réside dans la présence d'un programme. Il faut donc que le dispositif fonctionne sur la base d'instructions préétablies. Le dispositif ne peut pas être purement mécanique. Une boîte à

1. Rapport explicatif de la Convention sur la cybercriminalité, n. 22.
2. Voir notamment les remarque formulées en ce sens dans le Rapport explicatif de la Convention sur la cybercriminalité, nn. 137, 300, 302 ou 325.

musique ou une horloge ne sont donc pas des systèmes informatiques. Enfin, le traitement des données doit s'effectuer de manière automatique. Il ne suffit pas que le dispositif se limite à un stockage passif des données, il faut qu'il exécute automatiquement un processus de transformation de ces données. Un appareil photographique, un dictaphone ou une clé USB ne sont donc pas des systèmes informatiques.

Dans ses lignes directrices, le Comité de la Convention sur la cybercriminalité a précisé que la définition de « système informatique » incluait, par exemple, les **téléphones mobiles modernes** qui sont multifonctionnels et ont parmi leurs fonctions la capacité de produire, traiter et transmettre des données, telles que l'accès à Internet, l'envoi d'e-mails, la transmission de pièces jointes, le téléchargement de contenus ou de documents. Il en va de même des **assistants numériques personnels**, avec ou sans fonctionnalité sans fil qui produisent, traitent et transmettent également des données.[3] 4

La définition qui a été retenue appréhende volontairement le système informatique sous l'angle de sa **fonctionnalité**, et non de sa forme. Cette approche lui confère une souplesse suffisante pour évoluer dans le temps et inclure des technologies qui n'existaient pas encore en 2001, telles que les *smartphones*, l'Internet des objets (*IoT*) ou le *cloud computing*. 5

A. Un dispositif

L'informatique repose fondamentalement sur le traitement de données. Cette dernière notion sera développée ci-dessous au chiffre III. A ce stade, les données peuvent être définies comme des informations numériques immatérielles. Afin de pouvoir être traitées, ces informations requièrent toutefois un **ensemble de composants matériels** qui permettent tant leur traitement que leur stockage. 6

Bien qu'elle ne constitue pas l'élément le plus important du système informatique, la **carte mère** représente néanmoins l'ossature. Il s'agit d'une grande carte électronique qui sert de support à l'ensemble des composants du système. L'élément véritablement central du système informatique est le **processeur.**[4] Il représente le cœur du système, dans la mesure où il traite l'ensemble des instructions et des demandes qui lui parviennent des différents 7

3. T-CY Note d'orientation 1, ch. 3
4. Egalement appelé CPU (*Central Processing Unit*).

composants. Une fois les données traitées, le processeur doit pouvoir les stocker temporairement quelque part, car il n'est doté d'aucune mémoire.[5] Les données sont dès lors provisoirement stockées dans la **mémoire vive.**[6] Cette mémoire ne peut cependant stocker des données que lorsque le système informatique est sous tension. Lorsqu'il s'éteint, toutes les données contenues dans cette mémoire sont perdues. Il est donc nécessaire de prévoir un stockage durable de ces données sur un périphérique approprié, tel qu'un disque dur, un disque dur externe, une clé USB, un DVD, etc.

8 Les derniers composants indispensables au fonctionnement du système informatique sont les **périphériques**. Les périphériques d'entrée permettent l'introduction des données dans le système, tels que la souris, le clavier ou le scanner. On y oppose les périphériques de sortie qui assurent la restitution des données traitées par le système, comme l'écran, l'imprimante ou le graveur de DVD. Tous ces éléments matériels sont appelés *hardware* et forment un dispositif.

9 Il serait toutefois réducteur de penser que tous les composants qui forment le dispositif doivent nécessairement être localisés en **un seul lieu** de manière compacte, car cela reviendrait à limiter la notion de dispositif à un ordinateur personnel ou à un *smartphone*. Or, il existe actuellement des superordinateurs qui occupent chacun une halle entière. A l'inverse, il existe aussi des dispositifs dont les composants sont éparpillés tout autour du globe.

10 Le dispositif peut fonctionner de manière **isolée** ou de manière interconnectée. Avant la démocratisation d'Internet au milieu des années 90, la plupart des dispositifs fonctionnaient de façon isolée. Depuis lors, ce mode de fonctionnement constitue plutôt l'exception, réservée à des situations qui nécessitent un niveau de sécurité maximal, notamment afin d'éviter toute intrusion par le biais de connexions externes.

11 Les dispositifs sont **interconnectés** lorsqu'ils sont reliés entre eux au moyen d'une connexion filaire ou sans fil, telle que les ondes, les liaisons infrarouges, la fibre optique ou les liaisons satellitaires, formant ainsi un réseau. Celui-ci peut être limité à une certaine zone géographique, par exemple une

5. En réalité, les processeurs sont dotés d'une mémoire cache pour stocker les informations qui seront immédiatement nécessaires à la suite des calculs. Cette mémoire cache est toutefois très limitée.
6. La mémoire vive est également appelée RAM (*Random Access Memory*).

habitation, une entreprise ou une université. Il s'agit alors d'un réseau local (*Local Area Network* ou LAN). Ce réseau peut toutefois aussi s'étendre sur une zone beaucoup plus vaste, par exemple, une ville, un pays ou un continent. On parle alors de réseau étendu (*Wide Area Network* ou WAN). Le plus grand réseau étendu est Internet puisqu'il s'agit d'un réseau formé d'une multitude de réseaux interconnectés s'étendant au monde entier.

Enfin, la notion de dispositif comprend aussi les **autres appareils** qui permettent aux ordinateurs connectés aux réseaux de s'échanger des données. A ce titre, les serveurs, les routeurs, les commutateurs (*switches*), les modems et les passerelles (*gateways*) doivent aussi être qualifiés de dispositifs. 12

B. Un programme

Aux éléments matériels (*hardwares*) s'opposent les éléments logiciels (*softwares*), lesquels regroupent l'ensemble des programmes qui permettent **le fonctionnement et l'exploitation** des différents composants du système informatique. 13

Un programme peut être défini comme un **ensemble de commandes** qui, lorsqu'elles sont exécutées par un système informatique, permettent d'obtenir un résultat déterminé. 14

Tout comme pour les composants matériels, il convient de distinguer les programmes en fonction de la tâche qu'ils remplissent. Le programme de « démarrage » de tout système informatique est le **BIOS (***Basic Input and Output System*) ou **UEFI** (*Unified Extensible Firmware Interface*). Il est contenu dans une puce reliée à la carte mère et fournit les éléments nécessaires à l'amorçage du système. De plus, il assure la gestion de base des différents composants matériels du système informatique et joue le rôle d'interface entre ces composants et le système d'exploitation. 15

Le **système d'exploitation** constitue, quant à lui, le programme central du système informatique. Il assure le fonctionnement global et cohérent du système en coordonnant les différentes requêtes adressées au système informatique par l'utilisateur ainsi que les interactions entre les composants matériels et les autres programmes. En d'autres mots, le système d'exploitation agit comme une interface essentielle entre les logiciels applicatifs et les éléments matériels du système. 16

17 Enfin, les programmes applicatifs remplissent chacun une **fonction** spécifique. A titre d'exemples, Word© permet le traitement de texte, Photoshop© le traitement d'images, Outlook© la réception et l'envoi de courriels. Ces programmes reposent néanmoins sur le système d'exploitation pour accéder aux ressources matérielles et exécuter les tâches pour lesquelles ils ont été conçus.

C. Un traitement des données automatique

18 Le traitement automatisé des données désigne le fait que les données sont traitées de manière automatique par un programme, **sans** qu'une **intervention humaine** directe ne soit nécessaire.[7] Ce traitement peut porter tant sur l'acquisition que sur le stockage ou la restitution des données.

19 Comme on le verra ci-dessous au chiffre III, les données constituent des informations numériques immatérielles. Afin de pouvoir être traitées par un système informatique, les informations issues du monde matériel doivent être converties dans un **langage compréhensible par le dispositif**. Ainsi, une pression exercée sur une touche de clavier, un bouton de souris ou un écran tactile est traduite en langage binaire et transformée en signaux électriques, logiques ou optiques.

20 Une fois l'information matérielle convertie en signaux électriques, logiques ou optiques, le programme est en mesure de procéder au traitement automatisé des données. Lorsque le traitement est terminé, les données sont à nouveau traduites dans un **langage intelligible pour l'utilisateur**. Le programme peut ainsi, par exemple, afficher des caractères alphabétiques sur un écran lorsqu'un utilisateur presse sur les touches d'un clavier, transmettre les informations visuelles affichées à l'écran à une imprimante afin qu'elles soient reproduites sur du papier lorsque l'utilisateur clique sur l'icône « imprimer » ou encore établir une communication téléphonique lorsque l'utilisateur appuie sur le symbole du téléphone vert sur l'écran tactile de son *smartphone*. Chaque instruction donnée par l'utilisateur au système informatique engendre la création de données informatiques, lesquelles sont traitées de manière automatisée par des programmes, puis restituées à l'utilisateur sous une forme qui lui est compréhensible.

7. Rapport explicatif de la Convention sur la cybercriminalité, n. 23.

D. Perspectives

1. La dématérialisation des systèmes informatiques

Dès les années 80, l'idée de l'informatique distribuée a fait son apparition, notamment à travers le slogan lancé par Sun Microsystems : « *The network is the computer !* » (« Le réseau, c'est l'ordinateur ! »). Cette approche repose sur la **mise en commun de ressources** de calcul afin de traiter des volumes de données plus importants. Dans cette perspective, lorsque le réseau considéré est Internet, l' « ordinateur » qu'il représente se compose de l'ensemble des ordinateurs qui y sont connectés, ce qui représente une capacité de calcul particulièrement considérable. C'est dans ce contexte qu'apparaissent, à partir de la fin des années 90 et avec la démocratisation d'Internet, des projets de calcul répartis. Ces derniers consistent à proposer à des particuliers de mettre à disposition, via Internet, la puissance de calcul de leurs ordinateurs personnels lorsqu'ils ne les utilisent pas, afin de procéder à des calculs qui nécessitent des capacités de traitement très élevées. 21

Avec le temps, cette logique de mutualisation ne s'est plus seulement limitée au processeur. C'est l'ensemble de l'architecture informatique qui a progressivement été repensée pour devenir une **architecture distribuée**, en ce sens que les différentes ressources disponibles ne se trouvent plus nécessairement localisées au même endroit ni sur une même machine.[8] Un exemple emblématique d'architecture distribuée ayant connu un essor fulgurant au début des années 2000 est le modèle dit « pair à pair » (*peer-to-peer*). Ce modèle permet le partage de fichiers au sein d'une architecture dans laquelle chaque ordinateur joue à la fois le rôle de client et de serveur. 22

Entre la fin des années 2000 et le début des années 2010 est apparu le *cloud computing* (« informatique en nuage »), lequel consiste à recourir à des serveurs informatiques distants, connectés à Internet, pour stocker, gérer et traiter des données, plutôt que de s'appuyer sur un serveur local ou un ordinateur personnel.[9] Cette technique permet notamment à l'utilisateur de créer un système informatique virtuel, d'y installer un système d'exploitation et des applications et d'y générer, traiter et sauvegarder des données. Il suffit à cet égard de disposer d'un terminal connecté à Internet, toutes les autres 23

8. https://fr.wikipedia.org/wiki/Architecture_distribuée
9. https://fr.wikipedia.org/wiki/Cloud_computing

ressources étant mises à disposition de manière virtuelle et décentralisée, provenant de lieux et parfois de fournisseurs de services divers répartis dans le monde entier. Dans une telle configuration, il apparaît aisé de comprendre que la qualification de « système » puisse devenir problématique, dès lors qu'il n'existe plus d'unité matérielle des composants.

2. L'Internet des objets (IoT)

24 Depuis quelques années, on assiste à une véritable explosion du nombre d'**objets connectés**. Qu'il s'agisse de montres, de fours, de télévisions ou de véhicules, la quasi-totalité des objets du quotidien existe sous une forme qui peut être connectée à Internet.

25 Dans les années 90, SCHMID affirmait, en s'appuyant sur le Message du Conseil fédéral, que les distributeurs à nourriture, à essence, à billets, les photocopieurs ou les machines à sous ne pouvaient pas être qualifiés de systèmes informatiques, au motif que le législateur fédéral avait voulu limiter la notion de système informatique aux seuls dispositifs capables d'accomplir **des fonctions dites « supérieures ».**[10]

26 Cette opinion ne peut plus être défendue aujourd'hui. Les objets connectés font désormais pleinement partie d'Internet, peuvent être pilotés à distance et sont en mesure d'exécuter tellement de tâches qu'ils réalisent l'ensemble des critères qui permettent de les qualifier de systèmes informatiques au sens de l'art. 1 let. a CCC. Ce **changement de paradigme** n'est toutefois pas sans soulever de sérieux problèmes. Les objets connectés ne bénéficient en effet généralement pas de mesures de protection équivalentes à celles des ordinateurs traditionnels. Les cybercriminels peuvent donc plus facilement accéder indûment à une montre connectée afin d'en extraire les moyens de paiement qu'elle renferme, déverrouiller une porte reliée à un système domotique pour pénétrer dans une habitation ou encore accéder à un réseau d'entreprise en se connectant sans droit à la machine à café connectée de sa cafétéria, qu'accéder à un ordinateur personnel spécialement protégé contre tout accès. Il en résulte que le champ d'application de l'art. 2 CCC, pour les Etats qui n'exigent pas comme la Suisse que l'infraction soit commise en violation de mesures de sécurité, se révèle particulièrement vaste et est appelé à s'étendre encore davantage dans les années à venir.

10. Schmid, § 2 nn. 19 et 50 et le renvoi à la FF 1991 II 988.

3. L'intelligence artificielle

Comme on l'a vu ci-dessus (au chiffre II, lettre B), la définition posée par l'art. 1 let. a CCC suppose qu'un système informatique soit doté d'un programme. Ce programme exécute en principe une série de commandes prédéfinies par l'humain. Avec l'essor de l'intelligence artificielle, le **caractère immuable des programmes** ne va plus nécessairement de soi. Les systèmes fondés sur l'intelligence artificielle sont en effet capables d'apprentissage autonome et peuvent, dans certaines configurations, modifier leur propre code source ou adapter les paramètres de l'environnement dans lequel ils évoluent. Se pose dès lors la question de savoir si la notion de système informatique, telle qu'elle est actuellement définie, demeure suffisamment large pour appréhender ces évolutions technologiques ou si une redéfinition s'impose afin de tenir compte des développements futurs dans le domaine de l'intelligence artificielle. A notre avis, la définition actuelle est formulée de façon assez large pour inclure les évolutions technologiques connues à ce jour. En effet, même si l'intelligence artificielle est en mesure de réécrire le code source d'un programme pour s'adapter à son environnement, le système informatique continue à fonctionner sur la base d'un programme. 27

Deux problématiques émergentes risquent toutefois de nécessiter une redéfinition dans les années à venir. La première est l'intelligence artificielle agentique autonome et déployée, c'est-à-dire des agents capables de négocier, migrer entre environnements, créer d'autres agents ou modifier leur propre infrastructure sans intervention humaine. Cela pose le problème de l'unité du système informatique, car on ne parviendrait plus à déterminer clairement à partir de quand un essaim d'agents constitue encore un système informatique ou plusieurs. De plus, la Convention ignore la notion de système informatique éphémère, distribué et auto-organisé. La seconde problématique est celle de l'intelligence artificielle neuromorphique, à savoir sans programmes séparés. On le voit par exemple avec les puces Loihi d'Intel qui imitent le cerveau humain. Contrairement aux processeurs traditionnels, ces puces traitent l'information par événements et intègrent la mémoire au processeur. Il n'existe donc plus de « programme » distinct du matériel. L'exécution et l'apprentissage sont indissociables, de sorte que la définition actuelle du système informatique deviendrait obsolète. 28

A moyen terme, il serait donc nécessaire d'**étendre la définition** du système informatique, d'une part, aux agents autonomes déployés et, d'autre part, à 29

tout dispositif matériel ou hybride qui réalise un traitement de données par apprentissage, y compris lorsque l'exécution ne repose pas sur un programme distinct.

III. DONNÉES INFORMATIQUES (LET. B)

30 Les données informatiques sont définies comme « *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* » (art. 1 let. b CCC). Cette définition, reprise de celle de l'Organisation internationale de normalisation (ISO), se caractérise par sa **neutralité technologique**. Cela lui confère l'avantage d'avoir remarquablement résisté à l'évolution fulgurante des technologies depuis l'adoption de la Convention en 2001.

A. La forme des données

31 Les systèmes informatiques utilisent un **langage** fondamentalement différent de celui des humains. Un texte, une image ou une œuvre musicale réalisée par l'humain n'a, en tant que telle, aucune signification pour un ordinateur. Pour pouvoir être comprise et traitée, cette information doit être convertie dans un langage intelligible pour la machine. C'est dans cette perspective que la définition de « données informatiques » retenue dans la Convention utilise les termes « qui se prête à un traitement ». Ils signifient que la représentation de faits, d'informations ou de concepts doit pouvoir être traitée directement par un système informatique, sans nécessiter une transformation préalable destinée à en permettre la reconnaissance par celui-ci.[11] Les données informatiques sont donc des informations qui peuvent directement être comprises et exploitées par un ordinateur.

32 L'informatique repose sur un **système binaire**, ce qui signifie qu'il n'utilise que les chiffres 0 et 1. Cette unité élémentaire d'information est appelée *bit*.[12] Une suite de huit bits constitue un octet (p. ex. 10011101), lequel permet de représenter 2^8, soit 256 valeurs distinctes. Ce système rend possible la traduction d'informations issues du langage humain en indications compréhensibles par la machine. Selon le programme utilisé, un octet peut

11. Rapport explicatif sur la Convention sur la cybercriminalité, n. 25.
12. Binary digit.

représenter un chiffre, une lettre, une couleur ou même un son. A titre d'exemple, lorsqu'un utilisateur appuie sur la lettre « a » du clavier de son ordinateur dans un programme de traitement de texte, cette action est convertie en langage binaire sous la forme « 01100001 ». Cet octet constitue une donnée que l'ordinateur est en mesure de traiter en affichant un « a » à l'écran. De la même manière, les couleurs sont converties en valeurs réparties sur trois axes : rouge, vert et bleu. La valeur 0 indique que la couleur est absente et la valeur 255 que la couleur est d'intensité maximale. Ainsi, un pixel de couleur abricot dans un programme de dessin sera représenté par les valeurs 230 sur l'échelle rouge, 126 sur l'échelle verte et 48 sur l'échelle bleu, soit, en langage binaire, « 111001101111111011000000 ». Cette donnée de 24 bits permet au programme de dessin d'afficher un pixel couleur abricot sur la page blanche.

Les exemples qui précèdent illustrent que, en informatique, la donnée 33
informatique est l'unité élémentaire qui contient une information. A l'inverse, lorsqu'un ensemble de données sont réunies pour former un tout cohérent, on parle de **fichier**. Il peut s'agir d'un texte, d'une image, d'une vidéo ou d'un enregistrement sonore.

B. Les types de données

La définition de l'art. 1 let. b CCC n'opère **pas de distinction** entre les 34
différents types de données. Toutes les données informatiques sont concernées, qu'elles soient personnelles ou non, privées ou publiques, compréhensibles par l'humain ou uniquement par la machine. Le contenu des données est également sans importance, qu'il s'agisse de données factuelles (dates, heures, mesures, etc.), de renseignements (rapports, analyses, etc.) ou de concepts abstraits (modèles, algorithmes, codes, etc.). Constituent donc des données au sens de l'art. 1 let. b CCC les données stockées sur des supports de sauvegarde, les données temporaires, les données en transit, les métadonnées et même les données chiffrées.

Aux données créées par l'humain il faut à notre avis ajouter celles qui sont 35
produites automatiquement par un système informatique à partir de données préexistantes, qu'on appelle **données dérivées ou inférées**, notamment par des procédés de transformation, de combinaison ou d'analyse algorithmique. A titre d'exemple, on peut citer les profils d'utilisateurs, les scores, les prédictions ou les classifications générées sans intervention humaine directe.

Bien qu'il ne s'agisse pas de données initialement fournies par un utilisateur, elles doivent à notre avis aussi être englobées dans la définition de l'art. 1 let. b CCC, dès lors qu'elles se prêtent à un traitement informatique et sont exploitables par un système informatique.

36 La définition de données informatiques s'étend selon nous également aux données **volatiles** (ou éphémères), notamment celles stockées temporairement dans la mémoire vive d'un système, générées dynamiquement lors de l'exécution d'un programme ou destinées à disparaître automatiquement après un laps de temps très court. Bien que leur durée de vie soit brève, elles revêtent une importance particulière dans le cadre des enquêtes pénales, en particulier en cas d'accès illégal (art. 2 CCC) ou d'atteinte à l'intégrité du système (art. 5 CCC) au moyen d'une attaque par déni de service distribué.

37 Au regard de la définition des données informatiques axée uniquement sur la fonction, il importe peu que les données soient intelligibles pour un être humain. Des données demeurent des données informatiques même lorsqu'elles sont **chiffrées, compressées, fragmentées** ou stockées sous une forme qui ne permet pas une lecture immédiate. Le chiffrement des données n'est pas pertinent du point de vue juridique, puisqu'il constitue uniquement une modalité technique de traitement des données visant à en restreindre l'accès. Dès lors, le statut juridique des données ne se modifie pas du fait qu'elles sont chiffrées ou rendues temporairement inutilisables par des cybercriminels.

C. Les programmes

38 La précision « y compris un programme », voulue par les rédacteurs de la Convention, vise à lever toute ambiguïté quant à l'inclusion des **programmes** dans la définition de l'art. 1 let. b CCC. Cette approche est tout à fait cohérente à double titre. Sous l'angle informatique, un programme est un ensemble d'instructions contenu dans un code source, lui-même composé d'une multitude de caractères, c'est-à-dire des données, qui déterminent la manière dont les données qui lui sont fournies doivent être traitées. D'un point de vue systématique, l'inclusion des programmes dans la définition de données informatiques s'inscrit dans la volonté clairement affirmée des rédacteurs de la Convention de ne pas opérer de distinction entre les différents types de données.

D. Perspectives

Bien qu'il fût impossible, au moment de la rédaction de la Convention, de prévoir les développements futurs de l'informatique, le choix d'une définition **technologiquement neutre** a permis d'y intégrer tous les nouveaux types de données apparus depuis 2001. Tel est notamment le cas des crypto-actifs,[13] des données générées par les objets connectés ainsi que les *datasets*, c'est-à-dire les collections structurées de données destinées à l'entraînement de modèles d'apprentissage automatique. 39

E. Excursus : la distinction entre données relatives à l'abonné, données relatives au trafic et données de contenu en droit pénal suisse

L'évolution fulgurante des technologies au cours des trente dernières années a nécessité des **adaptations législatives très importantes** afin de distinguer quels types de données pouvaient être obtenus et à quelles conditions. La première Loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT) a été adoptée le 6 octobre 2000 et est entrée en vigueur le 1er janvier 2002. Elle a été entièrement révisée en 2016, puis a subit plusieurs révisions partielles, dont notamment une importante en 2024. 40

Le législateur a considéré que toutes les données n'avaient pas la même importance. Il est parti de la prémisse que plus l'atteinte à la vie privée, garantie par l'art. 13 Cst., était importante, plus les conditions auxquelles ces données pouvaient être obtenues devaient être élevées. La loi opère ainsi une distinction entre **trois types de données** : les données relatives à l'abonné (*Bestandesdaten*), les données relatives au trafic (*Randdaten*) et les données de contenu (*Inhaltsdaten*). 41

La Convention sur la cybercriminalité opère cette même distinction à son article 18. 42

1. Les données relatives à l'abonné

Les données relatives à l'abonné comprennent les **informations d'identification du titulaire** d'un raccordement. Il s'agit en particulier du nom, du prénom, de la date de naissance, de l'adresse et, si elle est connue, de 43

13. Voir à ce sujet le commentaire de l'art. 32, n. 19.

la profession de l'usager (art. 21 al. 1 let. a LSCPT), ainsi que des ressources d'adressage (art. 21 al. 1 let. b LSCPT) et des types de services (art. 21 al. 1 let. c LSCPT) qui ont été utilisés.

44 Ces données correspondent à celles énumérées à l'**art. 18 § 3 CCC**, à savoir : le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service (let. a) ; l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services (let. b) ; toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services (let. c)[14].

45 Il s'agit des **données les moins sensibles**. Leur obtention ne porte qu'une atteinte minime à la sphère privée. En droit suisse, leur obtention est donc soumise uniquement aux conditions de l'art. 197 al. 1 CPP et ne nécessite pas d'autorisation du Tribunal des mesures de contrainte.

2. Les données relatives au trafic (ou données secondaires)

46 Les données relatives au trafic sont les données indiquant avec **qui, quand, combien de temps et d'où** la personne surveillée a été ou est en communication ainsi que les caractéristiques techniques de la communication considérée (art. 8 let. b LSCPT).

47 Dans un arrêt de principe[15], le Tribunal fédéral a en particulier considéré que **l'historique des adresses IP** des membres s'étant connectés à un réseau social fait partie des données relatives au trafic et non des données relatives à l'abonné. Cet arrêt qui a été très critiqué en doctrine, a été récemment confirmé dans un arrêt non-publié[16].

48 La Convention sur la cybercriminalité les définit à l'art. 1 let. d CCC. Elles seront examinées en détail au chapitre V ci-dessous[17].

14. Pour plus de détails au sujet de cette disposition, voir le commentaire de l'art. 18 CCC nn. 24 et 25.
15. ATF 141 IV 108 consid. 5.
16. Arrêt 6B_1353/2023 du 6 novembre 2024 consid. 4.3.4.1 et 5.2.4.
17. Voir également à ce sujet le commentaire de l'art. 18 CCC n. 26.

Ces **données** sont **plus sensibles** que les données relatives à l'abonné. Le législateur suisse a donc décidé de poser des exigences plus strictes à leur obtention. Il faut donc que les conditions de l'art. 197 al. 1 et 273 al. 1 CPP, soient réalisées cumulativement. L'obtention de ces données n'est donc possible que lorsqu'il existe de graves soupçons laissant présumer qu'un crime ou un délit a été commis. De simples suppositions ou de vagues soupçons ne suffisent pas. L'obtention de ces données n'est pas non plus possible en cas de contravention. A cela s'ajoute que l'obtention doit se justifier au regard de la gravité de l'infraction (principe de proportionnalité) et que les mesures prises jusqu'alors dans le cadre de l'instruction sont restées sans succès ou les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance (principe de subsidiarité). 49

L'obtention de ces données n'est en outre possible qu'avec l'**autorisation** du Tribunal des mesures de contrainte (art. 274 CPP). 50

3. Les données de contenu

Les données de contenu correspondent à la **substance** même **des communications** (art. 8 let. a LSCPT). Il s'agit de l'expression écrite ou orale de la pensée humaine, notamment du texte rédigé par l'auteur d'un courriel ou d'un message ou des paroles prononcées par un interlocuteur lors d'une conversation téléphonique. 51

La surveillance des données de contenu est **la forme de surveillance la plus intrusive** et porte l'atteinte la plus grave au secret des télécommunications et à la sphère privée. Il va dès lors de soi que les exigences posées par le législateur suisse sont les plus élevées des trois types de données. 52

Les données de contenu sont mentionnées à l'art. 21 CCC. Les rédacteurs de la Convention étaient également d'avis que ces données ne pouvaient pas être obtenues pour poursuivre n'importe quelle infraction. Ils ont donc intégré le **principe de proportionnalité** en prévoyant que ces données ne pouvaient être collectées que pour poursuivre certaines infractions graves qui devaient être définies en droit interne. 53

La collecte des données de contenu est régie par l'**art. 269 CPP**. Elle nécessite l'existence de graves soupçons laissant présumer la commission d'un crime ou d'un délit énuméré exhaustivement à l'art. 269 al. 2 CPP. Dans ce cas également, de simples suppositions ou de vagues soupçons ne suffisent pas. 54

L'obtention de ces données doit en outre se justifier au regard de la gravité de l'infraction (principe de proportionnalité). Il ne suffit donc pas que l'infraction poursuivie figure dans la liste de l'art. 269 al. 2 CPP, il faut en outre que la gravité concrète de l'infraction dans le cas d'espèce justifie la mesure de surveillance. Enfin, les mesures prises jusqu'alors dans le cadre de l'instruction sont restées sans succès ou les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance (principe de subsidiarité).

55 Tout comme pour les données relatives au trafic, l'obtention des données de contenu n'est possible qu'avec l'**autorisation** du Tribunal des mesures de contrainte (art. 274 CPP).

IV. FOURNISSEUR DE SERVICES (LET. C)

56 Selon l'art. 1 let. c CCC, « *l'expression « fournisseur de services » désigne toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs* ». Cette définition opère une distinction entre **deux types** de fournisseurs : les fournisseurs d'accès et les fournisseurs de stockage ou de contenu.

A. Les fournisseurs d'accès

57 Les fournisseurs de services visés à l'art. 1 let. c ch. 1 CCC sont les fournisseurs d'accès (*access provider*), c'est-à-dire ceux qui permettent aux utilisateurs de **se connecter à un réseau** et de **communiquer entre eux** au moyen d'un système informatique.

58 Il s'agit en premier lieu des opérateurs de télécommunications (p. ex. Swisscom, SFR, Deutsche Telekom, Vodafone, TIM) qui permettent aux particuliers de se connecter à Internet. Cette définition doit à notre avis être comprise de manière bien plus large et s'étendre à l'ensemble des **entités qui fournissent l'accès à un réseau** par l'intermédiaire d'un système informatique. Sont ainsi concernés les entreprises privées ou les collectivités publiques qui mettent à dispositions des utilisateurs des points d'accès à Internet (p. ex. les compagnies ferroviaires, les hôtels, les communes, etc.), les entreprises privées ou les collectivités publiques qui exploitent un réseau

privé et fournissent à leurs utilisateurs un accès à ce réseau, ainsi que les particuliers qui disposent d'un point d'accès à Internet ou à un réseau domestique, notamment sous la forme d'une borne WiFi, et qui offrent à un tiers la possibilité de s'y connecter.

Cette **interprétation extensive** est confirmée par les rédacteurs de la Convention, qui souligne dans leur Rapport explicatif qu'il est indifférent que les utilisateurs forment un groupe fermé ou que le fournisseur offre ou non ses services au public, gratuitement ou contre le paiement de droits. Le groupe fermé peut être constitué par les salariés d'une entreprise privée auxquels les services sont fournis par un réseau d'entreprise.[18] 59

A notre avis, la formulation « qui offre aux utilisateurs de ses services la possibilité de communiquer » englobe non seulement les entités publiques ou privées qui fournissent l'accès au réseau, mais également toutes celles qui **rendent matériellement possible la communication**. La notion de « fournisseur d'accès » s'étend ainsi à l'ensemble des entités qui mettent à disposition une infrastructure ou un service permettant la transmission, le routage ou l'acheminement des données à travers le réseau, pour autant qu'elles offrent une prestation fonctionnelle de communication aux utilisateurs. Ne sont en revanche pas concernés les acteurs purement techniques ou industriels, qui se limitent à la fabrication, à la fourniture ou à la maintenance d'équipements sans offrir eux-mêmes de service de communication. 60

Sous l'angle purement fonctionnel, la définition de l'art. 1 let. c ch. 1 CCC concerne aussi certaines catégories d'**acteurs intermédiaires du réseau** qui, sans fournir un accès classique à Internet, jouent un rôle déterminant dans la possibilité effective de communiquer au moyen d'un système informatique. Tel est notamment le cas des fournisseurs de services de réseaux privés virtuels (*Virtual Private Network* ou VPN), qui assurent à leurs utilisateurs un accès sécurisé et anonyme à des ressources accessibles via le réseau, combinant des fonctions de routage, de transmission et de chiffrement des communications. 61

Toujours du point de vue fonctionnel, peuvent également être visés par l'art. 1 let. c ch. 1 CCC les **opérateurs de services d'infrastructure** essentiels à la 62

18. Rapport explicatif sur la Convention sur la cybercriminalité, n. 26.

communication sur Internet, tels que les fournisseurs de services de résolution de noms de domaine (DNS) accessibles au public ou les opérateurs de points d'échange Internet (*Internet Exchange Points* ou IXP), pour autant qu'ils offrent une prestation permettant l'acheminement ou l'interconnexion des communications entre utilisateurs ou fournisseurs de réseaux.

B. Les fournisseurs de stockage ou de contenu

63 Les **fournisseurs de services** visés par l'art. 1 let. c ch. 2 CCC sont ceux qui mettent à disposition, gratuitement ou contre rémunération, des espaces de stockage (*hosting providers*) ou du contenu pour les sites web (*content providers*).

64 Les **fournisseurs de stockage** (*hosting providers*) sont des entités qui offrent aux utilisateurs d'Internet des serveurs qui permettent le stockage ou le traitement de données. Ils se subdivisent en **deux catégories** : ceux qui stockent ou traitent des données pour le compte des entités mentionnées au point (i) et ceux qui stockent ou traitent des données pour le compte des utilisateurs des services proposés par les personnes visées au point (ii) :[19]

65 La première catégorie regroupe les fournisseurs de stockage qui traitent ou conservent les données des **fournisseurs d'accès**. Il s'agit en particulier des données relatives au trafic (voir chiffre V ci-dessous), des données du système de noms de domaine (*Domain Name System* ou DNS) qui associe les noms de domaines à l'adresse IP des serveurs sur lesquels ils sont hébergés ou encore des données concernant les différents serveurs par lesquels transitent les courriels.

66 La seconde catégorie concerne les fournisseurs qui stockent ou traitent les données des **utilisateurs** des fournisseurs d'accès. Sont visés, notamment, les entités qui hébergent des sites web, qui proposent des espaces permettant le déploiement de systèmes informatiques virtuels, ou encore des environnements dans lesquels des données peuvent être sauvegardées, gérées ou traitées à distance (*cloud computing*).

67 Dans le contexte du *cloud computing*, la qualification de fournisseur de services au sens de l'art. 1 let. c ch. 2 CCC s'applique indifféremment aux différents modèles de services communément distingués, à savoir

19. Rapport explicatif sur la Convention sur la cybercriminalité, n. 27.

l'infrastructure en tant que service (*Infrastructure as a Service* ou IaaS), la plateforme en tant que service (*Platform as a Service* ou PaaS) et le logiciel en tant que service (*Software as a Service* ou SaaS). Quelle que soit la forme retenue, ces modèles impliquent tous le stockage, le traitement ou la mise à disposition de données informatiques pour le compte de tiers, ce qui justifie leur inclusion dans la définition de fournisseurs de services visés par l'art. 1 let. c ch. 2 CCC.

Font également partie des fournisseurs de services les entités qui exploitent des **réseaux de diffusion de contenu** (*Content Delivery Networks* ou CDN). Ces acteurs assurent la mise en cache, le stockage temporaire et la distribution optimisée de données au moyen de serveurs géographiquement répartis. 68

La définition de l'art. 1 let. c ch. 2 CCC n'est toutefois pas destinée à s'appliquer à un simple fournisseur de contenu (p. ex. à une personne qui passe un contrat avec un fournisseur d'hébergement pour qu'il héberge son site web), si celui-ci ne propose pas en outre des services de communication ou d'autres services de traitement des données.[20] A l'inverse, entrent selon nous dans le champ d'application de la définition de l'art. 1 let. c ch. 2 CCC les sites web qui, au-delà de la mise à disposition de contenus, fournissent des **services de communication**, tels que les sites web qui mettent à disposition des boîtes aux lettres électroniques, des messageries instantanées ou des forums de discussion. Il en va de même des sites web qui offrent des **services de traitement de données**, notamment le chiffrement de données, la traduction de textes, l'analyse financière de données ou encore la collecte automatisée de données non-structurée et leur conversion en données organisées (*web scraping*). 69

Cette analyse s'applique également aux **plateformes en ligne** et aux **réseaux sociaux** qui, au-delà de la diffusion de contenus, offrent des fonctionnalités structurées de communication et d'interaction entre utilisateurs. Ces services impliquent généralement la création de comptes, l'échange de messages, la publication de contenus, ainsi que le traitement automatisé de données à des fins de classification, de publicités ciblées ou de modération. 70

20. Rapport explicatif sur la Convention sur la cybercriminalité, n. 27.

C. Perspectives

71 Enfin, à l'instar de la définition retenue pour les données informatiques, la définition de fournisseur de services est conçue de manière technologiquement neutre. Cette approche lui a permis d'intégrer les **nouveaux types de services** apparus depuis 2001, en particulier les entités qui proposent des services basés sur l'intelligence artificielle pour traiter ou générer des données. Il convient toutefois de préciser que ce n'est pas l'intelligence artificielle en tant que telle qui est visée par la définition, mais bien les fonctions de stockage, de traitement ou de communication de données informatiques qu'elle permet d'assurer.

V. DONNÉES RELATIVES AU TRAFIC (LET. D)

72 La dernière définition fournie par la convention figure à l'art. 1 let. d CCC, aux termes duquel les données relatives au trafic « *désignent toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent* ». Ces données revêtent un **statut juridique particulier**, dans la mesure où elles peuvent servir d'indices, voire de preuves, dans des instructions pénales. Elles sont générées par les différents systèmes informatiques qui interviennent dans la chaîne de communication afin d'acheminer celle-ci de son point d'origine à sa destination. Elles sont donc des auxiliaires de la communication elle-même.[21]

73 Les données relatives au trafic sont nécessaires pour trouver la **source de la communication** ; c'est un point de départ permettant de réunir d'autres preuves ou un élément constitutif de la preuve de l'infraction.[22] Toutefois, en raison du volume considérable de communications échangées quotidiennement, les données relatives à ces communications ont une durée de conservation très limitée. Il est dès lors essentiel d'agir avec célérité afin de retracer l'itinéraire de la communication suspecte avant que les traces ne disparaissent. Compte tenu de la durée souvent importante des procédures ordinaires d'entraide judiciaire internationale en matière pénale, la Convention prévoit la faculté de recourir à la procédure de divulgation rapide

21. Rapport explicatif sur la Convention sur la cybercriminalité, n. 28.
22. Rapport explicatif sur la Convention sur la cybercriminalité, n. 29.

prévue à l'art. 17 CCC. Celle-ci permet d'obtenir sans délai des informations sur l'itinéraire de la communication et de réunir d'autres preuves avant qu'elles ne soient effacées, ou encore d'identifier un suspect.[23] Cette procédure accélérée et moins formelle demeure compatible avec le principe de proportionnalité, dans la mesure où l'obtention de données relatives au trafic porte une atteinte sensiblement moindre aux droits de la personnalité que l'obtention de données relatives au contenu, dès lors qu'elle ne révèle pas le contenu de la communication, mais uniquement son cheminement.

L'art. 1 let. d CCC dresse une liste **exhaustive** des catégories de données relatives au trafic qui sont soumises à un régime particulier dans la Convention,[24] à savoir : l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent. 74

L'**origine** et la **destination** correspondent aux points du réseau à partir desquels une communication est émise et reçue. Ils sont identifiés, selon le mode de communication utilisé, par des numéros de téléphone ou, plus généralement, par des adresses IP attribuées aux systèmes informatiques concernés à un moment donné. Ces identifiants ne permettent pas nécessairement d'identifier directement un utilisateur final, notamment en présence d'adresses IP dynamiques, partagées ou dissimulées par des procédés tels que la traduction d'adresses réseau (NAT), les services de relais (p. ex. le réseau TOR) ou les réseaux privés virtuels (VPN). Ils revêtent une importance particulière pour l'enquête pénale, puisqu'ils permettent de découvrir le système informatique ou le point d'accès au réseau à l'origine ou à la destination de la communication. 75

L'**itinéraire** décrit le parcours emprunté par la communication à travers les différents points de relais du réseau, en particulier les routeurs, les serveurs intermédiaires ou les autres infrastructures de transit. Il correspond à la succession des systèmes informatiques par lesquels les données sont acheminées depuis leur point d'origine jusqu'à leur destination. En pratique, cet itinéraire peut être partiellement ou totalement reconstitué à partir des données générées par ces différents systèmes, sous réserve des limitations techniques liées notamment à l'architecture du réseau, à l'utilisation de services intermédiaires ou au chiffrement des communications. 76

23. Rapport explicatif sur la Convention sur la cybercriminalité, n. 29.
24. Rapport explicatif sur la Convention sur la cybercriminalité, n. 30.

77 L'**heure** et la **date** sont exprimées en temps universel coordonné (UTC). Ces informations sont essentielles lorsqu'on se trouve en présence d'adresses IP dynamiques. Etant donné que ces adresses sont réattribuées en permanence en fonction des besoins des utilisateurs, il est indispensable de disposer de ces informations pour pouvoir demander au fournisseur d'accès à quel système informatique il a attribué une adresse IP à un moment donné. Ces renseignements doivent être obtenus dans les plus brefs délais, dès lors que, selon les Etats, ils ne sont conservés que pour une durée comprise entre six et vingt-quatre mois au maximum. Une fois ce délai écoulé, les données sont détruites et il devient impossible d'identifier l'utilisateur auquel une adresse IP a été attribuée. Cette difficulté n'existe en revanche pas avec les adresses IP statiques, du fait qu'elles sont durablement attribuées aux mêmes utilisateurs.

78 La **taille** de la communication est exprimée en bits ou en octets et correspond au volume de données échangées. Elle peut constituer un indice pour les enquêteurs sur le type de données échangées, dans la mesure où certains types de contenus, tels que les images, les enregistrements sonores ou les contenus audiovisuels, génèrent en principe des volumes de données plus importants que de simples messages textuels. Cet indicateur doit toutefois être interprété avec prudence, compte tenu des techniques contemporaines de compression, de fragmentation et de chiffrement des flux de données.

79 La **durée** de la communication est mesurée en heures, minutes et secondes. Elle correspond au laps de temps pendant lequel une communication a été établie ou un échange de données a eu lieu entre les systèmes informatiques concernés. Cette information peut fournir des éléments contextuels utiles à l'enquête, notamment pour distinguer des communications ponctuelles de connexions prolongées ou répétées, sans toutefois révéler le contenu des échanges intervenus durant cette période.

80 Enfin, le **type de service sous-jacent** fait référence au mode de communication ou à la catégorie fonctionnelle de service utilisée dans le cadre de l'échange de données, tels que la messagerie électronique, les services de messagerie instantanée, la visualisation de contenus audiovisuels en ligne ou encore le téléchargement de données. Il s'agit d'une qualification générale du service mobilisé, qui peut s'avérer délicate à établir avec précision lorsque plusieurs services sont combinés au sein d'un même flux de communication ou lorsque les données sont encapsulées ou chiffrées.

BIBLIOGRAPHIE

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

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 10.01.2026 (cité : Rapport explicatif de la Convention sur la cybercriminalité).

Comité de la Convention cybercriminalité (T-CY), Guidance Notes, disponible sous https://www.coe.int/fr/web/cybercrime/guidance-notes, visité le 10.01.2026 (cité : Note d'orientation).

COMMENTAIRE

Art. 2 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jérémie Müller

PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 2 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 2 CCC N. XXX.

Chapitre II: Mesures à prendre au niveau national

Section 1: Droit pénal matériel

Titre 1: Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Art. 2 Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

TABLE DES MATIÈRES

I. Géneralités 33
II. Bien Juridiquement protégé 34
III. Éléments constitutifs fondamentaux 34
A. Un système informatique 34
B. Un accès au système informatique 35
C. L'illicéité 37
D. L'intention 38
IV. Éléments constitutifs supplémentaires facultatifs 39
A. Accès en violation des mesures de sécurité 39
B. Le dessein d'obtenir des données informatiques ou un autre dessein spécial 41
C. Un système informatique connecté à un autre système informatique 43
V. Comparaison avec le droit suisse 44
Bibliographie 45
Travaux législatifs 46

I. GÉNERALITÉS

L'accès illégal à un système informatique constitue l'**infraction de base** dans le domaine de la cybercriminalité. Il s'agit souvent du comportement délictueux préalable nécessaire à la commission d'une autre infraction informatique, telle que l'atteinte à l'intégrité de données (art. 4 CCC), l'atteinte à l'intégrité du système (art. 5 CCC), la falsification informatique (art. 7 CCC) ou la fraude informatique (art. 8 CCC). Toutefois, certains cybercriminels se contentent d'accéder sans droit à un système informatique, par bravade ou pour le seul défi technique que cela représente, sans commettre d'infraction subséquente. Il est donc justifié d'ériger en infraction ce comportement en tant que tel, plutôt qu'il soit absorbé par les infractions réprimées par les articles suivants. Ainsi, l'auteur se rend coupable d'accès illégal du seul fait qu'il se fraie un accès vers un système informatique. Il n'est pas nécessaire qu'il vole ou modifie des données dans le système informatique. 1

D'aucuns pourraient voir dans le *hacking* une activité ludique, relativement inoffensive, à laquelle s'adonnent quelques *geeks* en quête de nouveaux défis. La réalité est toutefois tout autre. Ce comportement est bien plus **répandu** qu'on pourrait le croire au premier abord et ses auteurs poursuivent des buts bien moins honorables que le simple divertissement. 2

Naturellement, la mise en place de mesures de sécurité fortes est le moyen le plus efficace pour protéger un système informatique contre des accès non-autorisés. Compte tenu de la menace ou de l'atteinte à la sécurité des systèmes et des données informatiques que le *hacking* représente, les mesures techniques doivent être accompagnées de **mesures législatives** destinées à dissuader les cybercriminels de passer à l'acte ou à les sanctionner en cas de commission d'actes malveillants[25]. De cette manière, l'intérêt des organisations et des particuliers à pouvoir diriger, exploiter et contrôler leurs systèmes informatiques sans perturbation ni entrave d'aucune sorte est protégé au mieux[26]. 3

25. Rapport explicatif de la Convention sur la cybercriminalité, n. 45.
26. Rapport explicatif de la Convention sur la cybercriminalité, n. 44.

II. BIEN JURIDIQUEMENT PROTÉGÉ

4 L'art. 2 CCC protège **l'inviolabilité** des systèmes informatiques. Cette protection par le droit pénal s'impose pour au moins deux raisons.

5 D'une part, l'accès illégal à un système informatique peut engendrer des **coûts** de remise en état importants chez l'ayant-droit. Les auteurs modifient en effet souvent des données pour s'introduire à l'intérieur du système. De plus, les victimes ne se rendent souvent compte de l'intrusion que quelque temps après qu'elle a eu lieu. Il est dès lors particulièrement difficile de retrouver ce qui a été modifié par les auteurs, ainsi que les nouvelles données générées par le système informatique à la suite de cette modification. Une fois identifiées, ces données doivent être remises dans leur état d'origine. Ces opérations peuvent nécessiter beaucoup de temps travail et peuvent donc être très onéreuses[27].

6 D'autre part, l'accès illégal permet aux auteurs de **consulter** des informations auxquelles ils ne devraient pas avoir accès (p. ex. rapports confidentiels, secrets commerciaux, listes de clients, pièces comptables, numéros de carte de crédit, données personnelles, ...). Ces informations peuvent ensuite être revendues au marché noir, ce qui peut engendrer un dommage encore bien plus important pour l'ayant-droit que la seule remise en état de la protection du système[28].

III. ÉLÉMENTS CONSTITUTIFS FONDAMENTAUX

A. Un système informatique

7 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

27. Rapport explicatif de la Convention sur la cybercriminalité, n. 44.
28. Rapport explicatif de la Convention sur la cybercriminalité, n. 44.

permettent la connexion de ces différents éléments les uns aux autres (câbles, routeur, borne wifi, ...).

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. 8

B. Un accès au système informatique

On pourrait être tenté de comparer l'accès illégal à un système informatique à l'infraction de violation de domicile. L'accès au système informatique serait ainsi l'équivalent numérique de l'introduction dans le logement. Cette **analogie** a ceci de rassurant que l'on peut très bien se représenter intellectuellement la situation. Le monde virtuel est toutefois plus complexe que cela et les contours des notions juridiques nécessairement plus flous. 9

Il est compliqué de faire une analogie avec le monde réel. S'il fallait néanmoins en faire une, l'accès à un système informatique pourrait être comparé au fait d'entrer dans un **château-fort** du Moyen-Âge. L'accès au château est limité par un mur d'enceinte et des douves. La porte d'entrée principale est généralement surveillée par des gardes. Ceux-ci contrôlent que les personnes qui entrent dans la forteresse y sont bien autorisées. Une fois à l'intérieur, les individus peuvent accéder à certaines parties du château et pas à d'autres, en fonction de leur rang. Le rang est défini par le seigneur auquel le château appartient. Dans chaque partie du château se trouvent des objets qui peuvent être regardés, touchés, modifiés ou même détruits. Pour ces objets également, c'est le seigneur du château qui détermine qui peut faire quoi avec quel objet. Le seigneur est le seul à pouvoir accéder à toutes les pièces du château et à pouvoir agir comme bon lui semble avec tous les objets du château. 10

Dans un système informatique le fonctionnement est **similaire** à celui du château-fort. Pour pouvoir accéder au système informatique l'utilisateur doit généralement entrer un identifiant et un mot de passe. Une fois connecté, l'utilisateur peut accéder à tout ou partie du système informatique en fonction de son niveau d'accréditation, qui est déterminé par l'administrateur du système informatique. Ce niveau d'accréditation détermine également ce que l'utilisateur peut faire ou non dans les parties du système informatique auxquelles il a accès, à savoir uniquement voir le titre des documents contenus dans un dossier, les ouvrir pour les lire, les éditer ou les supprimer. 11

L'administrateur est le seul à pouvoir accéder à tout le système informatique et à disposer des droits qui lui permettent d'effectuer toutes les actions qu'il souhaite avec les données qui s'y trouvent.

12 L'analogie avec le monde réel s'arrête cependant là. En effet, la notion d' « accès » dans le monde virtuel ne peut pas être comparée à celle de « pénétrer », dans le monde réel. En informatique, la notion d' « accès » signifie que l'auteur parvient à établir une **connexion** avec tout ou partie d'un système informatique. Il n'y a donc pas à proprement parler de déplacement physique de l'auteur d'un endroit vers un autre.

13 Dans la forme simple de l'infraction, le **moyen** utilisé par l'auteur pour se connecter au système informatique est sans importance. L'auteur peut donc établir une connexion au moyen d'un accès local ou d'un accès à distance. Si l'auteur établit une connexion locale avec un système informatique auquel il a physiquement accès, celle-ci se fera au moyen d'un clavier – matériel ou virtuel – et d'une souris, voire simplement avec les doigts pour les tablettes et les *smartphones*. Il peut aussi utiliser un terminal pour se connecter à un système informatique central. Si l'auteur décide au contraire d'établir une connexion à distance, il peut passer par n'importe quel réseau de télécommunication. Le type de réseau (local, public, privé, ...), ainsi que le type de connexion (avec ou sans fil) sont sans importance.

14 **L'étendue** de l'accès n'est pas non plus décisif pour la réalisation de l'infraction. L'accès peut être total, auquel cas il s'étend à l'ensemble du système informatique. Il peut aussi n'être que partiel. Dans ce cas il ne concerne qu'une partie du système informatique. Tel est par exemple le cas lorsque l'auteur n'accède qu'à la session d'un utilisateur ou à une partie des données stockées sur un serveur.

15 L'infraction est **consommée** dès que la connexion avec le système informatique est établie. Plus rien n'empêche alors l'auteur de prendre connaissance des données informatiques contenues dans le système informatique. Il n'est cependant pas nécessaire que l'auteur en prenne connaissance pour que l'infraction soit consommée. En pratique, ces deux évènements coïncident néanmoins le plus souvent, car au moment où l'accès est établi, les données s'affichent à l'écran.

16 La notion d'accès au sens de l'art. 2 CCC doit clairement être **distinguée** de l'atteinte à l'intégrité des données qui figure à l'art. 4 CCC. Pour réaliser

l'infraction, il suffit que l'auteur se ménage un accès vers un système informatique. Même si, en pratique, l'établissement d'un accès illégal entraîne régulièrement la modification de données, de telles détériorations ne sont pas nécessaires à la commission de l'infraction.

Enfin, seul l'établissement d'un accès illégal est punissable. Le **maintien** d'un accès, établi de manière licite, après que l'ayant-droit du système informatique a informé l'utilisateur qu'il n'était plus autorisé à y accéder, n'est pas punissable. On peut notamment penser à l'employé qui, au cours de son activité professionnelle, utilise son ordinateur privé pour se connecter au réseau de l'entreprise et qui, une fois licencié, continue à consulter des fichiers de la société. L'absence de punissabilité ne dure toutefois que le temps de la connexion. S'il interrompt la connexion et en établit une nouvelle, il se rend alors coupable de l'infraction. Cette absence de punissabilité constitue à notre avis clairement une lacune improprement dite, les Parties n'ayant sans doute tout simplement pas envisagé cette possibilité lors de l'élaboration du texte. 17

C. L'illicéité

Pour être punissable, l'auteur doit avoir agi sans droit. Cela implique de déterminer dans un premier temps si le système informatique est public – c'est-à-dire ouvert à tous – ou si son **accès** est **limité**, voire une combinaison des deux. Si le système informatique est public, l'accès ne peut en aucun cas être illicite et toute infraction est exclue. En revanche, si l'accès à tout ou partie du système informatique est restreint, celui qui y accède sans autorisation est punissable. 18

C'est l'ayant droit du système informatique qui détermine qui est **autorisé** à accéder à quelle partie du système informatique. Sont ainsi punissables non seulement les personnes qui n'ont pas été autorisées à accéder au système informatique, mais également celles qui ont été autorisées à accéder à une partie du système informatique, mais qui accèdent à une autre partie du système informatique à laquelle l'accès ne leur a pas été accordé. Ne sont en revanche pas punissables les personnes qui ont été autorisées à accéder au système informatique par son ayant-droit et qui se conforment aux limites de cet accès. 19

20 L'ayant droit du système informatique n'en est pas toujours l'administrateur. C'est en particulier le cas des systèmes informatiques de taille moyenne et grande. Dans ces situations, la gestion du système informatique est déléguée par son ayant-droit à un administrateur tiers. Cet **administrateur** peut être soit une personne physique, soit une personne morale. Dans les deux cas, l'ayant-droit du système informatique autorise l'administrateur à y accéder pour accomplir sa mission. L'administrateur n'accède donc pas sans droit au système informatique tant qu'il le fait dans le but d'accomplir sa mission. En revanche, l'accès est non-autorisé lorsqu'il s'effectue dans un autre but, comme par exemple consulter des informations privées ou confidentielles qui ne lui sont pas destinées.

21 Lorsque la gestion du système informatique est déléguée à une **entreprise**, toutes les personnes physiques chargées de cette mission au sein de cette société sont autorisées à y accéder. Tel n'est en revanche pas le cas des personnes physiques au sein de cette personne morale auxquelles cette tâche n'a pas été attribuée. Si ces personnes accèdent au système informatique, elles le font sans droit, car elles ne le font pas pour accomplir la mission qui a été confiée à la personne morale.

22 La personne spécifiquement mandatée pour **tester** la sécurité du système informatique, qui réussit à accéder au système informatique en déjouant les mesures de protection mises en place, n'agit pas de manière illicite, car elle y a été autorisée par son ayant-droit.

D. L'intention

23 L'accès illégal est **intentionnel**. L'intention doit porter sur tous les éléments objectifs de l'infraction. L'auteur doit donc avoir conscience qu'il accède sans droit à un système informatique et en avoir la volonté. Le dol éventuel suffit. Si l'auteur se doute qu'il accède à tout ou partie d'un système informatique auquel il ne devrait pas avoir accès, mais établit une connexion malgré tout, il se rend coupable d'accès illégal. En revanche, si l'auteur commet une erreur de manipulation et établit une connexion non-autorisée, malgré lui, l'intention fait défaut et l'infraction n'est pas réalisée.

24 La norme ne réprime que l'établissement de l'accès illégal et non le fait de **maintenir** l'accès contre la volonté de l'ayant-droit. Partant, celui qui accède

à un système informatique par inadvertance, mais qui, une fois connecté, en explore le contenu, n'est pas punissable.

Lorsque l'auteur pense à tort que le système informatique auquel il accède est public ou qu'il pense à tort être en droit d'y accéder pour une autre raison, il commet une **erreur** sur les faits. 25

IV. ÉLÉMENTS CONSTITUTIFS SUPPLÉMENTAIRES FACULTATIFS

Au moment de l'élaboration de la Convention sur la cybercriminalité, une majorité des Parties voulaient ériger en infraction le **piratage** pur et simple. D'autres étaient en revanche opposés à une pénalisation générale du *hacking*, au motif que la simple intrusion ne cause pas forcément des dommages et que, dans certains cas, les actes de *hacking* permettent même de découvrir des failles de sécurité et de les combler[29]. Pour tenir compte de ces considérations et comme les législations nationales de nombreux pays contenaient déjà des dispositions qui réprimaient le piratage sous des formes diverses, il a été donné la possibilité aux Parties de limiter la punissabilité de l'accès illégal en exigeant la réalisation d'un ou plusieurs éléments constitutifs supplémentaires. 26

A. Accès en violation des mesures de sécurité

La Convention sur la cybercriminalité donne tout d'abord la possibilité aux Parties de ne sanctionner l'accès illégal que lorsqu'il est commis en violation de mesures de sécurité. L'**Allemagne**, la **Finlande**, le **Japon**, la **Lituanie**, le **Pérou**, la **République slovaque**, la **République tchèque** et la **Suisse** ont fait usage de cette faculté[30]. 27

Cette exigence supplémentaire signifie que le système informatique doit être **protégé** contre un accès non-autorisé. En d'autres termes, si l'auteur accède sans droit à un système informatique qui n'est pas protégé, il n'est pas punissable. 28

La notion de **mesures de sécurité** doit être comprise de manière large. Elle englobe tant les mesures de sécurité physiques que virtuelles. En ce qui 29

29. Rapport explicatif de la Convention sur la cybercriminalité, n. 49.

concerne les mesures de sécurité physiques, le système informatique peut par exemple se trouver dans une pièce fermée à laquelle on ne peut accéder qu'avec une clé, un badge magnétique, une empreinte digitale, rétinienne ou vocale. Sur le plan virtuel, les mesures de sécurité peuvent notamment consister en une protection par pare-feu, code PIN, mot-de-passe, ou encore une double, voire même triple authentification.

30 Si l'auteur ne parvient pas à déjouer les mesures de sécurité ou s'il décide spontanément de mettre un terme à son activité avant de les avoir franchies, seule une **tentative** est envisageable. Cela pose toutefois problème puisqu'à

30. 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 § 202a du Code pénal allemand ; Déclaration de la Finlande consignée dans l'instrument de ratification déposé le 24 mai 2007 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=FIN, visité le 21.1.2024), en lien avec le chapitre 38, section 8 du Code pénal finlandais ; 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. 2 et 3 de la Loi japonaise sur l'interdiction de l'accès à un système informatique non autorisé ; Déclaration 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=10&codePays=LIT, visité le 21.1.2024), en lien avec l'art. 198[1] du Code pénal lituanien ; 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. 2 de la Loi péruvienne sur les délits informatiques ; Déclaration de la République slovaque consignée dans l'instrument de ratification déposé le 8 janvier 2008 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185 &codeNature=10&codePays=SLK, visité le 21.1.2024), en lien avec le § 247 du Code pénal slovaque ; Déclaration de la République tchèque consignée dans l'instrument de ratification déposé le 22 août 2013 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185 &codeNature=10&codePays=CZE, visité le 21.1.2024), en lien avec le § 230 du Code pénal tchèque ; 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[bis] CP.

la lecture de l'art. 11 § 2 CCC, on constate qu'il n'est pas exigé des Parties qu'elles répriment la tentative d'accès illégal. Chaque Etat est donc libre de traiter cet aspect comme il le souhaite, de sorte que ce comportement pourrait, selon la législation nationale des Etats Parties, ne pas être punissable du tout.

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

Une autre possibilité donnée aux Parties est d'exiger que l'auteur ait agi dans un **dessein spécial**. Plusieurs Etats ont fait usage de cette possibilité. 31

Les **Etats-Unis d'Amérique** ont décidé d'exiger que l'auteur ait agi dans le but d'obtenir des données[31]. Bien que cette possibilité ait été donnée aux Parties, son utilisation est regrettable car elle vide la norme d'une grande partie de sa substance. Cette disposition a en effet spécifiquement été élaborée pour réprimer les actes des hackers qui accèdent à des systèmes informatiques par bravade, sans toutefois s'intéresser aux données qu'ils contiennent. Exiger ce dessein spécial précis semble donc contraire à l'esprit de la norme. 32

La **Belgique**, quant à elle, a déclaré n'incriminer l'accès illégal que lorsqu'il est commis dans une intention frauduleuse ou à dessein de nuire[32]. L'intention frauduleuse semble se rapporter à la volonté d'obtenir un avantage indu pour soi-même ou pour autrui. Quant au dessein de nuire, il s'agit vraisemblablement de la volonté de causer un préjudice à autrui sous quelque forme que ce soit. 33

La **Principauté d'Andorre** et la **République slovaque** ont décidé de ne poursuivre l'accès illégal que s'il était commis dans le but d'obtenir des 34

31. 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 18 § 1030 section a chiffre 1 à 3 du Code des Etats-Unis (Computer Fraud and Abuse Act).
32. 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. 550bis § 2 du Code pénal belge.

données sans droit, de les détériorer (en ce qui concerne la Principauté d'Andorre uniquement) ou dans un autre dessein délictueux[33]. Cette formulation vise à éviter que des auteurs échappent à la condamnation en raison du fait qu'ils poursuivaient un autre dessein que l'obtention ou la détérioration de données. A notre avis, elle doit toutefois être interprétée à la lumière des desseins spéciaux énumérés à l'art. 2 CCC et s'y apparenter à la fois en ce qui concerne le but poursuivi par l'auteur et son intensité délictuelle. Le 1er janvier 2021, le Code pénal slovaque a été modifié et la réserve de la République slovaque adaptée[34]. Le § 247 a été remanié. Dans sa forme simple, cette disposition n'exige plus aucun dessein spécial (§ 247 par. 1). Le § 247 par. 2 prévoit en revanche une forme qualifiée lorsque l'auteur cause un préjudice considérable.

35 Enfin, le **Canada** a indiqué qu'il ne poursuivrait l'accès illégal que s'il était commis avec une intention délictueuse[35]. Cette dernière notion est particulièrement peu 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.

36 Le **Chili** avait initialement émis une réserve identique à celle du Canada[36]. Il a toutefois modifié sa législation en 2022. Dans sa nouvelle version, l'*acceso ilícito* est punissable lorsqu'il est commis intentionnellement[37]. Un dessein

33. Réserve consignée dans une Note Verbale du Ministère des Affaires étrangères d'Andorre, datée du 14 octobre 2016, déposée avec l'instrument de ratification le 16 novembre 2016 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2& codePays=AND), en lien avec les art. 182 et 225 du Code pénal andorran ; Déclaration de la République slovaque consignée dans l'instrument de ratification déposé le 8 janvier 2008, (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10 &codePays=SLK, visité le 21.1.2024), en lien avec l'ancien § 247 du Code pénal slovaque.
34. Déclaration consignée dans l'instrument de ratification déposé le 8 janvier 2008, amendée dans une Note verbale de la Représentation Permanente de la République slovaque, datée du 30 avril 2021, enregistrée au Secrétariat Général le 30 avril 2021 (disponible sous https://www.coe.int/fr/web/conventions/full-list? module=declarations-by-treaty&numSte=185&codeNature=10&codePays=SLK, visité le 21.1.2024), en lien avec le nouveau § 247 du Code pénal slovaque.
35. Déclaration consignée dans une Note Verbale de la Mission du Canada auprès de l'Union européenne, déposée avec l'instrument de ratification le 8 juillet 2015 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=CAN, visité le 21.1.2024), en lien avec l'art. art. 342.1 du Code pénal canadien.

spécial n'est plus exigé. Cependant, lorsque l'accès illégal est commis dans le but d'obtenir ou d'utiliser les données contenues dans le système informatique, la peine est augmentée[38].

C. Un système informatique connecté à un autre système informatique

La Convention sur la cybercriminalité permet enfin aux Parties de limiter la punissabilité de l'accès illégal aux **connexions** établies sans droit avec un système informatique par l'intermédiaire d'un autre système informatique. En faisant usage de cette possibilité, les Parties peuvent exclure les cas dans lesquels l'auteur accède physiquement au système informatique qu'il vise, sans passer par un réseau. 37

Les seuls Etats à avoir fait usage de cette possibilité sont la **République slovaque** et le **Japon**[39]. Le Code pénal slovaque a depuis été modifié. La nouvelle teneur du § 247, entrée en vigueur le 1er janvier 2021, ne prévoit plus cette exigence dans sa version actuelle, de sorte que la réserve de la République slovaque a été adaptée[40]. 38

36. 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. 2 de la Loi chilienne N° 19.223 sur les délits informatiques.
37. Art. 2 al. 1 de la Loi chilienne N° 21.459 sur les délits informatiques.
38. Art. 2 al. 2 de la Loi chilienne N° 21.459 sur les délits informatiques.
39. Déclaration de la République slovaque consignée dans l'instrument de ratification déposé le 8 janvier 2008 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185 &codeNature=10&codePays=SLK, visité le 21.1.2024), en lien avec l'ancien § 247 du Code pénal slovaque ; 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. 2 et 3 de la Loi japonaise sur l'interdiction de l'accès à un système informatique non autorisé.
40. Déclaration consignée dans l'instrument de ratification déposé le 8 janvier 2008, amendée dans une Note verbale de la Représentation Permanente de la République slovaque, datée du 30 avril 2021, enregistrée au Secrétariat Général le 30 avril 2021 (disponible sous https://www.coe.int/fr/web/conventions/full-list? module=declarations-by-treaty&numSte=185&codeNature=10&codePays=SLK, visité le 21.1.2024), en lien avec le nouveau § 247 du Code pénal slovaque.

V. COMPARAISON AVEC LE DROIT SUISSE

39 En droit suisse, le *hacking* est réprimé par l'**art. 143bis CP**. Cette disposition sanctionne l'accès indu au système informatique d'autrui, spécialement protégé contre tout accès, au moyen d'un dispositif de transmission de données. Cette norme ne correspond toutefois pas aux exigences de l'art. 2 CCC à trois égards.

40 Premièrement, la convention n'effectue pas de distinction entre les systèmes informatiques. Elle protège l'intégrité de tous les systèmes informatique, indépendamment de leur appartenance. L'art. 143bis al. 1 CP, en revanche, incrimine uniquement l'accès indu au système informatique « **appartenant à autrui** ». Compte tenu du fait que cette disposition se trouve dans le titre 2 du Code pénal, soit des infractions contre le patrimoine, cette formulation doit être interprétée au regard des droits réels[41]. Le système informatique doit donc appartenir à une personne autre que l'auteur. Si l'auteur est le propriétaire ou le copropriétaire du système informatique, cet élément constitutif n'est pas réalisé puisqu'il n'appartient pas à autrui. Ainsi, si plusieurs sessions ont été ouvertes dans le même système informatique, l'auteur, (co)propriétaire du système informatique, qui accède à une autre session que la sienne n'est pas punissable[42]. La doctrine majoritaire estime au contraire qu'il faut comprendre par « appartenant à autrui » qu'une personne autre que l'auteur est autorisée à accéder et à disposer du système informatique ou d'un sous-système informatique[43]. Une telle interprétation rendrait toutefois la notion « appartenant à autrui » redondante avec l'élément constitutif de l'illicéité de l'accès. Si le législateur a mentionné ces deux éléments de manière distincte, c'est qu'il s'agit de deux notions qui doivent être analysées indépendamment l'une de l'autre. Pour être conforme à la convention, le terme « autrui » figurant à l'art. 143bis al. 1 CP devrait donc être supprimé.

41 L'art. 143bis al. 1 CP exige que l'auteur ait accédé au système informatique à l'aide d'un **dispositif de transmission de données**[44]. Cela a par exemple

41. Schmid, § 5 n. 17. Contra : Weissenberger, n. 12 ad art. 143bis CP.
42. Schmid, § 5 n. 17.
43. Dupuis et al., n. 10 ad art. 143bis CP ; Pfister, pp. 105-106; Stratenwerth / Bommer, § 14 n. 39 ; Trechsel / Crameri, n. 4 ad art. 143bis CP ; Weissenberger, n. 13 ad art. 143bis CP.
44. Dupuis et al., n. 17 ad art. 143bis CP ; Trechsel / Crameri, n. 7 ad art. 143bis CP ; Weissenberger, n. 17 ad art. 143bis CP.

pour conséquence que l'auteur qui profite de l'absence de sa victime pour entrer dans son bureau et se connecter directement à son ordinateur ne se rend pas coupable d'accès indu à un système informatique puisqu'il n'utilise pas un dispositif de transmission de données[45]. L'art. 2 § 2 CCC permet aux Parties de limiter la poursuite pénale à l'accès illégal commis au moyen d'un système informatique connecté à un autre système informatique. La Suisse n'a toutefois pas déclaré faire usage de cette possibilité. En conséquence, l'élément constitutif de l'accès au moyen d'un dispositif de transmission de données devrait être supprimé.

Enfin, l'art. 143bis 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 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 l'accès indu à un système informatique d'office[46]. 42

Au vu de ce qui précède, force est de constater que le droit suisse n'est **pas conforme** à l'art. 2 CCC. L'art. 143bis CP devrait par conséquent être modifié. 43

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

Dupuis Michel / Geller Bernard / Monnier Gilles / Moreillon Laurent / Piguet Christophe / Bettex Christian / Stoll Daniel (éditeurs), Code pénal - Petit commentaire, 2. éd., Bâle 2017

Pfister Christa, Hacking in der Schweiz, Diss., Zürich, 2008

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

45. FF 1991 II 979 ; Pfister, p. 115 ; Trechsel / Crameri, n. 7 ad art. 143bis CP ; Weissenberger, n. 18 ad art. 143bis CP.
46. Schwarzenegger, p. 317 et les références citées.

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

Stratenwerth Günter / Bommer Felix, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 8. éd., Berne, 2022

Trechsel Stefan / Crameri 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 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, visité le 21.1.2024

COMMENTAIRE

Art. 3 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jérémie Müller

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 49
II. Bien juridiquement protégé 49
III. Éléments constitutifs de base 49
A. Des données informatiques 49
B. Une transmission non publique 50
1. La notion de transmission 50
2. Le caractère non public 51
C. Le cas particulier des émissions électromagnétiques 52
D. L'interception par des moyens techniques 53
E. L'illicéité 54
F. L'intention 56
IV. Éléments constitutifs supplémentaires facultatifs 56
A. Le dessein d'obtenir des données informatiques ou un autre dessein spécial 56
B. Un système informatique connecté à un autre système informatique. 58
V. Comparaison avec le droit suisse 58
Bibliographie 60
Travaux législatifs 60

I. GÉNÉRALITÉS

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. 1

II. BIEN JURIDIQUEMENT PROTÉGÉ

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[47]. 2

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Des données informatiques

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. 3

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. 4

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

B. Une transmission non publique

1. La notion de transmission

5 Contrairement à ce que l'étymologie du terme « **transmission** »[48] 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, 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

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

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, ...).

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[49]. 10

2. Le caractère non public

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[50]. Il importe donc peu que les données transmises soient publiques ou privées. Seule la **nature** de la transmission est déterminante. 11

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 ». 12

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. 13

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 14

49. A ce sujet, voir le ch. IV let. B ci-dessous.
50. Rapport explicatif de la Convention sur la cybercriminalité, n. 54.

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.

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.

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. 19

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. 20

D. L'interception par des moyens techniques

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. 21

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. 22

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[51].

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

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

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[52].

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 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[53]. 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[54]. 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

52. Arrêt CourEDH Szabó et Vissy contre Hongrie du 12 janvier 2016 (37138/14).
53. 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).
54. Arrêt CourEDH Barbulescu contre Roumanie du 5 septembre 2017 (61496/08).

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 indue 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[55].

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.

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

Le **Canada**, le **Japon** et le **Pérou** ont indiqué qu'ils ne poursuivraient 34
l'interception illégale que si elle était commise avec une intention délictueuse[56]. Cette dernière notion est particulièrement peut 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.

Le **Chili** avait initialement émis une réserve identique à celle du Canada, du 35
Japon et du Pérou[57]. Il a toutefois modifié sa législation en 2022. Dans sa nouvelle version, l'*interceptación ilícita* ne nécessite plus de dessein spécial[58].

La **Suisse**, quant à elle, a déclaré qu'elle ne poursuivrait l'interception illégale 36
que si l'auteur avait agi dans un dessein d'enrichissement illégitime[59].

Alors qu'ils avaient déclaré ne poursuivre l'accès illégal qu'à la condition que 37
l'auteur soit animé par un dessein spécial[60], 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.

---

56. Déclaration consignée dans une Note Verbale de la Mission du Canada auprès de l'Union européenne, déposée avec l'instrument de ratification le 8 juillet 2015 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=CAN, visité le 21.1.2024), en lien avec l'art. 342.1 du Code pénal canadien ; 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.
57. 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.
58. Art. 3 de la Loi chilienne N° 21.459 sur les délits informatiques.
59. 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.
60. Voir Art. 2 CCC nn. 32-34.

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**[61].

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[62].

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[63] 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 »[64]. Il s'agissait selon lui d'une combinaison des art. 143, 143bis et 321ter CP. En réalité, tel n'est absolument pas le cas.

41 L'**art. 143bis CP** ne réprime que les intrusions dans un système informatique et non l'interception de données[65].

61. 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.
62. Voir Art. 2 CCC n. 38.
63. FF 2010 4275.
64. FF 2010 4282.
65. Weissenberger, n. 17 et 20 ad art. 143bis CP.

En ce qui concerne l'**art. 321ter 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[66]. 42

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. 43

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 »[67]. Le bien juridique protégé par l'art. 143 CP devrait donc être adapté. 44

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[68]. Or, en pratique, c'est le cas le plus courant, car les données transmises électroniquement ne sont généralement pas spécialement protégées contre tout accès[69]. 45

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[70]. 46

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[71]. 47

66. Oberholzer, n. 3 ad art. 321ter CP ; Trechsel / Lehmkuhl, n. 3 ad art. 321ter CP.
67. FF 1991 II 977 ; SCHMID, § 4 n. 14ss ; Trechsel / Crameri, n. 2 ad art. 143 CP.
68. Treccani, p. 218ss.
69. Schwarzenegger, p. 320.
70. Schwarzenegger, pp. 320-321.
71. Schwarzenegger, p. 321 ; Treccani, p. 233.

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 Jacquey, 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

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 / Crameri 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, 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

COMMENTAIRE

Art. 4 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jérémie Müller

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 65
II. Bien juridiquement protégé 65
III. Éléments constitutifs de base 65
A. Des données informatiques 65
B. Un comportement punissable 66
1. La suppression et l'effacement de données 66
2. L'endommagement, la détérioration et l'altération de données 67
3. Le mode de commission 68
C. L'illicéité 69
D. L'intention 70
IV. Élément constitutif supplémentaire facultatif 70
V. Comparaison avec le droit suisse 72
Bibliographie 73
Travaux législatifs 73

I. GÉNÉRALITÉS

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. 1

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. 2

Au vu de l'importance croissance 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. 3

II. BIEN JURIDIQUEMENT PROTÉGÉ

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 informatiques[72]. 4

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Des données informatiques

Aux termes de l'art. 1 let. b CCC, « l'expression "données informatiques" désigne toute **représentation** de faits, d'informations ou de concepts sous 5

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

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. 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 support[73].

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

73. 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).

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.

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 récupérables[74]. 10

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

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 ISO[75]. 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. 11

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. 12

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 13

74. 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.
75. Norme ISO 27001.

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 existantes[76]. Cette modification peut concerner tant la forme que le contenu des données. Il s'agit d'un terme très large qui englobe 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*[77] 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

76. Rapport explicatif de la Convention sur la cybercriminalité, n. 61.
77. Application programmée pour effectuer une ou plusieurs tâches déterminées de manière automatisée.

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

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. 18

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*, *Telegraph* 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. 19

Un autre cas de modification de données par acte concluant réside dans les **mises 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 l'utilisateur à installer une nouvelle version de l'application, faute de quoi elle devient inutilisable, ou les données illisibles, se rend punissable. 20

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 21

ne peut toutefois être opérée que dans des cas graves et doit être soumise à un contrôle judiciaire postérieur[78].

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 souhaite[79]. 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 recréation des données, de même qu'aux conséquences de la disparition ou de l'impossibilité d'utiliser les données.

78. Arrêt CourEDH Szabó et Vissy contre Hongrie du 12 janvier 2016 (37138/14).
79. Rapport explicatif de la Convention sur la cybercriminalité, n. 64.

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. 27

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 devait être interprétée comme ayant causé des dommages sérieux[80]. 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 graves[81]. On constate donc que même si la lettre de la convention permettait une interprétation très large, tous les Etats 28

80. 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&num Ste=185&codeNature=2&codePays=LIT, visité le 21.1.2024), en lien avec l'art. 198^2 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).

81. 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.

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. 144bis 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. 144bis 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. 144bis ch. 1 CP protège le droit de disposer de données intactes[82]. 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. 144bis 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 transformation[83]. La notion d'« effacement » évoquée dans la convention, à savoir la destruction définitive de données, est identique en droit suisse[84]. 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 données[85].

32 Enfin, l'art. 144bis 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 donné qu'il existe un conflit

82. Schmid, § 6 n. 14 ; Trechsel / Crameri, n. 2 ad art. 144bis CP ; Weissenberg, n. 6 ad art. 144bis CP.
83. Corboz, n. 5 ad art. 144bis CP ; Schmid, § 6 n. 26 ; Trechsel / Crameri, n. 5 ad art. 144bis CP ; Weissenberg, n. 21-22 ad art. 144bis CP.
84. Corboz, n. 5 ad art. 144bis CP ; Schmid, § 6 n. 27 ; Trechsel / Crameri, n. 6 ad art. 144bis CP ; Weissenberg, n. 8 ad art. 144bis CP.
85. Corboz, n. 5 ad art. 144bis CP ; Schmid, § 6 n. 29 ; Trechsel / Crameri, n. 7 ad art. 144bis CP ; Weissenberg, n. 33 ad art. 144bis CP.

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 cas[86] 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 / Crameri 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)

86. Schwarzenegger, p. 317.

Art. 4 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

COMMENTAIRE

Art. 5 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jérémie Müller

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 77
II. Bien juridiquement protégé 78
III. Éléments constitutifs de base 78
A. Un système informatique 78
B. Un comportement punissable 78
1. L'introduction de données 78
2. La transmission de données 79
3. L'endommagement, la détérioration et l'altération de données 80
4. La suppression et l'effacement de données 81
5. Le mode de commission 82
C. Une entrave grave au fonctionnement du système informatique 83
D. L'illicéité 84
E. L'intention 85
IV. Comparaison avec le droit suisse 86
Bibliographie 87
Travaux législatifs 88

I. GÉNÉRALITÉS

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. 1

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. 2

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 2007[87]. 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. 3

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**. 4

87. Ottis, pp 163-168.

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**[88].

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.

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

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

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.

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. 10

2. La transmission de données

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. 11

Au fil du temps, les **performances** des systèmes informatiques, en particulier les serveurs, ont considérablement augmenté. Les techniques de répartition de charge[89] et de haute disponibilité[90] 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 12

89. 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.
90. 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.

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. 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 ISO[91].

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.

91. Norme ISO 27001.

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. 16

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. 17

4. La suppression et l'effacement de données

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 support[92]. 18

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. 19

92. 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*).

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 évidement être commis directement par une personne physique. Cela prendrait toutefois beaucoup de temps. En pratique, les cybercriminels utilisent donc plutôt des maliciels ou des bots[93] 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.

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

C. Une entrave grave au fonctionnement du système informatique

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. 25

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 fonctions[94]. 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. 26

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. 27

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 punissable[95]. L'entrave qui résulterait 28

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

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 librement[96]. 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) »[97].

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 **mises 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

95. Rapport explicatif de la Convention sur la cybercriminalité, n. 66.
96. Rapport explicatif de la Convention sur la cybercriminalité, n. 67.
97. Rapport explicatif sur la Convention sur la cybercriminalité, n. 67.

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 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.

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. 32

E. L'intention

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. 33

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. 144bis 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 144bis 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 correctement[98], alors que l'art. 144bis ch. 1 CP assure un droit de disposition sur des données[99]. 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. 144bis 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. 144bis ch. 1 CP), car elle 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. 144bis ch. 1 CP. C'est notamment le cas d'envois « 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 »[100]. Ces actes ne sont pas non plus

98. Rapport explicatif de la Convention sur la cybercriminalité, n. 65.
99. ATF 129 IV 230 consid. 2.1.1 ; Schmid, § 6 n. 14 ; Trechsel / Crameri, n. 2 ad art. 144bis CP ; Weissenberg, n. 6 ad art. 144bis CP.

correctement réprimés par l'art. 179septies CP (utilisation abusive d'une installation de télécommunication) pour trois raisons. Premièrement, parce que l'art. 179septies 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).

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. 39

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/Crameri 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

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

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)

COMMENTAIRE

Art. 6 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jérémie Müller

PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 6 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 6 CCC N. XXX.

Art. 6 Abus de dispositifs

[1] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux art. 2 à 5 ci-dessus,

ii. d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les art. 2 à 5; et

b. la possession d'un élément visé à la let. a. ch. i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les art. 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au par. 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux art. 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le par. 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au par. 1. let. a. ch. ii du présent article.

TABLE DES MATIÈRES

I. Généralités 92
II. Bien juridiquement protégé 92
III. Éléments constitutifs de base 93
A. Un objet illicite 93
1. Un dispositif permettant la commission d'une infraction mentionnée aux art. 2 à 5 CCC 93
2. Des données permettant d'accéder à un système informatique dans le but de commettre l'une des infractions mentionnées aux art. 2 à 5 CCC 94
B. Un comportement punissable 94
1. La production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition 94
2. La possession 96
C. L'illicéité 96
D. L'intention 97
E. Un dessein spécial 97
IV. Les reserves 98
A. Quant aux comportements punissables 98
B. Quant au matériel illicite 100
V. Comparaison avec le droit suisse 102
Bibliographie 103
Travaux législatifs 103

I. GÉNÉRALITÉS

1 La commission des infractions réprimées aux art. 2 à 5 CCC nécessite en principe l'utilisation d'**outils informatiques**. Tous les cybercriminels ne sont toutefois pas capables de créer ces outils eux-mêmes. Ils cherchent par conséquent à les acquérir auprès de tiers. Au fil du temps, cette demande a conduit à la création d'un véritable marché noir, notamment sur le *dark net*. De nos jours, presque n'importe qui peut acquérir des *malwares* en tout genre, louer des *bots-nets* ou même mandater des cybercriminels pour accomplir des tâches spécifiques. Compte tenu du risque que ce marché noir représente pour l'ensemble des systèmes informatiques et leurs utilisateurs légitimes, les Parties ont décidé de sanctionner pénalement certains actes, potentiellement dangereux, en amont, avant la commission des infractions visées aux art. 2 à 5 CCC[101]. L'art. 6 CCC s'appuie sur des instruments adoptés par le Conseil de l'Europe (Convention européenne sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel – STE nº 178) et l'Union européenne (Directive 98/84/EC du Parlement européen et du Conseil en date du 20 novembre 1998 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel), ainsi que sur les dispositions adoptées dans certains pays en la matière[102].

II. BIEN JURIDIQUEMENT PROTÉGÉ

2 En réprimant toutes les formes de commerce ou de possession de matériel destiné à commettre l'une des infractions réprimées par les art. 2 à 5 CCC, les Parties rendent punissables les **actes préparatoires** à la commission de ces infractions. Le but est donc de renforcer la protection des biens juridiques protégés par les art. 2 à 5 CCC, à savoir l'inviolabilité et le bon fonctionnement des systèmes informatiques, ainsi que l'intégrité, la disponibilité et la confidentialité des données.

101. Rapport explicatif de la Convention sur la cybercriminalité, n. 71.
102. Rapport explicatif de la Convention sur la cybercriminalité, n. 71.

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Un objet illicite

1. Un dispositif permettant la commission d'une infraction mentionnée aux art. 2 à 5 CCC

La notion de dispositif n'est définie ni dans le texte de la convention ni dans son rapport explicatif. A notre avis, un **dispositif** au sens de l'art. 6 CCC est un ensemble de pièces, d'éléments ou de données destiné à accomplir une ou plusieurs fonctions précises. On en veut pour preuve que les Parties citent expressément le programme informatique à titre d'exemple de dispositif. Comme il ressort clairement de l'adjonction des termes « y compris », la notion se veut bien plus large que les seuls programmes informatiques. En plus des virus, vers, chevaux de Troie, bombes logiques et autres maliciels qui font indiscutablement partie des programmes visés par cette disposition, on trouve donc aussi des dispositifs matériels tels que les micros, les caméras ou les robots. 3

Le **champ d'application** de la norme se limite toutefois aux dispositifs conçus ou adaptés pour commettre l'une des infractions réprimées par les art. 2 à 5 CCC. Il s'agit donc de dispositifs ou de programmes qui sont conçus, par exemple, pour altérer, voire détruire des données, ou pour s'ingérer dans le fonctionnement des systèmes, tels que les programmes-virus, ou bien des programmes conçus ou adaptés pour accéder à des systèmes informatiques[103]. Les dispositifs qui ne permettent pas d'accomplir de tels actes ne sont pas concernés par l'art. 6 § 1 let. a ch. 1 CCC. Il en va de même des dispositifs qui permettent de commettre une autre infraction, notamment l'une de celles réprimées par les art. 7 à 10 CCC. 4

Au moment de l'élaboration de la convention, une discussion approfondie a eu lieu pour déterminer si les dispositifs visés devaient être ceux qui étaient conçus exclusivement ou spécialement pour permettre la commission d'infractions, ce qui excluait les **dispositifs à double usage**, ou s'il fallait au contraire aussi inclure ces derniers. Les Parties ont finalement conclu qu'il ne fallait pas limiter la poursuite pénale aux seuls dispositifs conçus exclusivement pour commettre des infractions, car cela aurait 5

103. Rapport explicatif de la Convention sur la cybercriminalité, n. 72.

considérablement réduit le nombre de cas auxquels la norme pourrait s'appliquer. Les Parties ont cependant aussi écarté l'hypothèse consistant à étendre la norme à l'ensemble des dispositifs, y compris licites, qui pourraient permettre la commission des infractions d'une manière ou d'une autre, car la réalisation de l'infraction n'aurait alors reposé plus que sur l'intention de l'auteur. C'est donc une solution intermédiaire qui a été adoptée.

6 Sont ainsi visés par l'art. 6 § 1 let. a ch. 1 CCC les dispositifs **principalement** conçus ou adaptés pour permettre la commission de l'une des infractions réprimées par les art. 2 à 5 CCC. Cette formulation exclut les dispositifs à double usage[104], à moins que l'usage principal soit de commettre une infraction.

2. Des données permettant d'accéder à un système informatique dans le but de commettre l'une des infractions mentionnées aux art. 2 à 5 CCC

7 Afin de couvrir l'ensemble des moyens utilisés par les cybercriminels pour commettre l'une des infractions réprimées par les art. 2 à 5 CCC, les Parties ont également rendu punissables les actes visant à mettre à disposition des mots de passe, codes d'accès et données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique (art. 6 § 1 let. a ch. 2 CCC). Le but est d'éliminer toute **lacune**. Cette approche est parfaitement justifiée au regard du grand nombre de mots de passe et autres données d'accès qui ont été dérobés et qui sont proposés à la vente sur le *dark net*.

B. Un comportement punissable

8 Les Parties ont voulu réprimer toutes les formes de mise à disposition d'objets illicites, de même que leur possession. En revanche, on constate que la simple fourniture d'**instructions** – par exemple sous forme de textes ou de vidéos – sur la manière de fabriquer des objets illicites n'est pas punissable.

1. La production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition

9 L'art. 6 § 1 let. a CCC énumère plusieurs comportements punissables relatifs au commerce. Cette liste est **exhaustive**. Afin de n'oublier aucun

comportement, elle se termine néanmoins par une clause générale (« Auffangtatbestand »).

La « **production** » est la fabrication du matériel illicite en vue de son utilisation pour commettre l'une des infractions figurant aux art. 2 à 5 CCC. Le terme de « production » comprend l'ensemble des étapes nécessaires à la réalisation de l'objet. Cela comprend donc l'écriture du code du maliciel – en langage informatique – ou encore le décryptage d'un mot de passe. 10

L'art. 6 § 1 let. a CCC sanctionne ensuite la « **vente** ». Ce terme désigne la remise d'un objet illicite mentionné dans ce paragraphe en échange d'une somme d'argent. La devise dans laquelle la somme est payée n'a pas d'importance. Cette somme peut même être payée en cryptomonnaies. La remise doit toutefois être onéreuse. Il ne peut pas s'agir d'une donation. 11

L' « **obtention pour utilisation** » implique un comportement actif de la part de celui qui cherche à se procurer du matériel interdit. Il faut s'être mis en relation avec quelqu'un qui détient le matériel prohibé et l'avoir acquis à titre gratuit ou contre rémunération. La manière dont le matériel est remis est sans importance. Le transfert peut donc se faire par voie électronique, par envoi postal ou même par remise en main propre. Ce qui est déterminant, c'est que l'auteur obtienne le matériel illicite dans le but de l'utiliser pour commettre l'une des infractions réprimées par les art. 2 à 5 CCC. Si l'objectif est de commettre une autre infraction ou simplement de collectionner ce type de matériel, l'auteur n'est pas punissable. 12

Le quatrième comportement mentionné dans la liste est l'« **importation** ». Ce terme désigne le fait d'introduire un objet illicite dans le pays qui sanctionne cet acte. L'importation de matériel prohibé crée un risque important qu'il soit par la suite remis à des tiers. Pour réduire ce risque, la simple introduction dans le pays est interdite, même si l'importateur n'est qu'un maillon de la chaîne entre le producteur du matériel et l'utilisateur final. 13

L'art. 6 § 1 réprime encore la « **diffusion** ». Il s'agit de la transmission de matériel illicite à un nombre indéterminé de personnes qui n'en ont pas nécessairement fait la demande. L'envoi du matériel peut se faire par n'importe quel mode, que ce soit par voie informatique, par courrier postal ou par remise en main propre. 14

104. Rapport explicatif de la Convention sur la cybercriminalité, n. 73.

15 Pour éviter toute lacune, la liste se termine par « d'**autres formes** de mise à disposition ». Cette hypothèse permet d'englober tous les cas qui ne correspondent pas exactement aux notions examinées ci-dessus, mais qui permettent néanmoins à l'auteur de fournir des objets illicites à des tiers. Cette expression inclut, par exemple, la création ou la compilation de liens hypertextes qui visent à faciliter l'accès à du matériel illicite[105].

2. La possession

16 L'art. 6 § 1 let. b CCC réprime la **possession** de l'un des objets mentionnés ci-dessus[106]. Tout comme pour les comportements énumérés à l'art. 6 § 1 let. a CCC, l'auteur doit détenir le matériel prohibé dans l'intention de commettre l'une des infractions sanctionnées par les art. 2 à 5 CCC. Si l'auteur détient ce matériel dans le but de commettre une autre infraction ou simplement à des fins de collection, il n'est pas punissable.

17 Les Parties ont toutefois laissé une certaine marge de manœuvre à chaque Etat pour déterminer si la possession d'un seul élément suffisait à réaliser l'infraction, ou s'il fallait en posséder un certain **nombre**. Force est toutefois de constater que cette possibilité semble surtout avoir été introduite en faveur des Etats-Unis d'Amérique, lesquels ont été les seuls à en faire usage[107]. Ils n'ont toutefois pas précisé le nombre minimal d'éléments qu'il fallait posséder pour être punissable. Ils se sont simplement référés au nombre prévu dans la loi fédérale des Etats-Unis applicable.

C. L'illicéité

18 L'exigence selon laquelle l'auteur doit avoir agi **sans droit** permet aux Parties de créer des exceptions à la répression pénale. Cela leur permet notamment d'exclure du champ d'application de l'art. 6 CCC les autorités de poursuite pénale qui détiennent légalement du matériel illicite, sous forme de séquestres, dans le cadre de leurs enquêtes.

19 L'art. 6 § 2 réserve expressément l'hypothèse dans laquelle l'auteur n'agit pas sans droit, à savoir que les comportements énumérés à l'art. 6 § 1 let. a ch. 1

105. Rapport explicatif de la Convention sur la cybercriminalité, n. 72.
106. Voir chiffre III. A ci-dessus.

CCC ne sont pas punissables s'ils n'ont pas pour but de commettre une infraction réprimée par les art. 2 à 5 CCC. Ainsi, par exemple, les dispositifs d'essai (également appelés « dispositifs de craquage ») et les dispositifs d'analyse de réseaux conçus par les professionnels pour évaluer la fiabilité de leurs produits informatiques ou contrôler la sécurité des systèmes sont fabriqués à des **fins légitimes** et leurs utilisateurs sont donc considérés comme agissant « avec droit »[108].

D. L'intention

L'abus de dispositifs est **intentionnel**. L'intention doit porter sur tous les éléments objectifs de l'infraction. Si l'auteur possède ou fournit un programme informatique ordinaire à un tiers sans se douter qu'il pourrait aussi être utilisé pour commettre l'une des infractions réprimées par les articles 2 à 5 CCC, il n'est pas punissable. 20

E. Un dessein spécial

En plus de l'intention, l'auteur doit avoir agi dans le **dessein** de commettre l'une des infractions visées aux articles 2 à 5 CCC[109]. Il ne suffit par conséquent pas que l'auteur veuille fabriquer un programme malveillant uniquement pour le défi technique que cela représente ou pour en faire la collection. De même, il ne suffit pas que l'auteur veuille utiliser le programme malveillant ou le mot de passe dans le but de commettre une infraction autre que celles réprimées par les art. 2 à 5 CCC. 21

Le but poursuivi par l'auteur doit être la commission, par lui-même ou par un tiers auquel il fournit le matériel prohibé, de l'une des infractions sanctionnées par les art. 2 à 5 CCC. L'art. 6 CCC consacre une infraction de **mise en danger abstraite**. Il n'est donc pas nécessaire que le matériel illicite soit effectivement utilisé ultérieurement pour commettre l'une de ces infractions. Il suffit que l'acte punissable soit commis dans le but d'accomplir l'une des infractions réprimées par les art. 2 à 5 CCC. 22

107. Déclaration 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&code_Pays=USA, visité le 21.1.2024), en lien avec le titre 18 § 1030 du Code des Etats-Unis (Computer Fraud and Abuse Act).
108. Rapport explicatif de la Convention sur la cybercriminalité, n. 77.
109. Rapport explicatif de la Convention sur la cybercriminalité, n. 76.

IV. LES RESERVES

23 Les seuls comportements que les Parties doivent impérativement sanctionner est la vente, la distribution ou toute autre mise à disposition d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique. Elles ont en revanche la possibilité de **limiter** le champ d'application de cette norme en ce qui concerne les autres comportements punissables et/ou les objets illicites.

A. Quant aux comportements punissables

24 La convention permet aux Parties de **limiter** la poursuite pénale en refusant de poursuivre la production, l'obtention pour utilisation, l'importation et la possession de matériel illicite.

25 La **Géorgie**, la **Suisse**, le **Chili**, le **Japon** et le **Sri-Lanka** ont fait usage de cette possibilité pour limiter au maximum les comportements punissables[110].

110. Déclaration consignée dans une Déclaration du Ministre des Affaires Etrangères de la Géorgie, datée du 1er juin 2012, déposée avec l'instrument d'approbation le 6 juin 2012 (disponible sous https://www.coe.int/fr/web/ conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=GEO, visité le 21.1.2024), en lien avec l'art. 285 du Code pénal géorgien ; Réserve 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=2&codePays=SWI, en lien avec les art. 143bis al. 2 et 144bis ch. 2 du Code pénal suisse ; 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 la Loi chilienne N° 19.223 sur les délits informatiques ; Réserve 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=2&codePays=JAP, visité le 21.1.2024), en lien avec les art. 168-2 et 168-3 du Code pénal japonais et les art. 4, 5 et 6 de la Loi japonaise sur l'interdiction de l'accès à un système informatique non autorisé ; Réserve consignée dans une Note Verbale de l'Ambassade du Sri Lanka auprès de la Belgique, datée du 26 mai 2015, et dans l'instrument d'adhésion, déposés simultanément le 29 mai 2015 (disponible sous https://www.coe.int/fr/web/conventions/full-list? module=declarations-by-treaty&numSte=185&codeNature=2&codePays=LKA, visité le 21.1.2024), en lien avec l'art. 9 de la Loi sri-lankaise sur les crimes informatiques.

La **Principauté d'Andorre** a indiqué que l'obtention de dispositifs mentionnés à l'art. 6 § 1 let. a CCC destinés à l'utilisation n'était pas punissable dans son droit interne[111]. 26

L'**Azerbaïdjan** a déclaré qu'elle ne poursuivrait les comportements énumérés à l'art. 6 § 1 CCC que si un dommage sérieux survenait[112]. 27

L'**Ukraine** a expliqué qu'elle ne réprimerait pas l'obtention pour utilisation et d'autres formes de mise à disposition des éléments visés à l'art. 6 § 1 let. a ch. 1 CCC, ainsi que la production et l'obtention pour utilisation des éléments visés à l'art. 6 § 1 let. a ch. 2 CCC[113]. 28

Les **Etats-Unis d'Amérique** se sont réservés le droit de ne pas poursuivre la production, l'obtention pour utilisation, l'importation et la possession de matériel illicite conçu ou adapté pour permettre la commission des infractions réprimées par les art. 4 et 5 CCC[114]. 29

Israël a déclaré qu'il ne poursuivrait pas l'obtention pour utilisation ou l'importation de matériel illicite, ni la possession d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique[115]. 30

---

111. Réserve consignée dans une Note Verbale du Ministère des Affaires étrangères d'Andorre, datée du 14 octobre 2016, déposée avec l'instrument de ratification le 16 novembre 2016 (disponible sous https://www.coe.int/fr/ web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=AND, visité le 21.1.2024), en lien avec l'art. 182 du Code pénal andorran.
112. 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. 272.1 du Code pénal azerbaïdjanais.
113. Réserve de l'Ukraine consignée dans l'instrument de ratification déposé le 10 mars 2006 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2& codePays=U, visité le 21.1.2024), en lien avec l'art. 361 du Code pénal ukrainien.
114. Réserve 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=2&codePays=USA, visité le 21.1.2024), en lien avec la section a chiffre 6 du Computer Fraud and Abuse Act.
115. Réserve d'Israël consignée dans l'instrument d'adhésion déposé le 9 mai 2016 (disponible https://www.coe.int/ fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=ISR, visité le 21.1.2024), en lien avec la section 6 de la Loi informatique israélienne.

31 L'**Allemagne**, la **Principauté d'Andorre**, l'**Argentine** et le **Pérou** se sont limités à refuser de poursuivre la possession de matériel illicite (art. 6 § 1 let. b CCC)[116].

B. Quant au matériel illicite

32 La convention permet aussi aux Parties de limiter la poursuite en refusant de considérer comme illicite les **dispositifs**, y compris les programmes informatiques, principalement conçus ou adaptés pour permettre la commission de l'une des infractions réprimées par les art. 2 à 5 CCC.

33 La **Géorgie**, la **Norvège**, la **Suisse**, le **Japon** et le **Sri-Lanka** ont également fait usage de cette possibilité pour limiter au maximum le matériel punissable[117].

34 Le **Chili** avait initialement émis une réserve identique à celle de la Géorgie, de la Norvège, de la Suisse et du Japon[118]. Il a toutefois modifié sa législation en 2022. Dans sa nouvelle version, l'*abuso de los dispositivos* correspond à l'art. 6 CCC[119]. La réserve n'est donc plus nécessaire.

35 Les **Etats-Unis d'Amérique** se sont réservés le droit de ne pas poursuivre les dispositifs, y compris les programmes informatiques, conçus ou adaptés pour permettre la commission des infractions réprimées par les art. 4 et 5 CCC[120].

36 L'**Allemagne** a déclaré qu'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission

d'une infraction réprimée par les art. 2 à 5 CCC n'était pas du matériel

117. Déclaration consignée dans une Déclaration du Ministre des Affaires Etrangères de la Géorgie, datée du 1er juin 2012, déposée avec l'instrument d'approbation le 6 juin 2012 (disponible sous https://www.coe.int/fr/web/ conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=10&codePays=GEO, visité le 21.1.2024), en lien avec l'art. 285 du Code pénal géorgien ; Réserve de la Norvège consignée dans l'instrument de ratification déposé le 30 juin 2006 (disponible sous https://www.coe.int/fr/web/conventions/full-list? module=declarations-by-treaty&numSte=185&codeNature=2&codePays=NOR, visité le 21.1.2024), en lien avec la section 201 du Code pénal norvégien ; Réserve 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=2&codePays=SWI, en lien avec les art. 143bis al. 2 et 144bis ch. 2 du Code pénal suisse ; Réserve 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=2&codePays=JAP, visité le 21.1.2024), en lien avec les art. 168-2 et 168-3 du Code pénal japonais et art. 4, 5 et 6 de la Loi japonaise sur l'interdiction de l'accès à un système informatique non autorisé ; Réserve consignée dans une Note Verbale de l'Ambassade du Sri Lanka auprès de la Belgique, datée du 26 mai 2015, et dans l'instrument d'adhésion, déposés simultanément le 29 mai 2015 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty &numSte=185&codeNature=2&codePays=LKA, visité le 21.1.2024), en lien avec l'art. 9 de la Loi sri-lankaise sur les crimes informatiques.
118. 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).
119. art. 8 de la Loi chilienne N° 21.459 sur les délits informatiques.
120. Réserve 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=2&codePays=USA, visité le 21.1.2024), en lien avec la section a chiffre 6 du Computer Fraud and Abuse Act.
116. Réserve 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=2&codePays=GER, visité le 21.1.2024), en lien avec le §202c du Code pénal allemand ; Réserve consignée dans une Note Verbale du Ministère des Affaires étrangères d'Andorre, datée du 14 octobre 2016, déposée avec l'instrument de ratification le 16 novembre 2016 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185& codeNature=2&codePays=AND, visité le 21.1.2024), en lien avec l'art. 182 du Code pénal andorran ; Réserve de l'Argentine consignée dans l'instrument d'adhésion reçu et enregistré au Secrétariat Général le 5 juin 2018 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185& codeNature=2&codePays=ARG, visité le 21.1.2024), en lien avec l'art. 183 du Code pénal argentin ; Réserves 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=2&codePays=PER, visité le 21.1.2024), en lien avec l'art. 10 de la Loi péruvienne sur les délits informatiques.

punissable en droit allemand[121].

V. COMPARAISON AVEC LE DROIT SUISSE

37 Dans son Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, le Conseil fédéral indiquait que l'art. 6 CCC était couvert pour l'essentiel par l'**art. 144bis ch. 2 CP**, ainsi que par l'ajout d'un second alinéa à l'**art. 143bis CP**[122].

38 Or, même si la Suisse a fait usage de toutes les possibilités données par l'art. 6 § 3 CCC pour **limiter** au maximum les comportements punissable et le matériel illicite, il n'en demeure pas moins que le droit suisse est loin de satisfaire aux exigences minimales posées par l'art. 6 CCC, pour plusieurs raisons.

39 Premièrement, l'art. 144bis ch. 2 al. 1 CP ne s'applique qu'aux **logiciels**[123]. Il n'est donc pas applicable à d'autres dispositifs, ni aux mots de passe, ni aux code d'accès ou données informatiques similaires. A cela s'ajoute que les logiciels visés par l'art. 144bis ch. 2 al. 1 CP doivent être propres ou destinés à commettre une infraction réprimée par l'art. 144bis ch. 1 al. 1 CP[124]. Cela pose deux problèmes. D'une part, 144bis ch. 1 al. 1 CP ne satisfait pas entièrement aux conditions minimales de l'art. 4 CCC[125]. D'autre part, l'art. 144bis ch. 2 al. 1 CP fait complètement abstraction des logiciels propres ou destinés à commettre une infraction correspondant à celles réprimées par les art. 2, 3 ou 5 CCC. Ces logiciels ne sont donc pas punissables en droit suisse.

40 L'ajout de l'art. 143bis al. 2 CP ne permet de combler qu'une faible partie de ces **lacunes** très importantes. En effet, cette disposition ne réprime que le fait de mettre en circulation ou de rendre accessible un mot de passe, un programme ou toute autre donnée propres ou destinés à commettre l'infraction réprimée par l'art. 143bis al. 1 CP. Or, d'une part, cette norme ne correspond pas aux exigences minimales de l'art. 2 CCC[126]. D'autre part, elle

121. Réserve 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=2&codePays=GER, visité le 21.1.2024)
122. FF 2010 4285
123. Trechsel / Crameri, n. 13 ad art. 144bis CP ; Weissenberg, n. 48 ad art. 144bis CP.
124. Weissenberger, n. 50 ad art. 144bis CP.
125. Voir Art. 4 CCC n. 30ss.

ne réprime pas la mise en circulation ou le fait de rendre accessible un mot de passe, un programme ou toute autre donnée propres ou destinés à commettre une autre infraction que celle réprimée par 143bis al. 1 CP.

En définitive, même à supposer que l'art. 143bis al. 1 CP réponde aux exigences de l'art. 2 CCC et que l'art. 144bis ch. 1 al. 1 CP corresponde aux conditions minimales de l'art. 4 CCC, la **punissabilité** en droit suisse se limiterait à la mise en circulation ou au fait de rendre accessible un mot de passe, un programme ou toute autre donnée propres ou destinés à commettre l'infraction réprimée par l'art. 2 CCC, ainsi qu'à la fabrication, l'importation, la mise en circulation, la promotion, l'offre ou le fait de rendre accessibles d'une quelconque manière des logiciels propres ou destinés à commettre l'infraction réprimée par l'art. 4 CCC. 41

Pour correspondre aux exigences minimales de l'art. 6 CCC, il faudrait donc **adapter** les art. 143 al. 1, 143bis al. 1 et 144bis ch. 1 al. 1 CP dans le sens indiqué ci-dessus[127] ; créer l'équivalent de l'art. 5 CCC[128] et compléter chacune de ces dispositions en y ajoutant un alinéa qui réprimerait la vente, la distribution ou toute autre mise à disposition de mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans le but de commettre l'une de ces quatre infractions. 42

BIBLIOGRAPHIE

Trechsel Stefan/Crameri Dean, in : Trechsel Stefan/Pieth Mark (Hrsg.), 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 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

126. Voir Art. 2 CCC n. 39ss.
127. Voir Art. 2 CCC n. 39ss, Art. 3 CCC n. 40ss, Art. 4 CCC n. 30ss.
128. Voir Art. 5 CCC n. 33ss.

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

COMMENTAIRE

Art. 7 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jérémie Müller

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 107
II. Bien juridiquement protégé 107
III. Éléments constitutifs de base 107
A. Des données informatiques 107
B. Des données pertinentes dans les relations juridiques 108
C. Un comportement punissable 109
1. L'introduction de données 110
2. L'altération, la suppression et l'effacement de données 110
D. L'illicéité 112
E. L'intention 112
IV. Éléments constitutif supplémentaire facultatif 112
V. Comparaison avec le droit suisse 114
Travaux législatifs 114

I. GÉNÉRALITÉS

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 tromperie[129]. 1

II. BIEN JURIDIQUEMENT PROTÉGÉ

Le bien juridiquement protégé par cette norme est la **sécurité** et la **fiabilité** des données électroniques, susceptibles d'avoir des conséquences sur les relations juridiques[130]. 2

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Des données informatiques

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. 3

129. Rapport explicatif de la Convention sur la cybercriminalité, n. 81.
130. Rapport explicatif de la Convention sur la cybercriminalité, n. 81.

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 rédigé par un humain dans lequel la signature manuscrite est remplacée par l'apposition d'une signature électronique qualifiée[131]. 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.

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

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. 8

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. 9

C. Un comportement punissable

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 convaincre[132]. 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 déterminante[133]. 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 document[134]. 10

L'authenticité des données quant à leur **auteur** implique qu'elles proviennent effectivement de la personne dont elles semblent émaner. Dans cette 11

132. § 267 du Code pénal allemand ; § 223 du Code pénal autrichien ; art. 485 du Code pénal italien ; art. 441-1 du Code pénal français.
133. Rapport explicatif de la Convention sur la cybercriminalité, n. 82.
134. Rapport explicatif de la Convention sur la cybercriminalité, n. 82.

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 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 inexactes[135].

15 L'art. 7 CCC ne sanctionne que l'introduction de données qui entraine 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.

La **suppression** de données consiste à retenir et à cacher des données[136]. 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. 18

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 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. 19

135. Rapport explicatif de la Convention sur la cybercriminalité, n. 83
136. Rapport explicatif de la Convention sur la cybercriminalité, n. 83.

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 similaire[137]. Le rapport explicatif ne contient pas d'indication sur la manière dont la notion d'intention fraudeuse 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

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

ou celle d'autrui. L'avantage recherché doit toutefois être indu, c'est-à-dire contraire au droit.

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 frauduleuse[138]. 24

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 similaire[139]. 25

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 nuire[140]. 26

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 dommage[141]. 27

Enfin, le **Chili** avait dans un premier temps expliqué qu'il ne poursuivrait la falsification informatique que si elle était commise avec une intention 28

138. 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.
139. 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.
140. 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.

frauduleuse et qu'elle causait un préjudice à des tiers[142]. 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 CCC[143]. 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 1er janvier 1995[144].

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

141. 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.
142. 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.
143. Art. 5 de la Loi chilienne N° 21.459 sur les délits informatiques.

modification de la loi fédérale sur 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

144. FF 1991 II 956ss.

COMMENTAIRE

Art. 8 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jérémie Müller

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 119
II. Bien juridiquement protégé 119
III. Éléments constitutifs de base 119
A. Un système informatique 119
B. Des données informatiques 120
C. Un comportement punissable 120
1. Une manipulation de données 120
a. L'introduction de données 120
b. L'altération, la suppression et l'effacement de données 121
2. Une atteinte au fonctionnement du système informatique 121
D. Un préjudice patrimonial 122
E. L'illicéité 122
F. L'intention 123
G. Un dessin spécial 123
IV. Comparaison avec le droit suisse 124
Bibliographie 125
Travaux législatifs 125

I. GÉNÉRALITÉS

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 »[145]. 1

II. BIEN JURIDIQUEMENT PROTÉGÉ

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. 2

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Un système informatique

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, ...). 3

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. 4

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

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. 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 CCC[146]. 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.

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

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

Les notions d'altération, de suppression et d'effacement de données sont **identiques** à celles des art. 4, 5 et 7 CCC[147]. 10

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. 11

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. 12

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. 13

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. 14

2. Une atteinte au fonctionnement du système informatique

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 15

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

sorties sur imprimante et les actes affectant les enregistrements ou les flux de données, ainsi que l'ordre dans lequel les programmes sont exécutés[148].

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 économique[149]. 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

148. Rapport explicatif de la Convention sur la cybercriminalité, n. 87.
149. Rapport explicatif de la Convention sur la cybercriminalité, n. 88.

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.

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. 23

F. L'intention

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. 24

G. Un dessin spécial

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 l'ensemble des avantages économiques qui permettent un enrichissement. En d'autres termes, il s'agit de toute amélioration de la situation patrimoniale. 25

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. 26

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. 27

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 informatique[150].

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 correctement[151].

31 En ce qui concerne les **comportements** punissables, l'art. 147 CP réprime l'utilisation de données incorrecte[152], incomplète[153] ou indue[154]. 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

150. Rapport explicatif de la Convention sur la cybercriminalité, n. 90.
151. ATF 129 IV 22 consid. 4.2.
152. 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 / Crameri, 2008, n. 4 ad art. 147 CP.
153. 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 / Crameri, 2008, n. 5 ad art. 147 CP
154. 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 / Crameri, 2008, n. 6 ad art. 147 CP

puisqu'elle ne sanctionne pas la suppression de données qui auraient dû se trouver dans le système informatique[155].

Enfin, l'art. 147 CP ne sanctionne que la fraude informatique causée par une **manipulation de données**[156]. Le comportement mentionné à l'art. 8 let. b CCC ne tombe donc pas sous le coup de l'art. 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. 32

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

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/Crameri 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)

155. Fiolka, n. 10 ad art. 147 CP.
156. Schmid, § 7, n. 24

COMMENTAIRE

Art. 9 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jérémie Müller

PROPOSITION DE CITATION

Jérémie Müller, Commentaire de l'art. 9 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Müller, art. 9 CCC N. XXX.

Titre 3: Infractions se rapportant au contenu

Art. 9 Infractions se rapportant à la pornographie enfantine

[1] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a. la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;

b. l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;

c. la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;

d. le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;

e. la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du par. 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle:

a. un mineur se livrant à un comportement sexuellement explicite;

b. une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

c. des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du par. 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d ′âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les par. 1, al. d et e, et 2, al. b. et c.

TABLE DES MATIÈRES

I. Généralités 130
II. Bien juridiquement protégé 131
III. Éléments constitutifs de base 131
A. Une représentation pédopornographique 131
1. Les supports de la représentation 131
2. Le caractère pornographie 132
3. La notion de mineur 133
4. La notion de pornographie enfantine 133
B. Un comportement punissable 134
C. L'illicéité 136
D. L'intention 137
IV. Les réserves 138
A. Quant à l'âge des mineurs faisant l'objet de la représentation 138
B. Quant aux comportements punissables 139
C. Quant aux objets de la représentation 140
V. Comparaison avec le droit suisse 143
Bibliographie 143
Travaux législatifs 144

I. GÉNÉRALITÉS

1 L'avènement d'**Internet** a permis les échanges les plus lointains, les plus rapides et les plus efficaces que l'humanité n'ait connus. Elle a néanmoins aussi fourni des outils de communication très performants à des criminels qui, auparavant, étaient souvent isolés. C'est ainsi que des personnes produisant de la pédopornographie ont pu entrer en contact avec des personnes consommant ce type de supports dans le monde entier. L'échange d'idées, de fantasmes et de conseils entre pédophiles a contribué à appuyer, encourager ou faciliter les infractions sexuelles commises à l'encontre d'enfants[157].

2 Or, en plus de faciliter l'échange de matériel pédopornographique, le monde virtuel a également permis de garantir un certain **anonymat** aux auteurs et par voie de conséquence une forme d'impunité. Il n'est dès lors pas surprenant que ce type de délinquance se soit rapidement développé avec la généralisation d'Internet.

3 L'art. 9 CCC répond donc à la préoccupation exprimée par les membres du Conseil de l'Europe lors de leur 2e sommet en 1997, et reflète une **évolution internationale** en faveur de l'interdiction de la pornographie enfantine, comme le confirment l'adoption récente du Protocole facultatif à la Convention des Nations Unies relative aux droits de l'enfant se rapportant à la vente d'enfants, à la prostitution des enfants et à la pornographie impliquant des enfants, ainsi que la récente initiative de la Commission européenne sur la lutte contre l'exploitation sexuelle des enfants et la pornographie enfantine (COM2000/854)[158].

4 Cette disposition vise à renforcer les mesures de **protection** en faveur des enfants, notamment contre l'exploitation sexuelle, en modernisant le droit pénal de façon à restreindre plus efficacement l'utilisation des systèmes informatiques dans le cadre de la commission d'infractions sexuelles à l'encontre des enfants[159].

5 Dans les années suivant l'adoption de la Convention sur la cybercriminalité, la pornographie enfantine et plus largement l'exploitation sexuelle des enfants

157. Rapport explicatif de la Convention sur la cybercriminalité, n. 93.
158. Rapport explicatif de la Convention sur la cybercriminalité, n. 92.
159. Rapport explicatif de la Convention sur la cybercriminalité, n. 91.

sont demeurées des problématiques très importantes. Cela a conduit à l'élaboration de la **Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels**, adoptée à Lanzarote le 25 octobre 2007. L'art. 20 de ce traité s'inspire très largement de l'art. 9 CCC[160].

II. BIEN JURIDIQUEMENT PROTÉGÉ

6 L'art. 9 CCC protège deux biens juridiques différents. L'art. 9 § 2 let. a CCC protège directement l'**intégrité sexuelle des enfants**. Quant à l'art. 9 § 2 let. b et c CCC, ils protègent leur intégrité sexuelle de manière indirecte en interdisant tout comportement qui, sans nécessairement causer un préjudice à l' « enfant » représenté dans le matériel en question, pourrait néanmoins encourager ou inciter des enfants à participer à de tels actes. Ces dispositions s'inscrivent ainsi dans le contexte d'une sous-culture préconisant la maltraitance des enfants[161].

III. ÉLÉMENTS CONSTITUTIFS DE BASE

A. Une représentation pédopornographique

1. Les supports de la représentation

7 L'art. 9 CCC – tout comme l'art. 20 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels – vise exclusivement les **représentations visuelles** de pornographie enfantine. Cela englobe toutes les représentations qui peuvent être perçues par la vue, en particulier les photos, les dessins, les croquis, les peintures, les gravures, les sculptures, les vidéos et les films. Les enregistrements audio, ainsi que les textes ne sont pas concernés.

8 Dans le cadre de la Convention sur la cybercriminalité, la répression se limite aux représentations visuelles sous forme **numérique**. Le support sur lequel elles sont enregistrées importe peu. Il est ainsi sans importance qu'elles soient enregistrées sur un disque dur, une clé USB, un DVD ou même dans le *cloud*.

160. Rapport explicatif de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, n. 133.
161. Rapport explicatif de la Convention sur la cybercriminalité, n. 102.

2. Le caractère pornographie

9 La **notion** de pornographie n'est définie ni dans la Convention sur la cybercriminalité, ni dans le rapport explicatif. Ce dernier indique simplement que cette notion doit être interprétée conformément aux normes de droit interne qui traitent de la classification de la représentation comme obscène, incompatible avec les mœurs publiques ou ayant à un autre titre un effet pervers[162].

10 **En Suisse**, est considéré comme pornographique ce qui vise à provoquer une excitation sexuelle du consommateur alors que la sexualité est à tel point détachée de ses composantes humaines et émotionnelles que la personne en est réduite à un pur objet sexuel dont on peut disposer à volonté. Le comportement sexuel est grossier et mis exagérément au premier plan[163]. Entre dans la pornographie, la représentation insistante et répétitive d'actes tels que des fellations, cunnilingus et masturbations[164]. Cette définition ne semble ni licencieuse, ni particulièrement chaste. Elle paraît au contraire équilibrée et peut donc aisément être reprise au niveau international. Les éléments cardinaux de cette définition se retrouvent d'ailleurs aussi dans l'art. 20 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels – largement inspiré de l'art. 9 CCC – qui définit à son paragraphe 2 la pornographie enfantine comme tout matériel représentant de manière visuelle un enfant se livrant à un comportement sexuellement explicite, réel ou simulé, ou toute représentation des organes sexuels d'un enfant à des fins principalement sexuelles. On peut donc s'en tenir à cette définition.

11 Bien que le texte de l'art. 9 CCC ne le mentionne **pas expressément**, le matériel présentant un intérêt artistique, médical ou scientifique, n'est pas considéré comme pornographique[165].

12 Déterminer ce qui est **artistique** ou ce qui ne l'est pas est compliqué, surtout dans le contexte d'une convention internationale conclue entre des Etats aux cultures très diverses. A notre avis, le caractère artistique doit être évalué de cas en cas. De manière générale, on peut toutefois dire que du matériel doit

162. Rapport explicatif de la Convention sur la cybercriminalité, n. 99.
163. ATF 133 IV 31 consid. 6.1.1.
164. ATF 117 IV 276 consid. 4.
165. Rapport explicatif de la Convention sur la cybercriminalité, n. 99.

être qualifié d'artistique lorsque l'artiste présente une chose de manière originale, a vocation à transmette un message et est le fruit d'une véritable recherche. Cela s'oppose à une représentation crue, triviale ou vulgaire de la réalité.

Quant au matériel **médical** ou **scientifique**, il s'agit de supports nécessaires à la formation ou à la recherche. 13

3. La notion de mineur

Bien que les droits nationaux de certaines Parties à la convention connaissaient un âge de la majorité plus élevé (p. ex. Canada, Etats-Unis d'Amérique, Japon[166]), les Parties se sont accordées pour retenir que la notion de mineur s'entend en principe de toute personne âgée de **moins de 18 ans** (art. 9 § 3 CCC). Comme on le verra au chiffre IV ci-dessous, les Parties peuvent toutefois émettre des réserves pour exiger une limite d'âge inférieure. Dans tous les cas, cette limite doit cependant être de 16 ans au moins. 14

4. La notion de pornographie enfantine

L'art. 9 § 2 CCC définit la notion de pornographie enfantine en fournissant une liste de trois types de représentations punissables. Cette liste est **exhaustive**. 15

En premier lieu, il est question des représentations mettant en scène un mineur se livrant à un comportement sexuellement explicite. L'expression « comportement sexuellement explicite » désigne avant tout les **relations sexuelles**, y compris génito-génitales, oro-génitales, ano-génitales ou oro-anales[167]. Pour être punissable au sens de l'art. 9 § 2 let. a CCC, elles doivent impliquer au moins un mineur. Il importe en revanche peu qu'elles n'aient lieu qu'entre mineurs ou avec un ou plusieurs majeurs. Le genre ou l'orientation sexuelle de chacun des participants est également sans importance. 16

L'expression « comportement sexuellement explicite » est cependant **plus large** que les seules relations sexuelles. Elle comprend aussi la zoophilie commise avec un mineur, la masturbation d'un mineur, les violences sado- 17

166. https://www.oecd.org/els/family/PF_1_8_Age_threshold_Childhood_to_Adulthood.pdf, visité le 21.1.2024.
167. Rapport explicatif de la Convention sur la cybercriminalité, n. 100.

masochistes dans un contexte sexuel commises sur un mineur ou l'exhibition lascive des parties génitales ou de la région pubienne d'un mineur[168].

18 Dans l'ensemble des hypothèses qui précèdent, il est sans importance que le comportement représenté soit **réel** ou **simulé**[169]. L'auteur ne peut donc pas échapper à la condamnation simplement parce que le comportement sexuellement explicite n'a pas véritablement eu lieu.

19 Le deuxième type de représentations visé par l'art. 9 § 2 CCC concerne les images pornographiques qui montrent une personne qui **apparaît comme un mineur** se livrant à un comportement sexuellement explicite (art. 9 § 2 let. b CCC). Il s'agit d'images mettant en scène des personnes qui sont soit tout juste majeures, mais qu'on essaie de faire passer pour des personnes encore mineures, soit clairement majeures, mais qui, par leur habillement, leur maquillage ou les accessoires qu'elles portent, donnent l'apparence de personnes mineures.

20 L'art. 9 § 2 let. c CCC mentionne enfin les **images réalistes** représentant un mineur se livrant à un comportement sexuellement explicite. Cette dernière hypothèse concerne notamment les bandes-dessinées ou mangas, les photomontages, voire les images créées de toute pièce par des ordinateurs, comme peut le faire l'intelligence artificielle.

B. Un comportement punissable

21 L'art. 9 § 1 CCC énumère cinq comportements punissables. Cette liste est **exhaustive**.

22 Le premier comportement visé est la « **production** », c'est-à-dire la fabrication, d'une représentation pédopornographique en vue de sa diffusion par voie informatique. Le terme de « production » comprend l'ensemble des actes nécessaires à la réalisation de représentations de pornographie enfantine. On pense évidement avant tout à la fixation d'images sur un porteur d'images. Il s'agit toutefois aussi de la préparation du lieu et du matériel nécessaire à la réalisation des images, de la retouche des images une fois fixée sur un porteur d'image, du montage de photographies ou de films ou même la création d'images de synthèse par ordinateur. En d'autres termes, ce

168. Rapport explicatif de la Convention sur la cybercriminalité, n. 100.
169. Rapport explicatif de la Convention sur la cybercriminalité, n. 100.

comportement vise toutes les formes de création ou d'édition de supports visuels. Dans tous les cas, ce matériel doit cependant être destiné à la diffusion par voie informatique. La réalisation d'images numériques destinées à sa propre consommation n'est pas punissable au titre de production, mais uniquement en raison de sa possession (art. 9 § 1 let. e CCC).

L'art. 9 § 1 let. b CCC réprime ensuite l'**offre** ou la **mise à disposition** de pornographie enfantine par le biais d'un système informatique. Le terme « offrir » désigne un comportement commercial par lequel l'auteur informe sa clientèle qu'il dispose d'un ou plusieurs produits et leur propose de les acquérir. Le type de contrat (vente, échange, donation, ...) importe peu. La « mise à disposition » est une notion plus large que l' « offre », car elle ne signifie pas nécessairement que l'auteur fait une quelconque démarche active pour proposer un produit à sa clientèle. Il s'agit en fait de tout acte qui permet ou facilite l'accès à une représentation pédopornographique par voie informatique. Cela inclut notamment la mise en ligne de pornographie enfantine, par exemple en créant des sites web, ainsi que la création ou à la compilation d'hyperliens vers des sites contenant de la pornographie enfantine[170]. 23

Un autre comportement punissable consiste à **diffuser** ou à **transmettre** de la pornographie enfantine par le biais d'un système informatique. Ces deux notions font référence à des envois de données. La « diffusion » est une distribution de matériel pédopornographique à un nombre indéterminé de personnes qui n'en ont pas nécessairement fait la demande. La « transmission » en revanche est un envoi à une ou plusieurs personnes déterminées qui en ont fait la demande. L'envoi de la représentation pédopornographique peut être effectué par n'importe quelle voie informatique, soit notamment par courriel, par messagerie instantanée ou par transfert « peer-to-peer ». 24

L'art. 9 let. d CCC évoque encore « le fait de se **procurer** ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique ». Ce comportement consiste à obtenir activement de la pornographie enfantine, par exemple par téléchargement[171]. Les données doivent donc avoir été transférées vers le système informatique de l'auteur ou par l'auteur vers le système informatique d'un tiers. Il doit y avoir transfert de possession. 25

170. Rapport explicatif de la Convention sur la cybercriminalité, n. 95.
171. Rapport explicatif de la Convention sur la cybercriminalité, n. 97.

L'obtention doit se faire par la voie informatique. Une remise en main propre ou un envoi par la poste ne sont donc pas visés par la convention.

26 Enfin, le dernier comportement punissable est la « **possession** de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques » (art. 9 § 1 let. e CCC). La notion classique de possession suppose à la fois une maîtrise physique sur l'objet et une volonté d'exercer cette maîtrise. Dans le monde virtuel, l'exigence objective de la maîtrise physique sur l'objet doit, à notre avis, être assouplie en ce sens qu'il suffit que le possesseur soit en tout temps et librement capable d'accéder à ses données. C'est bien évidemment le cas si les données se trouvent dans un système informatique qui lui appartient, sur un support d'enregistrement de données tel qu'un disque dur externe, une clé USB ou dans la carte mémoire d'un appareil photographique. L'auteur est toutefois aussi en possession des données s'il les enregistre sur un serveur distant auquel il a accès ou s'il les sauvegarde dans le « cloud ».

27 Sans que l'on en comprenne la raison, le fait de **consulter** de la pédopornographie directement en ligne, sans se l'approprier, n'a pas été mentionné et n'est donc pas punissable. L'absence de mention de ce comportement dans la liste de l'art. 9 § 1 CCC semble particulièrement surprenante. Au regard de la volonté affichée de lutter contre la pornographie enfantine, la répression de la consommation paraît en effet tout aussi importante que la criminalisation de la production de représentations pédopornographiques. Cet oubli a heureusement été corrigé dans la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels. Son rapport explicatif mentionne d'ailleurs que le comportement mentionné à l'art. 20 al. 1 let. f vise à permettre les poursuites à l'encontre de ceux qui regardent des images d'enfants sur des sites de pornographie enfantine mais qui, en ne les téléchargeant pas, échappent à la répression pénale[172].

C. L'illicéité

28 L'auteur doit agir **sans droit**. Cet élément constitutif permet aux Parties de créer des exceptions à la répression pénale pour les auteurs agissant dans un

172. Rapport explicatif de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, n. 140.

intérêt digne de protection, similaire aux intérêts artistique, médical ou scientifique.

Cette expression permet aussi d'exclure du champ d'application de l'art. 9 CCC les **autorités de poursuite pénale** qui détiennent, de manière légale, des images de pédopornographie sous forme de séquestres dans les enquêtes qu'elles instruisent et jugent. 29

L'omniprésence des « **smartphones** », y compris entre les mains de mineurs, a entraîné diverses dérives. Il n'est ainsi pas rare de nos jours que des personnes – en particulier parmi les jeunes générations – s'envoient des photographies de leur parties intimes au cours de la phase de séduction. Cette pratique pose problème lorsque l'expéditeur d'une telle photographie est un mineur, car il produit de la pornographie enfantine en photographiant sa zone génitale, la transfère lors de l'envoi via un système de messagerie instantanée et même la possède s'il en conserve une copie sur son *smartphone*. Dans cette situation, le mineur est paradoxalement à la fois auteur et victime de l'infraction réprimée par l'art. 9 CCC. Dans le cadre de l'art. 9 § 2 let. a CCC, nous pensons que les Parties pourraient prévoir que le mineur qui prend une photographie à connotation sexuelle de lui-même, la transmet ou la possède n'agit pas sans droit. Le destinataire de l'envoi qui demande à recevoir une telle image en ayant connaissance de l'âge de l'expéditeur agit en revanche clairement sans droit. 30

S'agissant de l'art. 9 § 2 let. b CCC, l'expression « sans droit » pourrait également permettre à une Partie de prévoir, par exemple, qu'une personne n'est **pas punissable** s'il est établi que l'individu représenté n'est pas « un mineur » au sens de cette disposition[173]. 31

D. L'intention

L'infraction 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 produire, d'offrir, de mettre à disposition, de diffuser, de transmettre, de se procurer ou de procurer à un tiers ou encore de posséder de la pornographie enfantine. 32

Les Parties peuvent toutefois adopter une **norme plus spécifique**, auquel cas cette dernière norme s'appliquerait. Ainsi la responsabilité pourrait, par 33

exemple, être imposée s'il y a « connaissance et contrôle » de l'information transmise ou stockée. Il ne suffit, par exemple, pas qu'un fournisseur de services serve d'intermédiaire pour la transmission de cette représentation, par le biais d'un site web ou d'un bavardoir, entre autres moyens, en l'absence de l'intention requise. De plus, un fournisseur de services n'est pas tenu de surveiller le contenu pour éviter la responsabilité pénale[174].

IV. LES RÉSERVES

34 L'art. 9 § 3 et 4 CCC autorise les Parties à **restreindre la punissabilité** de trois manières différentes, à savoir par rapport à l'âge des mineurs, aux comportements punissables et aux objets de la représentation.

A. Quant à l'âge des mineurs faisant l'objet de la représentation

35 Dans le processus d'élaboration de la convention, les Parties ont convenu qu'il était important de fixer l'âge de la majorité de manière uniforme. Elles ont ainsi décidé que le terme « mineur » désignait toute personne âgée de **moins de 18 ans**. Cette limite a été fixée au regard de la définition d' « enfant » donnée par l'article 1 de la Convention des Nations Unies relative aux droits de l'enfant[175]. Il faut toutefois souligner ici que cet âge fait référence à l'exploitation d'enfants en tant qu'objets sexuels. Il doit donc être distingué de l'âge requis pour consentir à des relations sexuelles.

36 Etant donné que certains Etats ont fixé une limite d'âge inférieure dans leur législation nationale concernant la pornographie enfantine, la dernière phrase du paragraphe 3 autorise les Parties à définir une limite d'âge différente, laquelle, en tout état de cause, ne doit **pas** être **inférieure à 16 ans**[176].

37 Le seul Etat à avoir fait usage de cette possibilité est la **Suisse**[177]. Elle a fixé la limite à l'âge de 16 ans pour correspondre à la teneur de l'ancien article 197 al. 3 et 3bis CP. Le 16 juin 2010, la Suisse a toutefois signé la Convention du

173. Rapport explicatif de la Convention sur la cybercriminalité, n. 103.
174. Rapport explicatif de la Convention sur la cybercriminalité, n. 105.
175. Rapport explicatif de la Convention sur la cybercriminalité, n. 104.
176. Rapport explicatif de la Convention sur la cybercriminalité, n. 104.
177. Réserve 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=2& codePays=SWI, visité le 21.1.2024), en lien avec l'ancien art. 197 du Code pénal suisse.

Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels. L'art. 20 de cette convention réprime les infractions se rapportant à la pornographie enfantine. La notion d' « enfant » qui y est mentionnée est définie à l'art. 3 let. a comme toute personne âgée de moins de 18 ans. Aucune réserve ne pouvant être émise par rapport à l'âge limite, l'art. 197 CP a dû être adapté. La nouvelle teneur de cette disposition est entrée en vigueur le 1er juillet 2014. Elle correspond désormais à la définition générale figurant à l'art. 9 § 3 CCC. La réserve émise par la Suisse au moment de la ratification de la convention n'a donc plus lieu d'être.

B. Quant aux comportements punissables

La convention autorise aussi les Parties à limiter la poursuite pénale en refusant de poursuivre le fait de se **procurer** ou de procurer à un tiers des images pédopornographique et/ou le fait d'en **posséder**. 38

Au moment de ratifier la convention, l'**Ukraine**, le **Japon** et le **Sri Lanka** ont fait usage de cette possibilité pour ne pas poursuivre l'obtention et la possession de pornographie enfantine[178]. En 2014, le Japon a modifié sa législation et a pénalisé la possession de pornographie enfantine, ainsi que le fait d'en procurer à autrui[179]. L'obtention pour soi-même n'est toutefois toujours pas punissable. 39

Israël a précisé qu'elle refusait de poursuivre l'obtention de pornographie enfantine[180]. 40

178. Réserve de l'Ukraine consignée dans l'instrument de ratification déposé le 10 mars 2006 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2& codePays=U, visité le 21.1.2024), en lien avec l'art. 301 du Code pénal ukrainien ; Réserve 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=2& codePays=JAP, visité le 21.1.2024), en lien avec l'ancien art. 7 de la Loi japonaise sur la répression des activités relatives à la prostitution enfantine et la pornographie enfantine, et la protection de l'enfance ; Réserve consignée dans une Note Verbale de l'Ambassade du Sri Lanka auprès de la Belgique, datée du 26 mai 2015, et dans l'instrument d'adhésion, déposés simultanément le 29 mai 2015 (disponible sous https://www.coe.int/fr/ web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=LKA, visité le 21.1.2024), en lien avec les art. 286A à 286D du Code pénal sri lankais.
179. Nouvel art. 7 de la Loi japonaise sur la répression des activités relatives à la prostitution enfantine et la pornographie enfantine, et la protection de l'enfance

41 L'**Argentine** a indiqué que la possession de pornographie enfantine n'était pas punissable dans son droit national[181].

42 D'autres Etats ont émis des réserves concernant la punissabilité de l'obtention ou la possession de pornographie enfantine à certaines **conditions particulières**.

43 Le **Danemark** a ainsi déclaré qu'il renonçait à punir la possession d'images pornographiques impliquant des enfants âgés de 15 ans au moins, si le mineur concerné a consenti à cette possession[182].

44 Au moment de la ratification de la convention, le **Monténégro** a précisé que l'obtention et la possession de pornographie enfantine n'étaient pas punissables quand la personne qui apparaît dans ces matériaux a quatorze ans au moins et a donné son consentement[183]. Depuis lors, cette exception a été supprimée[184].

C. Quant aux objets de la représentation

45 La convention autorise enfin les Parties à limiter la poursuite pénale en refusant de considérer comme illicite les images mettant en scène une **personne qui apparaît comme un mineur** se livrant à un comportement sexuellement explicite et/ou des **images réalistes** représentant un mineur se livrant à un comportement sexuellement explicite.

46 La **Principauté d'Andorre**, la **Grande-Bretagne**, l'**Argentine**, le **Chili**, les **Etats-Unis d'Amérique**, le **Japon**, le **Pérou** et le **Sri Lanka** ont déclaré qu'ils

180. Réserve d'Israël consignée dans l'instrument d'adhésion déposé le 9 mai 2016 (disponible sous https://www. coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays= ISR, visité le 21.1.2024), en lien avec la section 214b du Code pénal israélien.
181. Réserve de l'Argentine consignée dans l'instrument d'adhésion reçu et enregistré au Secrétariat Général le 5 juin 2018 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&num Ste=185&codeNature=2&codePays=ARG, visité le 21.1.2024), en lien avec l'art. 128 du Code pénal argentin.
182. Réserve du Danemark consignée dans l'instrument de ratification déposé le 21 juin 2005 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2& codePays=DEN, visité le 21.1.2024), en lien avec le § 235 par. 3 du Code pénal danois.
183. Réserve du Monténégro consignée dans l'instrument de ratification déposé le 3 mars 2010 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2& codePays=MOT, visité le 21.1.2024).

ne poursuivraient pas les représentations mentionnées à l'art. 9 § 2 let. b et c CCC[185]. Au moment de la ratification de la convention, l'Islande avait émis une réserve dans le même sens. Cette réserve n'est toutefois plus d'actualité car la loi du 25 juin 2012 a introduit un nouvel art. 210a dans le Code pénal islandais qui réprime aussi les représentations visées à l'art. 9 § 2 let. b et c CCC.

Le **Danemark**, la **Hongrie**, le **Monténégro**, la **Suisse** et **Israël** ont indiqué qu'ils renonçaient à punir les représentations visuelles d'une personne qui 47

184. Art. 211 du Code pénal monténégrin.

apparaît comme un mineur se livrant à un comportement sexuellement explicite (art. 9 § 2 let. b)[186]. La **France** a émis une réserve similaire en précisant qu'elle ne poursuivrait pas les images mettant en scène une personne, majeure au moment de la prise de vue, mais apparaît comme un mineur et se livre à un comportement sexuellement explicite[187].

185. Réserve consignée dans une Note Verbale du Ministère des Affaires étrangères d'Andorre, datée du 14 octobre 2016, déposée avec l'instrument de ratification le 16 novembre 2016 (disponible sous https://www.coe.int/fr/ web/conventions/full-list?module=signatures-by-treaty&treatynum=185, visité le 21.1.2024), en lien avec l'art. 155 à 157bis du Code pénal andorran ; Réserve de la Grande-Bretagne consignée dans l'instrument de ratification déposé le 25 mai 2011 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=UK, visité le 21.1.2024), en lien avec la section 1 du Protection of Children Act 1978 britannique ; Réserve de l'Argentine consignée dans l'instrument d'adhésion reçu et enregistré au Secrétariat Général le 5 juin 2018 (disponible sous https://www.coe.int/fr/web/ conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=ARG, visité le 21.1.2024), en lien avec l'art. 128 du Code pénal argentin ; 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. 367quater du Code pénal chilien ; Réserve 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=2&codePays=USA, visité le 21.1.2024), en lien avec le titre 18 §§ 2252ss et 2421ss du Code des Etats-Unis ; Réserve 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=2& codePays=JAP, visité le 21.1.2024), en lien avec l'art. 2 de la Loi japonaise sur la répression des activités relatives à la prostitution enfantine et la pornographie enfantine, et la protection de l'enfance ; Réserves 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=2&codePays=PER, visité le 21.1.2024), en lien avec l'art. 183-A du Code pénal péruvien ; Réserve consignée dans une Note Verbale de l'Ambassade du Sri Lanka auprès de la Belgique, datée du 26 mai 2015, et dans l'instrument d'adhésion, déposés simultanément le 29 mai 2015 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-bytreaty&numSte=185&codeNature=2&codePays=LKA, visité le 21.1.2024), en lien avec les art. 286A à 286D du Code pénal sri lankais.

V. COMPARAISON AVEC LE DROIT SUISSE

Les comportements ainsi que les différentes représentations réprimées par la convention trouvent leur équivalent en droit suisse à l'art. 197 al. 4 et 5 CP[188]. Le droit suisse est entièrement **conforme** à l'art. 9 CCC. 48

BIBLIOGRAPHIE

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

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

Isenring Bernhard/Kessler Martin A., in : Niggli Marcel Alexander/Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

186. Réserve du Danemark consignée dans l'instrument de ratification déposé le 21 juin 2005 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2& codePays=DEN, visité le 21.1.2024), en lien avec les § 230 et 235 du Code pénal danois ; Réserve de la Hongrie consignée dans l'instrument de ratification déposé le 4 décembre 2003 (disponible sous https://www. coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays= HUN, visité le 21.1.2024), en lien avec la section 204 du Code pénal hongrois ; Réserve du Monténégro consignée dans l'instrument de ratification déposé le 3 mars 2010 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=MOT, visité le 21.1.2024), en lien avec l'art. 211 du Code pénal monténégrin ; Réserve 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=2&codePays=SWI, visité le 21.1.2024), en lien avec l'art. 197 du Code pénal suisse ; Réserve d'Israël consignée dans l'instrument d'adhésion déposé le 9 mai 2016 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=ISR, visité le 21.1.2024), en lien avec la section 214b du Code pénal israelien.
187. Réserve de la France consignée dans l'instrument d'approbation déposé le 10 janvier 2006 (disponible sous https://www.coe.int/fr/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2& codePays=FRA, visité le 21.1.2024), en lien avec l'art. 227-23 du Code pénal français.
188. Voir au sujet des différentes formes de représentations et des comportements punissables : Corboz, n. 55ss et 61ss ad art. 197 CP ; Trechsel/Crameri, n. 10ss et 16ss ad art. 197 CP ; Isenring/Kessler, n. 20ss et 47ss ad art. 197 CP.

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)

Conseil de l'Europe, Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote 25.10.2007, disponible à https://rm.coe.int/16800d3832, visité le 21.1.2024 (cité : Rapport explicatif de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels)

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 11 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Julian Mausbach

PROPOSITION DE CITATION

Julian Mausbach, Commentaire de l'art. 11 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Mausbach, Art. 11 CCC N. XXX.

Titre 5 Autres formes de responsabilité et de sanctions

Art. 11 Tentative et complicité

[1] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des art. 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

[2] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des art. 3 à 5, 7, 8, 9. par. 1. let. a et c de la présente Convention.

[3] Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le par. 2 du présent article.

TABLE DES MATIÈRES

I. Champ d'application 148
II. Punissabilité de la participation (art. 11, al. 1) 148
III. Punissabilité des tentatives (art. 11, al. 2 et al. 3) 149
Matériaux 150

I. CHAMP D'APPLICATION

1 L'art. 11 a pour but d'ancrer le principe de la punissabilité de la tentative et de la participation en ce qui concerne les éléments constitutifs définis dans la Convention. L'al. 1 part du principe que la participation intentionnelle à une infraction intentionnelle au sens des art. 2 à 10 est punissable et sanctionnable aussi bien au sens d'une complicité que d'une instigation.

2 L'al. 2 limite déjà la punissabilité des tentatives aux art. 3-5, 7, 8 et 9, al. 1, let. a et c de la convention. Cette limitation de la punissabilité des tentatives aux infractions énumérées peut être mise en œuvre par les Parties de manière à ce que la punissabilité des tentatives soit écartée dans son ensemble ou en partie (al. 3).

3 La Suisse n'a pas fait usage de la possibilité de limitation prévue à l'al. 3 et prévoit donc une punissabilité de la tentative par le biais d'un rattachement à la partie générale du code pénal.

II. PUNISSABILITÉ DE LA PARTICIPATION (ART. 11, AL. 1)

4 L'art. 11 al. 1 prévoit une punissabilité de la participation pour les art. 2 à 10. Contrairement à la partie générale du code pénal (qui contient les articles 24 et 25 CP), aucune distinction n'est faite entre l'incitation et la complicité. Comme la mise en œuvre de l'al. 1 s'est faite directement par le biais des dispositions de la partie générale du code pénal, l'aménagement qui y a été fait, par exemple en ce qui concerne la punissabilité des tentatives (art. 24, al. 2, CP), a également des effets dans le champ d'application de la convention ou sur la mise en œuvre correspondante. Il n'existe pas de conditions objectives allant au-delà des articles 24 et 25 CP et la mise en œuvre par le biais de ces articles est donc également congruente.

5 La double intention de participer prévue à l'al. 2 en ce qui concerne l'acte de participation et l'acte principal est également exigée par les dispositions de la partie générale, de sorte qu'aucun complément n'était nécessaire ici.

6 Il convient de mentionner le complément apporté à la norme pénale de l'art. 143bis CP. Pour les détails, nous renvoyons au commentaire correspondant de l'art. 6. En ce qui concerne la question de la participation et de la tentative, il convient de souligner que même après le complément apporté à l'art. 143bis

CP, la tentative de complicité et l'aide à une infraction principale qui n'a pas (encore) été tentée restent impunies.

III. PUNISSABILITÉ DES TENTATIVES (ART. 11, AL. 2 ET AL. 3)

L'al. 2 prévoit l'obligation d'étendre la punissabilité des tentatives aux dispositions mentionnées. Aucun critère objectif n'est mentionné à cet égard, pas plus qu'une punissabilité générale des tentatives n'est prévue. Ce dernier point s'explique notamment par le fait que les systèmes juridiques de certaines parties contractantes ne prévoient pas de sanction générale, mais une sanction échelonnée en cas de tentative. La réglementation adoptée promet donc une option de mise en œuvre qui peut être (et a été) réalisée sans bouleversement majeur des concepts juridiques fondamentaux des Etats parties. 7

La mise en œuvre de la punissabilité des tentatives a été effectuée par le biais de l'art. 22 en relation avec l'art. 10. Art. 10 al. 2 et al. 3 CP. Elle s'étend ainsi à toutes les infractions mentionnées à l'al. 2. Cela résulte du fait que leur mise en œuvre s'effectue à nouveau par le biais d'infractions de la partie spéciale du CP, qui sont elles-mêmes conçues au moins comme des délits au sens de l'art. 10 al. 2 CP. 8

Bien que l'al. 2 ne contienne aucune obligation d'étendre la punissabilité des tentatives aux dispositions non mentionnées à l'al. 2, la mise en œuvre par le biais d'articles du code pénal a pour conséquence qu'une punissabilité des tentatives est également donnée en Suisse en ce qui concerne l'art. 2, l'art. 9 dans son ensemble ainsi que l'art. 10 CCC. En particulier, en incluant les délits dans les titres (art. 251 ss CP), les délits relatifs à la protection du secret des postes et des télécommunications (art. 321ter CP) ainsi que l'article sur la pornographie (art. 197 CP), qui sont eux-mêmes conçus au moins comme des délits, une transposition a eu lieu qui entraîne une punissabilité de la tentative pour les art. 2 à 10. Il n'y a donc pas de dissonance avec la punissabilité expérimentale prévue en principe par le droit pénal suisse pour les délits et les crimes. 9

L'al. 3 prévoit la possibilité pour les Parties de renoncer en tout ou en partie à la punissabilité des tentatives. Cette disposition devrait permettre de remédier aux éventuelles difficultés de mise en œuvre des parties contractantes. La 10

marge de manœuvre ainsi accordée pour la mise en œuvre devrait permettre, dans la mesure du possible, une ratification sans modifications fondamentales de l'ordre juridique respectif. En Suisse, cette possibilité n'a pas été et ne doit pas être utilisée, même pour des faits isolés ou des parties de faits. Cela est convaincant du point de vue du contenu, car cela n'implique pas de rupture avec la conception de la punissabilité des tentatives en Suisse. La réglementation de l'al. 3, qui doit être comprise comme une concession à la praticabilité de la mise en œuvre dans les ordres juridiques des Parties, est donc restée sans conséquence en Suisse.

MATÉRIAUX

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2010/813/de, besucht am 17.10.2023

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, abrufbar unter https://rm.coe.int/16800cce5b, besucht am 17.10.2023 (zit. Explanatory Report)

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 12 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Ugur Gürbüz

PROPOSITION DE CITATION

Ugur Gürbüz, Commentaire de l'art. 12 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Gürbürz, art. 12 CCC N. XXX.

Art. 12 Responsabilité des personnes morales

[1] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:

a. sur un pouvoir de représentation de la personne morale;

b. sur une autorité pour prendre des décisions au nom de la personne morale;

c. sur une autorité pour exercer un contrôle au sein de la personne morale.

2 Outre les cas déjà prévus au par. 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au par. 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

TABLE DES MATIÈRES

I. Introduction 154
II. Champ d'application et objectifs 155
A. Paragraphe 1 : pour les actes commis par des personnes exerçant un pouvoir de direction 155
B. Paragraphe 2 : Violation du devoir de surveillance 156
C. Paragraphe 3 : Nature de la responsabilité 157
D. Paragraphe 4 : Responsabilité individuelle 157
III. Normes pénales comparables en Suisse 158
A. Sanctions et mesures pénales selon le CP 158
B. Art. 102 al. 1 CP : Responsabilité subsidiaire 158
C. Art. 102 al. 2 CP : Responsabilité primaire 160
D. Dispositions du droit pénal administratif 160
1. Art. 6 DPA : responsabilité de l'employeur 161
2. Art. 7 DPA : responsabilité de l'entreprise 161
IV. Mise en œuvre de l'aspect pénal en Suisse 162
V. Normes comparables de droit civil et administratif en Suisse 163
VI. Mise en œuvre de l'aspect civil et administratif en Suisse 164
Bibliographie 164
Matériaux 165

I. INTRODUCTION

1 Le principe "**societas delinquere non potest**", issu du droit romain, a été considéré pendant des décennies en Europe continentale comme une règle immuable permettant de focaliser le droit pénal sur l'individu et d'exonérer les entreprises de toute responsabilité pénale. Cette conception d'un ordre juridique sans responsabilité pénale directe des entreprises est devenue obsolète lorsque l'économie s'est caractérisée par des structures d'exploitation plus complexes et une répartition globale du travail, augmentant ainsi les possibilités d'abus ainsi que le danger et la nocivité d'éventuels comportements fautifs des entreprises. En Europe, les Pays-Bas en 1976, la France en 1994 et le Danemark en 1996 ont introduit la punissabilité des entreprises dans leur code pénal. En Suisse, le droit pénal des entreprises est réglementé dans le code pénal depuis le 1er octobre 2003, mais la Suisse est considérée comme l'un des pays pionniers en matière d'introduction de la punissabilité des personnes morales en comparaison internationale. Avant même l'introduction dans le code pénal, les articles 6 et 7 de la loi sur le droit pénal administratif (DPA) pouvaient être utilisés dès 1974 en cas d'infractions commises dans des entreprises commerciales conformément à l'article 26 de la LCD (loi fédérale contre la concurrence déloyale). Ces dispositions étaient toutefois considérées comme des exceptions au principe généralement admis à l'époque, selon lequel les personnes morales ne sont pas susceptibles de commettre un délit, et n'étaient pas considérées comme relevant du droit pénal.

2 Dans le cadre de l'effectivité de la poursuite pénale voulue par l'introduction de la Convention sur la cybercriminalité du Conseil de l'Europe - suivant la **tendance européenne** - les Parties contractantes se sont vu imposer à l'art. 12 CCC, comme déjà dans les dispositions pénales largement identiques de la Convention pénale sur la corruption, des règles identiques de responsabilité des personnes morales, à savoir prévoir une responsabilité pour les infractions commises par leurs organes et autres collaborateurs. L'article 12 de la CCC oblige également les États parties à veiller à ce que les personnes morales soient soumises à des sanctions ou mesures appropriées, y compris des sanctions financières. Le principe selon lequel les entreprises ne peuvent pas être punissables a également continué à être protégé par la Convention sur la cybercriminalité.

II. CHAMP D'APPLICATION ET OBJECTIFS

La **responsabilité des personnes morales** prévue à l'article 12 vise, d'une part, à rendre les entreprises responsables des actes punissables commis par des personnes exerçant une fonction dirigeante, lorsque ces actes sont accomplis pour le compte de la personne morale (paragraphe 1). D'autre part, il prévoit la responsabilité des personnes exerçant une fonction dirigeante qui n'ont pas supervisé ou contrôlé des employés ou des agents et que ce manquement a facilité la commission d'une infraction pénale par des employés ou des agents, telle que définie dans la Convention (paragraphe 2). La Convention laisse aux Parties le choix de régler la responsabilité de la personne morale sur le plan civil, administratif ou pénal (paragraphe 3). Elle stipule en outre que la responsabilité d'une personne morale ne doit pas faire obstacle à la punissabilité éventuelle d'une personne physique ayant commis l'infraction (paragraphe 4). 3

A. Paragraphe 1 : pour les actes commis par des personnes exerçant un pouvoir de direction

L'art. 12 al. 1 CCC oblige les Parties à établir la responsabilité de la personne morale pour les infractions commises par des personnes exerçant un pouvoir de direction au sein de l'entreprise ou y participant en tant qu'instigateur ou complice. La disposition établit une **responsabilité causale** et comprend **quatre éléments constitutifs**: 4

a) La Convention exige une **infraction aux normes pénales formulées aux articles 2 à 10 de la Convention**, à savoir l'accès illicite (art. 2), l'interception illicite (art. 3), l'atteinte aux données (art. 4), l'atteinte à un système (art. 5), l'utilisation abusive de dispositifs (art. 6), la contrefaçon informatique (art. 7), la fraude informatique (art. 8), les infractions liées à la pornographie enfantine (art. 9) et la violation du droit d'auteur et des droits voisins (art. 10). 5

b) La responsabilité pénale selon le texte de la Convention se limite aux infractions **commises pour le compte de la personne morale**. Le critère "*pour le compte de la personne morale*" établit un lien entre l'infraction et la personne morale. Le champ d'application est limité aux infractions commises pour le compte d'une personne morale. Cet avantage peut être financier ou autre. Les avantages financiers directs sont, entre autres, les produits obtenus à la suite d'infractions pénales et qui permettent à la personne morale soit de 6

s'enrichir, soit d'économiser une dépense. Il y a avantage d'une autre nature lorsque le bénéfice de la personne morale n'est pas (principalement) financier, par exemple lorsque des commandes sont passées à la personne morale à la suite de pots-de-vin. La Convention ne contient pas de définition légale de la notion de personne morale. L'article 12 a été établi sur la base de l'interprétation historique et européenne de la notion de "personne morale", à savoir toute entité ayant le statut de personne morale en vertu du droit applicable, à l'exception des États ou des autres entités publiques dans l'exercice de leurs prérogatives de puissance publique et des organisations internationales de droit public.

7 c) Conformément aux principes de droit privé selon lesquels les personnes morales ne peuvent agir que par l'intermédiaire de leurs organes, les actes des organes sont directement des actes de la personne morale et la personne morale est responsable des actes des organes envers les tiers lésés, la Convention exige que **l'infraction soit commise par une personne physique** qui **exerce** un **pouvoir de direction** au sein de la personne morale. Entrent dans cette catégorie, selon l'énumération des let. a à c, les personnes physiques qui tirent leur fonction de direction et de gestion d'un pouvoir de représentation, de décision ou de contrôle. Le texte de la Convention exige donc que la responsabilité des personnes morales soit conçue comme un délit spécial, sans pour autant présupposer une fonction formelle d'organe chez l'auteur.

8 d) La Convention exige en outre des Etats parties que la personne physique agisse dans le cadre de l'autorité dont elle dispose dans l'**exercice d'une activité commerciale**, c'est-à-dire qu'elle agisse dans le cadre du pouvoir de représentation, de décision ou de contrôle dont elle dispose auprès de la personne morale, afin d'engager la responsabilité de cette dernière conformément à l'art. 12 al. 1 CCC.

B. Paragraphe 2 : Violation du devoir de surveillance

9 L'art. 12 al. 2 CCC oblige les États parties à tenir les entreprises pour responsables,

a) lorsque les personnes physiques mentionnées à l'al. 1 let. a à c **manquent à leur devoir de surveillance** des employés subordonnés **en raison d'un manque de surveillance et de contrôle**,

b) qui comme conséquence causale de cette violation, commettent alors une infraction au sens des **articles 2 à 10 de la CCC**

c) pour le **bénéfice de la personne morale** .

Le paragraphe 2 étend donc la responsabilité de la personne morale aux actes commis par des personnes qui commettent une infraction en tant qu'employés **n'occupant pas un poste de direction** au sein de la personne morale, lorsque l'infraction a été rendue possible par le fait que le dirigeant n'a pas exercé une surveillance suffisante sur l'employé subordonné. 10

On considère qu'il y a **défaut de surveillance** lorsque des mesures appropriées et adéquates n'ont pas été prises pour empêcher des actes criminels au profit de la personne morale par des employés ou des agents. La nature et l'intensité de l'obligation de surveillance dépendent de la forme et de la taille de l'entreprise, de ses normes de sécurité et de ses pratiques commerciales. L'obligation de surveillance ne doit pas donner lieu à une obligation générale de surveillance. 11

C. Paragraphe 3 : Nature de la responsabilité

L'art. 12 al. 3 CCC a été introduit dans la convention afin de tenir compte, dans la mesure du possible, des principes juridiques nationaux des États parties. Selon cette disposition de la Convention, la **responsabilité des personnes morales** peut être **pénale, civile ou administrative**. Lorsqu'ils adoptent une réglementation en la matière, les États parties doivent veiller à ce que leurs sanctions ou mesures, pénales ou non, à l'encontre des personnes morales remplissent les critères de l'article 13, al. 2, de la CCC, selon lequel elles doivent être effectives, proportionnées et dissuasives et inclure des sanctions pécuniaires. 12

D. Paragraphe 4 : Responsabilité individuelle

L'art. 12 al. 4 CCC précise que la responsabilité des personnes morales n **'exclut pas** la **responsabilité individuelle d'une personne physique**. Cette disposition n'oblige pas les États parties à introduire une responsabilité pénale parallèle. 13

III. NORMES PÉNALES COMPARABLES EN SUISSE

A. Sanctions et mesures pénales selon le CP

14 La responsabilité pénale des entreprises a été introduite dans le Code pénal suisse le 1er octobre 2003. Les motifs de cette décision étaient la peur du crime organisé, la crainte de grands dangers créés par l'homme ainsi que la signature de la "Convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales". En ratifiant cette **convention de l'OCDE**, la Suisse s'est engagée, selon l'art. 2, à prendre les mesures nécessaires, conformément à ses principes juridiques, pour établir la responsabilité des personnes morales en cas de corruption d'un agent public étranger.

B. Art. 102 al. 1 CP : Responsabilité subsidiaire

15 Selon l'art. 102 al. 1 CP, un crime ou un délit - mais pas une contravention - est imputé à une entreprise lorsqu'un crime ou un délit est commis dans "l'entreprise dans l'exercice d'activités commerciales conformes à son but" et que "cet acte ne peut être imputé à aucune personne physique déterminée en raison du manque d'organisation de l'entreprise". L'entreprise est donc punissable à titre subsidiaire en cas **de manque d'organisation**.

16 Le reproche adressé à l'entreprise consiste en ce que

a) un crime **ou un délit** selon l'ordre juridique suisse au sens de l'art. 10 CP a été **commis à titre d'infraction préalable**.

b) l'acte incriminé a été commis **dans une entreprise** et l'auteur de l'acte incriminé doit être intégré dans l'entreprise sur le plan hiérarchique ou organisationnel,

c) l'infraction a été commise "**dans l'exercice d'activités commerciales**", ce qui exige un lien fonctionnel entre l'infraction et l'activité commerciale, c'est-à-dire une activité économique minimale en rapport avec les activités de l'entreprise et qui inclut donc l'action avec pouvoir de représentation, de décision ou de contrôle exigée par l'article 12 CCC,

d) l'acte incriminé a été commis **dans le cadre de l'objectif de l'entreprise**,

ce qui justifie, selon la majorité, une limitation aux risques typiques de l'entreprise,

e) et que l'entreprise est responsable du fait que les autorités de poursuite pénale ne peuvent pas trouver de **personne physique responsable** en raison d'un manque d'organisation.

Tant que la responsabilité des personnes morales 17

- d'une part, conformément à l'art. 12 al. 1 de la Convention, vise à rendre les entreprises responsables des actes punissables commis par des personnes exerçant une fonction dirigeante, dans la mesure où ces actes sont accomplis pour le bénéfice de la personne morale,
- et d'autre part, selon l'art. 12 al. 2 CCC, les personnes exerçant une fonction dirigeante qui ont omis de superviser ou de contrôler des employés ou des agents et que cette omission facilite la commission d'une infraction pénale par des employés ou des agents, telle que définie par la Convention,

ces deux variantes d'infraction trouvent un large écho dans la responsabilité pénale subsidiaire de l'entreprise selon l'art. 102 al. 1 CP. Cette disposition **couvre tous les délits selon la cyberconvention**, sans les énumérer explicitement.

La convention se limite aux infractions selon les articles 2 à 10 de la CCC, qui 18
sont commises au profit de la personne morale et par ses représentants. En revanche, la responsabilité selon le CP s'applique à tout crime ou délit commis dans le cadre de l'objet de l'entreprise par une personne dans l'exercice d'une activité commerciale. Par rapport au texte de la Convention, la responsabilité selon le CP va donc plus loin, car le CP **ne pré** suppose **pas d'infraction commise en faveur de la personne morale comme critère** de responsabilité de l'entreprise.

L'art. 102 al. 1 CP, selon lequel la sanction de la personne morale n'est possible 19
que si l'acte ne peut être imputé à aucune personne physique, et l'art. 12 al. 4 CCC, selon lequel la punissabilité de la personne morale ne doit pas affecter la responsabilité de l'auteur, ne sont pas en contradiction l'un avec l'autre, car une **responsabilité pénale des personnes physiques agissant** n'est **pas exclue par la responsabilité subsidiaire de l'entreprise**. En Suisse, il est

même possible de punir aussi bien la personne physique que la personne morale si le défaut d'organisation de l'entreprise est imputable à une personne physique et que cette personne ne peut être identifiée qu'après la condamnation de l'entreprise.

20 Comme peine, l'art. 102 al. 1 CP prévoit une **amende de cinq millions de francs au** maximum, ce qui correspond au texte de la Convention de l'art. 13 al. 2, selon lequel les Etats parties doivent imposer des sanctions pécuniaires.

C. Art. 102 al. 2 CP : Responsabilité primaire

21 Indépendamment de la punissabilité des personnes physiques, depuis le 1.10. 2003, une **entreprise est tenue pour responsable au premier chef** s'il s'agit d'une infraction visée aux articles 260ter CP (organisation criminelle), 260quinquies CP (financement du terrorisme), 305bis CP (blanchiment d'argent), 322ter CP (corruption d'agents publics suisses), 322quinquies CP (octroi d'un avantage), 322septies alinéa 1 CP (corruption d'agents publics étrangers) ou 322octies CP (corruption passive) et que l'entreprise n'a pas pris toutes les mesures organisationnelles nécessaires et raisonnables pour empêcher une telle infraction. La **violation des obligations** réside dans le non-respect des devoirs d'organisation qui favorisent les infractions incriminées, énumérées de manière exhaustive. Conformément à l'art. 102 al. 2 CP, la sanction s'ajoute à une éventuelle sanction d'une personne physique.

22 Aucun des délits visés aux art. 2 à 10 CCC ne figure dans la liste des délits de l'art. 102 al. 2 CP, raison pour laquelle la responsabilité des personnes morales selon l'art. 12 CCC reste sans importance par rapport à la responsabilité pénale primaire des entreprises. Il s'ensuit que, conformément aux dispositions légales existantes, **aucune imputation directe de la faute d'autrui à une entreprise n'est possible** en Suisse en relation avec les normes pénales formulées dans les articles 2 à 10 de la CCC.

D. Dispositions du droit pénal administratif

23 Avant l'introduction de la responsabilité pénale de l'entreprise et de la réglementation de l'imputabilité (art. 29 CP) dans le droit pénal fondamental et avant la ratification de la Convention sur la cybercriminalité, les personnes physiques et morales étaient tenues en Suisse de répondre des infractions commises dans les entreprises par la loi fédérale sur le droit pénal

administratif. Les dispositions correspondantes du droit pénal administratif **sont toujours en vigueur**: l'art. 6 DPA sanctionne les personnes physiques qui ont un lien particulier avec l'entreprise. L'art. 7 DPA traite de la punissabilité des personnes morales. Des recoupements sont possibles entre les dispositions du CP et celles du DPA. Les art. 6 et 7 DPA sont applicables tant que les lois renvoient explicitement à l'une des dispositions ou au droit pénal administratif dans son ensemble.

1. Art. 6 DPA : responsabilité de l'employeur

L'objet de la responsabilité pénale selon l'art. 6 DPA est toujours une **personne individuelle**. Si des infractions sont commises dans la gestion des affaires d'une personne morale, d'une société en nom collectif ou en commandite, d'une entreprise individuelle ou d'une collectivité de personnes sans personnalité juridique, ou de toute autre manière dans l'exercice d'activités commerciales ou de service, l'alinéa 1 prévoit que la disposition pénale s'applique à la personne physique qui a commis l'infraction. Les alinéas 2 et 3 concrétisent le fait que le chef d'entreprise, l'employeur, le mandant, le représenté, voire l'organe et le membre de l'organe, l'associé gérant, le liquidateur et la personne qui dirige effectivement l'entreprise doivent être tenus pour responsables tant qu'ils ont omis, intentionnellement ou par négligence, de prévenir une infraction commise par le subordonné, le mandataire ou le représentant ou d'en supprimer les effets, en violation d'une obligation juridique. L'article 6 est un délit d'omission en violation d'une obligation légale. La responsabilité de droit pénal administratif du chef d'entreprise qui découle de l'article 6 limite considérablement le champ d'application de la punissabilité subsidiaire de l'entreprise selon l'article 102 al. 1 CP et conduit à la décharge de l'entreprise, car elle permet de l'imputer à une personne physique. 24

2. Art. 7 DPA : responsabilité de l'entreprise

L'art. 7 DPA prévoit une responsabilité pénale subsidiaire de la personne morale en droit pénal administratif. Cette disposition vise à réduire le travail d'enquête des autorités de poursuite pénale **en cas de délits mineurs**, conformément au principe d'opportunité modéré. En même temps, elle contredit le principe de l'établissement de la vérité matérielle et le principe de légalité. Ainsi, selon l'art. 7 DPA, il est possible de renoncer à la poursuite d'une personne physique et de condamner à sa place la personne morale, la 25

société en nom collectif ou en commandite ou l'entreprise individuelle au paiement d'une amende, si les conditions suivantes sont remplies :

a) l'infraction est commise dans le cadre de l'activité commerciale

b) une amende de CHF 5'000.00 au maximum est envisageable et

c) l'identification de l'auteur individuel entraînerait des frais d'enquête disproportionnés.

Si une personne physique est identifiée comme auteur, l'application de l'art. 7 DPA est exclue. En droit pénal administratif, cette disposition ne remplace pas non plus l'art. 102 al. 1 CP. En raison de leur contenu réglementaire différent, les deux normes peuvent être appliquées.

IV. MISE EN ŒUVRE DE L'ASPECT PÉNAL EN SUISSE

26 En raison de la **large couverture du contenu de la Convention** par l'art. 102 al. 1 CP, le législateur a renoncé à juste titre à une responsabilité pénale primaire de l'entreprise en relation avec l'art. 12 CCC et à une extension du champ d'application qui en découlerait. Certes, la Convention consacre une responsabilité parallèle de l'entreprise qui, en Suisse, ne peut être assurée au niveau pénal que par la responsabilité pénale primaire de l'entreprise selon l'art. 102 al. 2 CP, mais elle n'exige pas des Etats parties qu'ils réglementent la responsabilité pénale des entreprises. L'article 12 de la Convention n'exige pas la création d'une norme pénale au sens strict, mais laisse aux Etats parties, à l'al. 3, le soin de régler la responsabilité de la personne morale également sur le plan du droit civil ou administratif. Etant donné que la responsabilité subsidiaire selon l'art. 102 al. 1 CP couvre toutes les infractions selon les articles 2 à 10 CCC, d'autant plus qu'elle garantit que les crimes et délits commis en faveur d'une entreprise ne restent pas impunis, le législateur est parti à juste titre du principe qu'une responsabilité primaire plus étendue irait au-delà de la mesure minimale requise par la convention. En vertu de l'art. 2 DPA, selon lequel la réglementation du droit pénal des entreprises du CP s'applique également au droit pénal administratif, dans la mesure où la DPA elle-même ou la loi administrative individuelle n'en dispose pas autrement, mais aussi en vertu de l'art. 7 DPA, selon lequel les associations de personnel peuvent être punies à la place des auteurs individuels difficilement

identifiables, la responsabilité des personnes morales est également garantie en cas d'infractions aux lois fédérales, comme par exemple à la loi sur le droit d'auteur.

Contrairement au libellé et à l'objectif de l'art. 12 al. 1 CCC, le législateur suisse n'a pas doté l'art. 102 CP d'une responsabilité causale. Alors que l'art. 12 al. 1 CCC prévoit qu'une personne morale supporte le risque de responsabilité lors de l'exercice d'un délit au sein de l'entreprise, indépendamment de toute faute, l'art. 102 CP exige une faute d'organisation pour la responsabilité pénale de la personne morale. Malgré cette différence, la Suisse satisfait néanmoins aux exigences de l'art. 12 CCC, car une "responsabilité" au sens de la convention n'implique pas nécessairement une punissabilité de la personne morale (cf. art. 12 al. 3 CCC). 27

V. NORMES COMPARABLES DE DROIT CIVIL ET ADMINISTRATIF EN SUISSE

L'ordre juridique suisse connaît, du point de vue du droit civil et administratif, différents instruments de responsabilité pour les dommages ainsi que de prévention de dommages futurs. Outre les **réglementations en matière de responsabilité et les mesures organisationnelles** dans le droit civil, il convient également de mentionner les **instruments de surveillance** des autorités. 28

Dans le détail, ces instruments sont notamment les suivants (liste non exhaustive) : 29

- Dissolution de l'association par le tribunal conformément à l'art. 78 CC, si le but de l'association est illicite ou immoral ;
- Dissolution de la fondation par l'autorité fédérale ou cantonale compétente conformément à l'art. 88 CC, dont le but est devenu illicite ou immoral ;
- Responsabilité de la société au titre de la responsabilité du chef d'entreprise selon l'art. 55 CO ;
- Responsabilité de la société pour les auxiliaires selon l'art. 101 CO ;

- Responsabilité de la société pour le dommage résultant d'un acte illicite commis par un associé dans l'exercice de ses fonctions, conformément à l'art. 567 al. 3 CO ;
- Responsabilité de la société pour les dommages résultant d'actes illicites commis par un liquidateur dans l'exercice de ses fonctions, conformément aux art. 586 CO et 743 CO ;
- Responsabilité de la société pour les dommages résultant d'actes illicites commis dans l'exercice de ses fonctions par une personne autorisée à gérer l'entreprise ou à la représenter, conformément aux art. 722 CO et 817 CO ;
- Dissolution de la société en cas de carences dans l'organisation selon l'art. 731b CO ;
- Responsabilité de la société coopérative pour les dommages résultant d'actes illicites commis dans l'exercice de ses fonctions par une personne autorisée à gérer l'entreprise ou à la représenter, conformément à l'art. 899 CO ;
- Sanctions administratives de l'Autorité fédérale de surveillance des marchés financiers conformément à la loi sur la surveillance des marchés financiers.

VI. MISE EN ŒUVRE DE L'ASPECT CIVIL ET ADMINISTRATIF EN SUISSE

30 Le droit civil et administratif suisse prévoit un **grand nombre de sanctions et de mesures** à l'encontre des sociétés en cas d'actes illicites commis dans l'exercice d'une activité commerciale. Tant que les sociétés sont gérées pour l'exploitation d'un commerce et non exclusivement pour commettre des infractions, les sanctions et mesures de droit civil et administratif sont en principe suffisantes pour assurer la sanction effective et dissuasive requise par l'article 13 al. 2 de la CCC.

BIBLIOGRAPHIE

Ackermann Jürg-Beat, Wirtschaftsstrafrecht der Schweiz, 2. Aufl., Bern 2021 (zit. Ackermann, Bearbeiter/in, § ... N ...).

Donatsch Andreas/Heimgartner Stefan/Isenring Bernhard/Maurer Hans/Riesen-Kupper Marcel/Weder Ulrich (Hrsg.), StGB/JStG Kommentar, Mit weiteren Erlassen und Kommentaren zu den Strafbestimmungen des SVG, BetmG, AIG und OBG, 21. Aufl., Zürich 2022 (zit. StGB/JStG Kommentar, Art. ... StGB N ...).

Forster Matthias, Die strafrechtliche Verantwortlichkeit des Unternehmens nach Art. 102 StGB, Bern 2006.

Frank Friedrich/Eicker Andreas/Markwalder Nora/Achermann Jonas (Hrsg.), Basler Kommentar zum Verwaltungsstrafrecht, 1. Aufl., Basel 2020 (zit. BSK-Bearbeiter/in, Art. ... VStrR N ...).

Heine Günter, Europäische Entwicklung bei der strafrechtlichen Verantwortlichkeit von Wirtschaftsunternehmen und deren Führungskräften, ZStrR 119 (2001), S. 22 ff.

Jean-Richard-dit-Bressel Marc, Das Desorganisationsdelikt in Finanzdienstleistungsunternehmen, SZW 2022, S. 572-585.

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar zum Strafrecht I, Art. 1-136 StGB, 4. Aufl., Basel 2019 (zit. BSK-Bearbeiter/in, Art. ... StGB N ...).

Riklin Franz, Schweizerisches Strafrecht – Allgemeiner Teil I – Verbrechenslehre, 3. Aufl., Zürich/Basel/Genf 2007.

MATÉRIAUX

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2010/813/de, besucht am 30.4.2024.

Botschaft zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz über das Jugendstrafrecht vom 21.9.1998, BBl 1999 II 1979 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1999/1_1979_1787_1669/de, besucht am 30.4.2024.

Bundesamt für Justiz, Vernehmlassungsentwurf, Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, Vorentwurf und Erläuternder Bericht, Bern, März 2009, abrufbar unter https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/cybercrime-europarat.html, besucht am 30.4.2024.

Dänischen Strafgesetzbuch, abrufbar unter https://www.retsinformation.dk/eli/lta/2022/1360, besucht am 30.4.2024.

Erläuternder Bericht zu dem Zweiten Protokoll zum Übereinkommen über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften (vom Rat angenommen am 12.3.1999), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A51999XG0331, besucht am 30.4.2024.

Französisches Strafgesetzbuch, abrufbar unter https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2024-01-19, besucht am 30.4.2024.

Niederländischen Strafgesetzbuch, abrufbar unter https://wetten.overheid.nl/BWBR0001854, besucht am 30.4.2024.

Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013L0040, besucht am 30.4.2024.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 16 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Ugur Gürbüz

PROPOSITION DE CITATION

Ugur Gürbüz, Commentaire de l'art. 16 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Gürbüz, art. 16 CCC N. XXX.

Titre 2 Conservation rapide de données informatiques stockées

Art. 16 Conservation rapide de données informatiques stockées

[1] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

[2] Lorsqu'une Partie fait application du par. 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

[3] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en oeuvre desdites procédures pendant la durée prévue par son droit interne.

[4] Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux art. 14 et 15.

TABLE DES MATIÈRES

I. Introduction 170
II. Champ d'application et objectifs 170
A. Alinéa 1 : Sauvegarde immédiate des données informatiques 171
B. Alinéa 2 : Saisie de données par voie de conservation 172
C. Alinéa 3 : obligation de garder le secret 173
D. Alinéa 4 173
III. Mise en œuvre en Suisse 173
A. Saisie par les autorités de poursuite pénale 174
B. Demande de sauvegarde à des personnes 175
C. Absence de disposition légale concernant l'ordre de conservation 176
D. Saisie bloquée par le Tribunal fédéral malgré une demande de mise sous scellés valable 178
Bibliographie 179
Matériaux 179

I. INTRODUCTION

1 Le fait que des cybercriminels professionnels et compétents utilisent de plus en plus les technologies les plus récentes et Internet à des fins illégales pose des défis croissants aux autorités. Toutefois, les possibilités techniques d'abus ne garantissent pas une sécurité permanente et absolue aux criminels tant que les autorités agissent de manière ciblée. En effet, **des traces sont laissées sur les supports de données et sur Internet** : chaque action effectuée en ligne, par exemple la consultation d'un site web, la publication sur les réseaux sociaux ou les achats en ligne, génère des données qui sont stockées et peuvent être retracées. La création d'images à partir de supports de données saisis permet de restaurer des données supprimées et non écrasées. Ces données, même si elles ne sont stockées que brièvement et temporairement, peuvent être utiles aux autorités de poursuite pénale pour identifier les auteurs, élucider des infractions ou mettre en place des mesures de surveillance, à condition qu'elles soient sauvegardées à temps.

2 Le fait que **des données informatiques** aient été **enregistrées** et soient encore **disponibles** au moment de l'enquête dépend, d'une part, du comportement du détenteur des données en matière de suppression et, d'autre part, des dispositions relatives à la protection des données en vigueur dans l'État contractant concerné.

II. CHAMP D'APPLICATION ET OBJECTIFS

3 En raison de leur caractère éphémère, les données informatiques sont faciles à manipuler, à modifier et à supprimer. Le risque de perte ou de destruction des données est donc élevé dans la pratique. Afin de ne pas faire dépendre la sauvegarde de ces données informatiques et des données de connexion dans les procédures pénales nationales de longues procédures d'obtention de preuves, mais d'empêcher rapidement et efficacement la suppression et la modification des données pertinentes pour la preuve au moyen d'une mesure de sauvegarde et d'accroître ainsi l'efficacité de la poursuite des infractions décrites plus en détail dans la Convention sur la cybercriminalité, les États parties se sont engagés à prendre les mesures législatives nécessaires à l'échelle nationale. La procédure visant à sécuriser immédiatement et en temps utile les données informatiques stockées est appelée dans la pratique

«**procédure de gel rapide**». Il ne faut pas confondre la procédure de gel rapide avec la sécurisation immédiate des données dans un contexte transfrontalier, appelée «demande de conservation», qui est régie par l'art. 29 CCC.

L'art. 16 CCC régit la **saisie immédiate des données**, mais n'autorise pas en soi les États contractants à ordonner la remise des données ou à en consulter le contenu, tant qu'aucune norme nationale ne le permet expressément. La remise des données est régie par l'art. 18 CCC, tandis que la perquisition et la saisie sont traitées à l'art. 19 CCC. 4

A. Alinéa 1 : Sauvegarde immédiate des données informatiques

L'art. 16, al. 1, CCC garantit la sauvegarde rapide des données informatiques au sein d'un État contractant afin de contrer le risque de dissimulation lié au caractère volatile des données informatiques. Les données doivent être protégées « *contre tout ce qui pourrait altérer ou détériorer leur qualité ou leur état* » et donc contre toute modification, détérioration ou suppression. La sauvegarde désigne la **conservation provisoire des données** et non le refus d'accès aux données. Les utilisateurs légitimes doivent pouvoir continuer à utiliser les données ou leurs copies tant qu'elles ne doivent pas être saisies en vertu de l'art. 19 CCC. 5

L'art. 16 CCC n'oblige pas les États contractants à restreindre l'offre ou l'utilisation de services, ni à introduire de nouvelles possibilités techniques pour la conservation et la collecte de données. Cette disposition n'entraîne donc pas d'obligation de conservation des données. Elle vise uniquement à garantir que les États contractants puissent, au niveau national, ordonner une **saisie accélérée** des données informatiques stockées afin de se prêter mutuellement assistance au niveau international. 6

La **mise en œuvre** concrète des mesures de sauvegarde est laissée à l'appréciation des parties contractantes. Dans la pratique, deux options sont envisageables : la sauvegarde des données originales et la création de copies identiques des données. 7

Selon le libellé de l'art. 16, al. 1, CCC, la sauvegarde concerne «*certaines données informatiques, y compris les données relatives au trafic, qui ont été stockées au moyen d'un système informatique*». Sont concernées toutes les données informatiques déjà collectées et enregistrées par les détenteurs de 8

données ou les fournisseurs de services, appelées «**stored computer data**». Les données de connexion et de trafic, appelées «traffic data», sont également mentionnées explicitement. La référence aux données de trafic sert à établir un lien entre les mesures prévues aux art. 16 et 17 CCC. Cette dernière disposition prévoit certaines particularités pour les données de trafic. Ne sont pas concernées les collectes prospectives en temps réel de données informatiques ni la conservation de données, dite « data retention ». Celles-ci sont régies par les art. 20 et 21 CCC.

9 La conservation peut être ordonnée ou réalisée de manière similaire.

a) Le terme «**ordonner**» désigne tant la décision judiciaire ou administrative visant à garantir la conservation des données que l'obligation pour le destinataire de la décision de coopérer activement. Ce dernier doit le faire en conservant les données sans les modifier et sans les détruire (cf. art. 16, al. 2, CCC).

b) La formulation «**ou de manière similaire**» permet aux États contractants d'organiser la conservation des données de manière flexible et avec leurs propres moyens, conformément à leur droit procédural.

10 Les États contractants devraient notamment prévoir des mesures de sauvegarde lorsqu'il y a lieu de supposer que les données informatiques sont particulièrement **susceptibles d'être perdues ou modifiées**. Cela peut être le cas, par exemple, lorsque les données sont soumises à un délai de conservation court en vertu de la politique commerciale, sont effacées à intervalles réguliers ou sont stockées de manière non sécurisée.

B. Alinéa 2 : Saisie de données par voie de conservation

11 L'art. 16, al. 2, CCC prévoit que lorsque des données informatiques sont saisies en vertu de l'art. 16, al. 1, CCC, les Etats contractants peuvent prendre des mesures et introduire des «**Preservation Orders**» afin de garantir l'intégrité de ces données informatiques pendant une durée limitée. Les États contractants ne sont toutefois pas tenus de prendre de telles mesures. Les États contractants doivent veiller à ce que leurs autorités chargées de l'enquête puissent, quelle que soit la procédure choisie, ordonner ou faire ordonner la sauvegarde immédiate/sans délai.

Sont considérées comme **destinataires de l'ordonnance** les personnes qui sont en possession de données informatiques enregistrées ou qui ont le pouvoir de disposer de ces données. 12

Les États contractants peuvent, dans leur droit interne, en tant que mesure au sens de l'art. 16, al. 2, CCC, obliger les destinataires de l'ordonnance à préserver, aussi longtemps que nécessaire, mais pendant 90 jours au maximum, l'intégrité des données informatiques qui font l'objet de l'ordonnance. Ils peuvent toutefois prévoir une prolongation de ce **délai de conservation**. La fixation d'un délai sert à donner aux autorités compétentes suffisamment de temps pour obtenir les autorisations nécessaires et engager des démarches juridiques telles que la perquisition, la saisie, la mise sous séquestre ou l'émission d'une ordonnance de remise, afin qu'elles puissent ensuite, dans un deuxième temps, prendre connaissance du contenu des données, notamment dans le cadre d'une entraide judiciaire au sens de l'art. 29 CCC. 13

C. Alinéa 3 : obligation de garder le secret

L'art. 16, al. 3, CCC exige des États parties qu'ils prennent les mesures législatives nécessaires pour que, lorsqu'une décision est adressée au **dépositaire ou à un tiers**, ceux-ci soient tenus, pendant une durée fixée par le droit interne, de procéder à la conservation des données de manière confidentielle. Cette mesure tient compte, d'une part, de la nécessité pour les autorités de poursuite pénale que les suspects et les tiers ne puissent pas avoir connaissance de l'enquête et, d'autre part, de la protection de la sphère privée des personnes concernées, en particulier celles qui sont mentionnées dans les données ou qui peuvent être identifiées. 14

D. Alinéa 4

Par les **renvois** à l'art. 16, al. 4, CCC, les Etats contractants s'engagent à garantir que les pouvoirs et procédures mentionnés à l'art. 16 CCC sont soumis aux conditions et garanties prévues aux art. 14 et 15 CCC. 15

III. MISE EN ŒUVRE EN SUISSE

La sauvegarde des données informatiques enregistrées conformément à l'art. 16 CCC constitue un **instrument d'enquête** important pour lutter contre les 16

infractions informatiques et liées aux technologies de l'information. Les États parties, y compris la Suisse, sont tenus de créer les conditions-cadres législatives et organisationnelles nécessaires à cet effet.

17 La Suisse n'a pas intégré la « procédure de gel rapide » prévue à l'art. 16 CCC en tant que mesure autonome dans le code de procédure pénale suisse en vigueur. Au lieu de cela, le **droit suisse** satisfait déjà aux exigences de l'art. 16 CCC de manière générale, dans la mesure où **les fournisseurs de services de télécommunication** sont tenus, d'une part, **en vertu des art. 21 al. 2 et 22 al. 2 LSCPT**, de veiller à ce que les données d'identification soient collectées lors de l'établissement de la relation client et restent accessibles pendant toute la durée de la relation client et jusqu'à six mois après sa fin, et, d'autre part, **conformément à l'art. 26, al. 5, LSCPT**, de conserver les données de trafic pendant six mois.

18 Même considérée séparément, la législation suisse en vigueur satisfait aux exigences de l'article 16 de la Convention. Selon le code de procédure pénale suisse, les données informatiques peuvent être saisies soit sur ordre écrit du ministère public dans le cadre d'une perquisition au sens des **articles 246 ss CPP**, soit être versées au dossier en vertu d'une décision de production au sens de l'**article 265 CPP**. En Suisse, la conservation des données informatiques enregistrées peut être divisée en deux catégories : la conservation par les autorités de poursuite pénale et la demande de conservation adressée à des personnes. Ces deux mesures peuvent également être prises par la police, sans décision du ministère public, en cas de danger imminent, ce qui garantit une conservation accélérée et proportionnée des données informatiques enregistrées.

A. Saisie par les autorités de poursuite pénale

19 En Suisse, la saisie provisoire de données est ordonnée par le ministère public (ou, le cas échéant, par le tribunal compétent) en vertu des art. 198, 241, al. 1, et **246 CPP** afin de permettre la recherche d'enregistrements. Cette mesure garantit que les données peuvent être examinées quant à leur contenu ou leur nature afin de déterminer leur valeur probante et, le cas échéant, de les saisir. Dans la pratique, ces perquisitions et la sauvegarde des données sont ordonnées par la police conformément à l'art. 312 CPP. La police procède alors à une perquisition conformément aux instructions du ministère public (ou du tribunal compétent) et saisit le support de données ou établit une copie

légale des données présentes sur les supports de données trouvés et à perquisitionner (ce que l'on appelle le « miroir des données »). La copie garantit que les données sont copiées sur un support externe et protégées contre toute manipulation. Dans les procédures pénales économiques notamment, cela permet de garantir que les données au sens de l'art. 16, al. 1, CC peuvent être conservées sans délai. D'autre part, les personnes concernées par la perquisition peuvent continuer à utiliser leurs appareils pour poursuivre leurs activités commerciales, dans le respect du principe de proportionnalité, tant que les appareils ne doivent pas être saisis en vue de leur confiscation conformément à l'art. 263 CPP en relation avec l'art. 69, al. 1, CP.

Afin de garantir la **sécurité des données stockées sur des serveurs numériques ou dans le cloud**, il est impératif de procéder immédiatement à une copie miroir des données sur place afin d'empêcher que celles-ci ne soient modifiées ou effacées par d'autres moyens d'accès. La base légale pour la réalisation de copies de tels enregistrements et données dans le cadre d'une perquisition est l'art. 247, al. 3, CPP. 20

B. Demande de sauvegarde à des personnes

En ce qui concerne la perquisition et la saisie de données, le ministère public (le cas échéant également le tribunal compétent) a en outre la possibilité, au sens des art. 263 et 265 CPP, d'ordonner par décision la remise et la saisie de données à savoir d'obliger concrètement le détenteur, sous peine des sanctions prévues à l'art. 292 CP et en fixant un délai, à remettre les supports électroniques et les données, sous forme d'originaux ou de copies, à titre de moyens de preuve. Cette procédure est désignée par les termes **« édition** » et « **éditer** ». Une telle remise ne peut toutefois être ordonnée que si le détenteur n'est ni la personne prévenue, ni une personne bénéficiant du droit de refuser de témoigner ou de faire des déclarations, ni une entreprise qui pourrait engager sa responsabilité pénale ou civile en cas de remise (art. 265, al. 2, CPP). Une autre condition préalable à la délivrance d'une ordonnance de production est que l'ordonnance soit adressée au détenteur effectif des données domicilié en Suisse, faute de quoi la voie de l'entraide judiciaire internationale en matière pénale doit être suivie. 21

Si une personne est tenue, en vertu de l'art. 2 LSCPT, de transmettre les métadonnées dont elle dispose sur une personne surveillée, les art. 269 ss 22

CPP. Dans la mesure où les conditions prévues à l'art. 269 al. 1 let. b et c CPP sont remplies et où le tribunal des mesures de contrainte a donné son autorisation, une saisie au sens de l'art. 263 CPP n'entre certes pas en ligne de compte, mais les **fournisseurs de services de télécommunication** domiciliés en Suisse, en tant que détenteurs des données accessoires, peuvent être contraints de procéder à une sauvegarde des données conformément à l'art. 273 CPP. L'obtention de données de situation n'est pas une mesure de contrainte et ne nécessite pas l'autorisation du tribunal des mesures de contrainte.

C. Absence de disposition légale concernant l'ordre de conservation

23 En Suisse, seuls les fournisseurs de services de télécommunication sont légalement tenus, en vertu de l'art. 2 LSCPT, de conserver les données d'identification et les données accessoires pendant six mois. En relation avec ces données conservées, diverses autorités fédérales et cantonales ont le droit, en vertu de l'**art. 15 LSCPT**, d'obtenir des renseignements sur les services de télécommunication au sens de l'art. 21 LSCPT ainsi que sur l'identité des auteurs d'infractions au sens de l'art. 22 LSCPT. Une telle communication de renseignements équivaut à une obligation de remise au sens de l'art. 265 CPP. Il ne s'agit pas ici d'une «preservation order» au sens de l'art. 16, al. 2, CCC.

24 En ratifiant la Convention sur la cybercriminalité, la Suisse ne s'est pas engagée à introduire les «preservation orders» dans son droit interne. Actuellement, le code de procédure pénale suisse ne prévoit pas non plus **de base légale** permettant d'ordonner aux détenteurs de données et aux fournisseurs de services de protéger les données contre la perte ou la modification et de les tenir à la disposition des autorités de poursuite pénale sans devoir les remettre immédiatement. Le message part du principe que la possibilité d'obliger quiconque à conserver des données par voie de décision administrative irait trop loin et serait difficilement compatible avec le principe de proportionnalité. Cette appréciation n'est plus d'actualité : en raison de la numérisation croissante, même les particuliers disposent aujourd'hui de capacités de stockage considérables sur leurs supports de données. De nombreuses entreprises dignes de confiance et disposées à coopérer disposent volontairement et conformément aux dispositions suisses en

matière de protection des données (LPD) de données pertinentes à des fins de preuve, telles que des données clients et des données techniques (non soumises à la LSCPT), sans être tenues de respecter un délai de conservation. Une injonction faite aux détenteurs de telles données de prolonger le délai de conservation à 90 jours au maximum constitue une mesure nettement moins contraignante que d'ordonner la perquisition des enregistrements auprès des détenteurs de données concernés (cf. ci-dessus N. 19 s.) ou de les obliger à remettre immédiatement l'intégralité des données (cf. ci-dessus N. 21 s.). En cas de prolongation du délai de conservation, les destinataires de la décision ne sont pas soumis à une charge disproportionnée compte tenu des possibilités techniques actuelles, et il existe un intérêt public à garantir que les données collectées volontairement par des particuliers puissent être conservées comme moyens de preuve aux fins de la recherche de la vérité avant d'être effacées.

En vertu de l'actuelle procédure pénale suisse, la conservation des données détenues par des personnes qui ne sont pas soumises à la LSCPT peut également être garantie par une décision échelonnée, conformément au principe juridique **argumentum a maiore ad minus** : Une décision au sens des art. 263 ss CPP peut être rendue, obligeant dans un premier temps le détenteur des données, sous peine de l'amende pour désobéissance prévue à l'art. 292 CP, à fournir des renseignements, à conserver les données et à en garantir la confidentialité, afin que les données pertinentes pour l'enquête puissent être versées au dossier dans un deuxième temps. Une telle obligation progressive n'est pas contraire au principe du numerus clausus en matière de mesures de contrainte (art. 197 al. 1 let. a CPP), car la première obligation de conserver les données a déjà pour but d'exiger ultérieurement les données pertinentes pour la preuve conformément à l'art. 263 CPP. Une telle obligation progressive porte moins atteinte aux droits du détenteur des données qu'une ordonnance de perquisition au sens des art. 246 ss CPP ou une injonction de produire au sens de l'art. 265 CPP. Le délai de conservation maximal de 90 jours prévu à l'art. 16, al. 2, CCC doit être respecté afin que la mesure ne dépasse pas le texte de la convention. 25

D. Saisie bloquée par le Tribunal fédéral malgré une demande de mise sous scellés valable

26 Ces dernières années, le Tribunal fédéral a dû se prononcer à plusieurs reprises sur le cas de figure suivant : après la saisie d'appareils électroniques, une copie de sauvegarde (copie miroir) des données qui s'y trouvaient a été effectuée par les autorités d'instruction ou par un service spécialisé mandaté, malgré la mise sous scellés. Le Tribunal fédéral estime qu'il est inadmissible qu'après une demande de scellés, une autorité d'instruction ordonne la copie des données ou la transmette à une personne ou à une autorité mandatée et liée par ses instructions. Au contraire, après avoir scellé les supports de données, l'autorité chargée de l'enquête doit présenter une demande de miroir au tribunal des mesures de contrainte, même si un miroir est absolument nécessaire pour protéger les données contre toute perte. La demande peut être présentée en même temps que la demande de descellage ou, en cas d'urgence, à titre superprovisoire. Après la mise sous scellés, seule la juridiction des mesures de contrainte est compétente pour ordonner une copie.

27 Cette jurisprudence a été critiquée à juste titre. Elle s'avère également contraire au droit international au regard de la Convention sur la cybercriminalité. Le Tribunal fédéral ignore ainsi que la Suisse s'est engagée à garantir la sauvegarde immédiate des données informatiques pertinentes pour la preuve dans les procédures nationales afin d'éviter toute perte de preuves. Par sa jurisprudence, le Tribunal fédéral introduit non seulement une procédure superprovisoire jusqu'alors inconnue devant le tribunal des mesures de contrainte, mais aussi une procédure dans laquelle, même en cas d'ordonnance rendue par un juge des mesures de contrainte, la collecte de données pertinentes pour la preuve peut être considérablement compromise en l'espace de quelques heures : Tant que l'autorité d'instruction ne peut pas faire ou faire faire une copie des données lors d'une perquisition sur place et doit s'adresser au tribunal des mesures de contrainte et attendre sa décision, il existe dans la pratique actuelle un risque considérable que des personnes autorisées à accéder aux données stockées sur des serveurs numériques ou dans le cloud les modifient ou les suppriment avant que le tribunal des mesures de contrainte ne se prononce sur la décision de mise en miroir . De nouvelles évolutions offrent également une protection accrue contre les accès des autorités, à condition de réagir immédiatement. Récemment, l'une des

plus grandes entreprises technologiques a introduit sur ses appareils (mobiles) une fonction de sécurité qui bloque le port USB 60 minutes après le dernier déverrouillage de l'appareil, avec pour conséquence que les données ne peuvent plus être lues à partir de ce moment-là et qu'aucun logiciel permettant une lecture ultérieure ne peut être installé sur l'appareil. Il faut s'attendre à ce que d'autres entreprises suivent cet exemple. Par conséquent, certaines situations à risque – tant nouvelles que celles prises en compte dans le rapport explicatif – ne peuvent être évitées que par l'intervention immédiate de l'autorité d'enquête, respectivement de la police ou de la personne mandatée par celle-ci lors de la perquisition sur place. La procédure définie par le Tribunal fédéral, qui consiste à déposer une demande de miroir superprovisoire auprès du tribunal des mesures de contrainte après la mise sous scellés, augmente considérablement le risque de perte de preuves. On ne peut donc pas parler ici d'une poursuite pénale plus efficace, comme le vise la Convention sur la cybercriminalité.

BIBLIOGRAPHIE

Burgermeister Daniel, Beweiserhebung in der Cloud, Master of Advanced Studies in Forensics (MAS Forensics), August 2015.

Graf Damian K., Praxishandbuch zur Siegelung, StPO inklusive revidierter Bestimmungen – VStrR – IRSG – MStP, Bern 2022.

Graf Damian K./Günal Rütsche Serdar, Datensicherung von Mobiltelefonen und Tablets – technische und (siegelungs-)rechtliche Herausforderungen im Strafverfahren, SJZ 121 (2025), S. 604 ff.

Hansjakob Thomas, Überwachungsrecht der Schweiz, Kommentar zu Art. 269 ff. StPO und zum BÜPF, Zürich 2018.

MATÉRIAUX

Bundesamt für Justiz, Vernehmlassungsentwurf, Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, Vorentwurf und Erläuternder Bericht, Bern, März 2009, abrufbar unter https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/cybercrime-europarat.html, besucht am 4.5.2025.

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2010/813/de, besucht am 4.5.2025.

Botschaft zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz über das Jugendstrafrecht vom 21.9.1998, BBl 1999 II 1979 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1999/1_1979_1787_1669/de, besucht am 4.5.2025.

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, abrufbar unter https://rm.coe.int/16800cce5b, besucht am 4.5.2025 (zit. Explanatory Report).

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), abrufbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679, besucht am 4.5.2025.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 18 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Damian K. Graf

PROPOSITION DE CITATION

Damian K. Graf, Commentaire de l'art. 18 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Graf, art. 18 CCC N. XXX.

Titre 3 Injonction de produire

Art. 18 Injonction de produire

[1] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b. à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux art. 14 et 15.

3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;

c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

TABLE DES MATIÈRES

I. Généralités 184
II. Ordonnance de remise de données informatiques (al. 1 let. a) 186
III. Ordonnance de remise de données de connexion auprès des fournisseurs d'accès (al. 1 let. b) 188
IV. Renvoi aux art. 14 et 15 CCC (al. 2) 192
V. Définition des données de trafic (al. 3) 192
VI. Conditions préalables à la licéité de la collecte de données en vertu du droit suisse de procédure pénale 194
Bibliographie 196
Matériaux 197

I. GÉNÉRALITÉS

1 Dans la section 2 (« Droit procédural ») du chapitre 2 (« Mesures à prendre au niveau national »), l'art. 18 CCC traite, sous le titre 3 (« Ordonnance de remise »), de la **communication de données** par les autorités pénales compétentes. Il distingue deux cas de figure : d'une part, la remise de données informatiques par une personne qui se trouve sur le territoire de l'État contractant concerné (al. 1, let. a) et, d'autre part, la communication de données de répertoire par des fournisseurs de services qui offrent leurs services dans l'État contractant (al. 1, let. b). Étant donné que ces derniers n'ont pas leur siège dans l'État contractant concerné et que les données de stock ne doivent pas nécessairement y être stockées, l'art. 18 CCC contient un élément **extraterritorial** (cf. n. 9 s.).

2 La décision de rendre des données constitue la **mesure la moins contraignante** par rapport aux mesures de contrainte qui portent plus profondément atteinte aux droits des personnes concernées (souvent non inculpées). Conformément au principe de proportionnalité, la possibilité d'une décision de production doit toujours être examinée avant de recourir à des mesures de contrainte plus étendues (telles qu'une perquisition domiciliaire) (cf. également art. 265, al. 4, CPP). Un aspect essentiel de cette mise en balance des intérêts est le risque de collusion et de perte de moyens de preuve si les données ne sont pas immédiatement saisies par les membres des autorités de poursuite pénale.

3 Sur le fond, l'art. 18 CCC se limite à la remise de données **concrètement déterminées ou déterminables, déjà existantes ou enregistrées dans le cadre d'une procédure pénale**. Il ne doit pas nécessairement s'agir d'une cyberinfraction au sens des art. 2 à 11 CCC ou d'une autre infraction commise à l'aide d'un système informatique ; il suffit que les moyens de preuve disponibles sous forme électronique permettent d'établir l'existence d'une infraction quelconque (art. 14, al. 2, CCC). Cela signifie également que les éléments de preuve demandés doivent au moins être **potentiellement pertinents**, c'est-à-dire qu'ils peuvent être importants pour l'enquête pénale ou ne doivent pas apparaître manifestement inutilisables, ce qui découle déjà du principe général de proportionnalité (condition préalable à une mesure étatique « appropriée »).

En vertu du libellé de la convention (« chaque Partie prend les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes » ; cf. également art. 14, al. 1, CCC), l'art. 18 CCC n'est **pas une norme d'application directe** qui entre en vigueur dès la ratification de la convention. Il fonde plutôt une obligation de droit international de promulguer des dispositions internes correspondantes. Contrairement à l'art. 32 CCC, l'art. 18 CCC ne peut donc pas être invoqué directement comme base pour une mesure de procédure pénale. 4

Toutefois, le Conseil fédéral a déclaré dans son message que **le droit suisse satisfait déjà aux exigences de l'art. 18 CCC.** Dans cette mesure, tant le libellé de l'art. 18 CCC que les documents y relatifs – en particulier le rapport explicatif sur la CCC et la note d'orientation n° 10 du Comité de la Convention sur la cybercriminalité (« T-CY ») du Conseil de l'Europe – peuvent servir d'**aides à l'interprétation** pour l'application des dispositions nationales, en premier lieu l'art. 265 CPP. En Suisse, il est en outre de principe que les normes doivent être interprétées, dans la mesure du possible, conformément aux conventions. 5

L'art. 18 CCC ne précise pas comment les mesures doivent être mises en œuvre dans le droit interne, mais se contente de définir le contenu minimal des normes nationales en matière de compétence et laisse à chaque État partie le soin d'intégrer les exigences de la convention dans son système de mesures d'obtention des preuves. L'art. 18, al. 2, CCC renvoie toutefois aux autres garanties minimales prévues aux art. 14 et 15 CCC, qui doivent également être respectées dans ce contexte. 6

L'art. 18 CCC ne précise pas non plus si et, dans l'affirmative, dans quelle mesure les données doivent être conservées, ni ne fixe de délais de conservation. Il ne contient notamment aucune obligation pour les fournisseurs d'accès de conserver des enregistrements sur leurs abonnés, d'en garantir l'exactitude, de vérifier l'identité des utilisateurs ou d'empêcher l'utilisation de pseudonymes. De telles obligations peuvent éventuellement découler de réglementations nationales au niveau de la loi ou de l'ordonnance. 7

II. ORDONNANCE DE REMISE DE DONNÉES INFORMATIQUES (AL. 1 LET. A)

8 **En l'espèce**, la demande de remise peut porter sur des « données informatiques » qui sont définies à l'art. 1, let. b, CCC comme « toute représentation de faits, d'informations ou de concepts sous une forme appropriée pour le traitement dans un système informatique, y compris un programme susceptible de déclencher l'exécution d'une fonction par un système informatique ». Cette notion englobe **tous les types de données**, en particulier les données d'inventaire, de connexion et de contenu (cf. n. 24 ss). L'art. 18 CCC exige uniquement que les données concernées puissent être exigées, sans toutefois se prononcer sur la compétence ou la procédure interne spécifique. Pour cette raison, il est par exemple tout à fait compatible avec les art. 18 et 15 CCC que la remise de données de connexion soit soumise, en droit suisse, à des exigences plus strictes que la remise de données d'inventaire ou de contenu et qu'elle nécessite en outre l'autorisation du tribunal des mesures de contrainte (cf. n. 27 s.).

9 **Sur le plan personnel**, l'art. 18, al. 1, let. a, CCC s'applique, selon son libellé explicite, à toutes les personnes morales et physiques qui, au moment de la décision, ont leur siège, leur domicile ou même seulement leur résidence temporaire dans l'État contractant. Contrairement à l'art. 32 CCC, non pas par le lieu de stockage des données, mais **à la personne en possession ou sous le contrôle de laquelle se trouvent les données à collecter.** L'art. 18 al. 1 let. a CCC s'applique également aux **fournisseurs d'accès** domiciliés en Suisse ; ceux-ci peuvent être contraints de mettre à disposition non seulement des données de base (cf. art. 18 al. 1 let. b CCC), mais aussi des données relatives au contenu et à la connexion.

10 Le lieu de stockage des données est, en d'autres termes, sans importance dans ce contexte. Par conséquent, même **les données stockées à l'étranger** peuvent être éditées chez une personne domiciliée en Suisse, pour autant que ces données « se trouvent en sa possession ou sous son contrôle » (« computer data in that person's possession or control »). L'art. 18, al. 1, let. a CCC autorise donc, tout comme l'art. 32 CCC, une forme de prise de preuve extraterritoriale. Cela est conforme à la jurisprudence du Tribunal fédéral relative à l'art. 18 CCC et à l'art. 265 CPP, selon laquelle ces dispositions **permettent la mise à disposition de toutes les données auxquelles le**

destinataire de la décision a accès ou est autorisé à accéder (« avoir un pouvoir de disposition, en fait et en droit, sur ces données »).

La notion de « possession ou contrôle » renvoie, d'une part, à la **possession physique** des données concernées sur le territoire de l'État contractant qui a rendu la décision (souveraineté sur les données) et, d'autre part, à des situations dans lesquelles les données recherchées ne se trouvent pas dans la sphère de garde du destinataire de la décision, mais où celui-ci peut **librement contrôler** leur remise (droit de disposition). Cela inclut, par exemple, une personne qui a stocké des données chez un fournisseur tiers, par exemple dans un cloud – dans ce cas, le fournisseur tiers est en possession des données et l'utilisateur en a le contrôle, et les deux peuvent être tenus individuellement responsables en tant que destinataires de la disposition. La possession et le contrôle peuvent donc être dissociés. Selon le rapport explicatif, il ne suffit toutefois pas de disposer de la capacité technique d'accéder à des données stockées à distance ; les données doivent plutôt être sous le contrôle légitime (« legitimate control ») du destinataire de la disposition. Le « contrôle » présuppose donc à la fois la possibilité d'accéder à ces données et le droit de le faire. Ce point doit être clarifié dans le détail. Le destinataire de la disposition doit **contribuer à** l'administration de la preuve s'il fait valoir l'absence de contrôle ou d'accès aux informations demandées. 11

Dans les **structures de groupe**, on ne peut pas partir du principe qu'une filiale a accès aux données de la société mère ou des sociétés sœurs. À l'inverse, en raison de leur position, les sociétés mères d'un groupe sont souvent susceptibles de disposer ou de contrôler les données au sein du groupe, que ce soit de fait ou de droit. Si, pour des raisons réglementaires ou de protection des données, les données restent chez les sociétés nationales et que la société mère n'y a manifestement pas accès, les données ne peuvent être exigées que de la société nationale. Si des solutions de stockage ou d'archivage internes ou externes à l'entreprise ou des centres de données sont utilisés, le droit de contrôle reste acquis à la personne qui externalise, tandis que l'entreprise qui conserve les données en est « propriétaire », car elles se trouvent dans sa sphère de contrôle. Par conséquent, les filiales ou sociétés partenaires de fournisseurs étrangers qui stockent des données en Suisse (par exemple dans des fermes de serveurs) sont également soumises à une obligation de remise, même si elles sont domiciliées en Suisse. 12

13 Ce qui est déterminant, c'est la possibilité d'accès effective ou juridique **au moment de la décision**. Une limitation de l'accès après réception d'une demande serait non seulement abusive, mais pourrait également constituer une infraction pénale selon la situation juridique dans les États contractants (cf. art. 305 CP [faveur]).

14 Comme on l'a vu (n. 9 s.), l'art. 18, al. 1, let. a, CCC ne se réfère pas directement au lieu de stockage des données. Une décision de remise rendue en Suisse peut toutefois viser des données stockées en Suisse, que les personnes ayant droit aux données se trouvent à l'étranger ou non (par exemple lorsqu'une personne domiciliée à l'étranger stocke des données en Suisse ou exploite un centre de données). Si seules les données se trouvent en Suisse, mais pas les personnes ayant droit aux données, la seule question qui se pose est de savoir comment la demande de remise peut être transmise à la personne domiciliée à l'étranger – une question qui se pose également sous let. b (cf. n. 20 s.).

III. ORDONNANCE DE REMISE DE DONNÉES DE CONNEXION AUPRÈS DES FOURNISSEURS D'ACCÈS (AL. 1 LET. B)

15 L'art. 18, al. 1, let. b, CCC se réfère à la remise de **données de base** par des **fournisseurs de services ou « service provider »** au sens de l'art. 1, let. c, CCC, qui offrent leurs **services sur le territoire de l'État contractant**. Cet article est donc à la fois plus restrictif et plus large que la let. a, dans la mesure où il se limite aux fournisseurs de services et à la remise de données relatives à l'abonnement («subscriber information») – par exemple l'identité du client ou des informations sur les transactions financières (cf. n. 24 ss) –, mais où il vise non seulement les fournisseurs suisses, mais aussi les fournisseurs étrangers (cf. à ce sujet n. 17 s.). Le lien interne nécessaire avec la Suisse est ici compris, à l'instar de la conception du droit des cartels, au sens du **principe d'effet**, raison pour laquelle les fournisseurs de services étrangers sont également concernés s'ils sont actifs sur le marché suisse. La condition préalable reste ici aussi que les données soient **en possession ou sous le contrôle** du destinataire de la décision (cf. à ce sujet n. 11 ss).

16 Contrairement à l'art. 32 CCC, qui repose sur le volontariat et suppose, pour une remise des données conforme au droit par les fournisseurs, une

autorisation dans les conditions générales du contrat ou dans un document similaire, une demande de remise est **contraignante** et doit être exécutée par les fournisseurs de services destinataires, pour autant qu'elle soit conforme aux exigences nationales de l'État contractant dans lequel les services sont offerts et qui a rendu la décision. L'accès facilité et plus efficace aux données d'inventaire semble approprié, étant donné que 80 à 90 % des données requises au niveau international sont des données d'inventaire ; l'art. 18, al. 1, let. b CCC contribue ainsi à alléger le système d'entraide judiciaire internationale.

La question de savoir quand un service est **« offert »** dans un État contractant a déjà fait l'objet d'une jurisprudence dans d'autres contextes en Europe : il est nécessaire que les activités du fournisseur de services soient dirigées vers les utilisateurs de l'État, c'est-à-dire que le fournisseur de services ait l'intention que les utilisateurs de cet État utilisent ses services. La simple accessibilité d'un site web ou la possibilité de s'y connecter depuis un autre pays ne suffit pas à cet égard. L'utilisation d'autres langues ou devises que celles habituelles dans l'État du siège, l'utilisation de domaines de premier niveau ou d'un indicatif téléphonique d'un État peuvent constituer des indices de l'« offre » d'un service. Ainsi, la plus haute juridiction belge a estimé que Yahoo! Inc. pouvait être contrainte, sous peine de sanctions, de divulguer des données relatives à ses clients, car Yahoo! Inc. participait activement à la vie économique belge en tant que fournisseur d'un service de messagerie électronique gratuit. Cela ressortait notamment de l'utilisation du domaine « www.yahoo.be », de l'utilisation de la langue nationale, de la diffusion de publicités basées sur la localisation des utilisateurs et de la mise en place d'un formulaire de réclamation et d'une rubrique FAQ pour les utilisateurs belges. Enfin, le nouvel art. 3, point 4, du règlement (UE) 2023/1543 relatif aux ordonnances européennes de production de preuves et aux ordonnances européennes de gel de preuves électroniques en matière pénale et à l'exécution des peines privatives de liberté après une procédure pénale du 12 juillet 2023 (« règlement e-Evidence ») exige que le critère de « fourniture de services dans l'UE » cumulativement (a) la création d'une possibilité pour les personnes physiques ou morales dans un État membre de recourir aux services et (b) un lien substantiel avec cet État membre, qui est considéré comme existant, par exemple, lorsque le prestataire de services dispose d'un établissement ou d'un nombre important d'utilisateurs dans cet État membre

17

ou dans plusieurs États membres ou que son activité est orientée vers ceux-ci. De tels critères peuvent également être utilisés pour l'art. 18 CCC.

18 Si des fournisseurs étrangers proposent un service sur le marché d'un État contractant, ils sont tenus de communiquer les données relatives aux utilisateurs de ce service dans l'État contractant concerné. C'est le cas, par exemple, lorsqu'une personne s'inscrit via l'adresse « .ch » du fournisseur de services, indique la Suisse comme lieu de résidence ou de siège ou utilise une adresse IP suisse au moment de l'inscription ou à une date ultérieure.

19 Au sein des organes du Conseil de l'Europe également, l'opinion prévaut que les données de base stockées sur un système informatique **à l'étranger** peuvent être exigées d'un **fournisseur national** (pour autant qu'elles soient sous son contrôle, cf. également n. 11 ss) et que des injonctions peuvent être adressées directement à un **fournisseur étranger**. Ces deux points sont également conformes à la lettre de l'art. 18 CCC.

20 Le Tribunal fédéral s'est déjà penché sur ces deux questions et a rendu un arrêt nuancé : Dans un arrêt du 16 novembre 2016, il a estimé que l'art. 18 CCC et l'art. 265 CPP autorisent la production de toutes les données auxquelles le destinataire de la décision a effectivement et légalement accès (« avoir un pouvoir de disposition, en fait et en droit, sur ces données »), y compris celles qui sont stockées à l'étranger. Dans un arrêt du 14 janvier 2015, elle a en revanche déclaré que l'art. 18 CCC ne permettait pas de s'adresser directement à un fournisseur étranger au moyen d'une décision de production, même si celui-ci offre ses services en Suisse – l'art. 32 CCC régit donc de manière exhaustive l'accès transfrontalier direct, et l'art. 25 al. 4 phrase 1 CCC stipule que l'entraide judiciaire internationale doit suivre les instruments habituels, sauf si une disposition contraire est « expressément » prévue dans la CCC. Le Tribunal fédéral a toutefois constaté que les filiales ou sociétés partenaires de fournisseurs étrangers qui stockent des données en Suisse (telles que des fermes de serveurs) sont soumises au droit suisse. Il n'a toutefois pas examiné le libellé de l'art. 18 CCC, ni le rapport explicatif ou le message, selon lesquels le législateur partait précisément du principe que le droit national répondait aux exigences de l'art. 18 CCC. Il n'appartient pas au Tribunal fédéral de passer outre la volonté claire du législateur. En outre, il n'y a pas de violation de la souveraineté lorsque des services sont fournis en Suisse, car dans ce cas, il existe précisément un lien interne suffisant avec la Suisse. Une limitation aux prestataires de services établis en Suisse rendrait en

outre l'art. 18, al. 1, let. b, CCC obsolète, car les fournisseurs d'accès ayant leur siège en Suisse sont déjà visés par l'art. 18, al. 1, let. a, CCC (cf. n. 9) et doivent donc non seulement remettre les données relatives à l'existence, mais aussi celles relatives au contenu et à la connexion. À bien y regarder, l'art. 18, al. 1, let. b, CCC peut donc également servir de base à la pratique courante en Suisse, qui repose principalement sur l'art. 32 CCC et selon laquelle les autorités de poursuite pénale adressent **des demandes directes aux fournisseurs étrangers** («demandes d'informations»). Cela vaut également dans le sens inverse : les fournisseurs suisses qui offrent leurs services sur des marchés étrangers peuvent être directement invités à divulguer des données par les autorités étrangères et, comme ils sont en principe soumis à une obligation de divulgation, ils ne sont pas punissables en vertu de l'art. 271 CP (« Acte interdit en vue d'un État étranger ») en cas de transmission des données.

En ce qui concerne la **notification** des décisions de remise, les grands fournisseurs mettent à disposition des « portails d'application de la loi » sur lesquels les autorités pénales suisses peuvent également s'enregistrer et saisir directement leurs demandes. Pour les petits fournisseurs de services, les demandes de remise peuvent être transmises par voie policière (via Interpol) ou, si cela est accepté, directement (par exemple par courrier électronique). L'art. 18, al. 1, let. b, CCC permet de renoncer à la voie formelle de l'entraide judiciaire et autorise les États contractants à transmettre directement les ordonnances de remise aux fournisseurs d'autres États contractants. Cela est admissible et approprié, car l'exigence d'une notification de la décision de production de documents par la voie de l'entraide judiciaire réduirait à néant les facilités que l'art. 18, al. 1, let. b, CCC vise précisément à permettre. Seule la notification directe garantit que les autorités de poursuite pénale puissent accéder efficacement et rapidement aux données nécessaires sans devoir recourir à la procédure d'entraide judiciaire, souvent longue et bureaucratique. Il est toutefois un fait que l'absence de coopération ne peut être **imposée** directement, mais uniquement par la voie formelle de l'entraide judiciaire au moyen de mesures coercitives allant au-delà de l'art. 18 CCC. 21

La demande de remise étant une **mesure d'obtention de preuves interne**, ce n'est pas le droit de l'État contractant dans lequel le fournisseur est établi qui est déterminant, mais celui de l'État contractant dans lequel il offre ses services. 22

IV. RENVOI AUX ART. 14 ET 15 CCC (AL. 2)

23 Les États peuvent, dans le cadre de l'art. 15 CCC, fixer **des conditions et des garanties** et exclure des données du champ d'application de l'art. 18 CCC. Il est ainsi justifié de limiter la remise de données de connexion à certaines infractions et d'exiger à cet effet l'autorisation du juge des mesures de contrainte (art. 273 CPP). Il est en outre admissible de lier les ordres de remise à des interdictions de communication, comme cela a été mis en œuvre dans le droit suisse (art. 73, al. 2, CPP).

V. DÉFINITION DES DONNÉES DE TRAFIC (AL. 3)

24 Sont considérées comme **données de trafic** toutes les informations – qui ne sont pas qualifiées de données de connexion ou de contenu – enregistrées par un fournisseur de services en relation avec un utilisateur ou un abonné de ses services. L'objectif central de la consultation des données de trafic est de déterminer l'**identité** de l'abonné ou de l'utilisateur et d'identifier les services utilisés par l'utilisateur. En outre, des informations commerciales telles que les données de facturation et de paiement peuvent également être pertinentes, notamment dans le cadre de la cyberfraude et d'autres infractions contre le patrimoine.

25 Selon l'art. 18, al. 3, CCC, les données de base comprennent toutes les informations relatives (a) à la nature du service de communication utilisé, aux mesures techniques prises à cet effet et à la durée du service ; (b) à l'identité de l'abonné, son adresse postale ou physique, ses numéros de téléphone et autres numéros d'accès, ainsi que les informations relatives à la facturation et au paiement disponibles sur la base du contrat ou de l'accord relatif au service ; ainsi que (c) d'autres informations sur l'emplacement de l'équipement de communication disponibles sur la base du contrat ou de l'accord relatif au service. En Suisse, les informations qui peuvent être communiquées en vertu de l'art. 22, al. 1, LSCPT sont précisées aux art. 36 à 38 de l'ordonnance du 15 novembre 2017 sur la surveillance de la correspondance postale et des télécommunications (OSCPT, RS 780.11). Sont notamment considérées comme données de base les éléments d'adressage tels que l'attribution d'un nom, d'un numéro de téléphone et d'une adresse à une adresse IP connue, ainsi que les contrats originaux et les copies des pièces d'identité présentées

lors de la conclusion du contrat et les informations techniques relatives aux télécommunications.

Il convient de distinguer les données de base des **données de contenu**, qui 26
comprennent le contenu de la communication ou les fichiers enregistrés, ainsi que des données de connexion ou **données relatives au trafic**, qui sont générées en relation avec une communication et qui permettent de déterminer l'origine, la destination, l'itinéraire, l'heure, la date, l'étendue ou la durée de la communication (art. 1, let. d, CCC). Le Tribunal fédéral distingue les données de base et les données accessoires en se basant sur le critère de délimitation suivant : si les autorités de poursuite pénale connaissent déjà une connexion Internet ou une adresse électronique qu'il suffit d'attribuer à une personne concrète, il s'agit d'une consultation de données de base. Si, en revanche, les autorités de poursuite pénale ont uniquement connaissance d'activités de communication internet punissables et que les adresses IP attribuées et les clients enregistrés doivent d'abord être déterminés à partir des données marginales de connexion de la communication concernée, il s'agit alors d'une collecte rétroactive (soumise à autorisation) de données marginales au sens de l'art. 273 CPP. Selon la jurisprudence, cela s'applique également de manière générale à la demande de remise d'un historique IP. Il convient donc de distinguer s'il s'agit de savoir qui a communiqué avec qui et quand (données de connexion au sens de l'art. 273 CPP) ou plutôt qui a utilisé un service déterminé à un moment connu (données de position au sens de l'art. 22, al. 1, LSCPT). Les **adresses IP d'enregistrement** d'un compte déjà connu doivent donc être considérées sans ambiguïté comme des données de position et non comme des données de communication, car elles servent exclusivement à identifier un participant et n'ont aucun lien avec la communication ultérieure via le compte. Les autres **« données d'accès »** (par exemple l'historique des adresses IP des connexions à un service non destiné à la communication, comme la connexion à un portefeuille crypté ou à un cloud) ne peuvent pas non plus être considérées à juste titre comme des données de connexion. Ces données ne concernent ni directement ni indirectement la communication entre les personnes et sa surveillance. Dans de tels cas, les adresses IP sont plutôt comparables à des traces laissées sur le lieu d'un crime, à l'instar d'une empreinte digitale ou d'ADN, et ne constituent pas des données secondaires dans le contexte de la communication humaine, mais plutôt des données de base. La décision du Tribunal fédéral relative à la

qualification des historiques IP en tant que données de trafic au sens de l'art. 273 CPP n'est pas suffisamment nuancée à cet égard.

VI. CONDITIONS PRÉALABLES À LA LICÉITÉ DE LA COLLECTE DE DONNÉES EN VERTU DU DROIT SUISSE DE PROCÉDURE PÉNALE

27 Pour les **données de base** au sens de l'art. 18, al. 3, CCC – c'est-à-dire en particulier les informations (même rétroactives) sur l'identité de la personne qui est ou était enregistrée comme titulaire ou destinataire de la facture auprès du fournisseur de services soumis au droit suisse (cf. n. 24 ss) –, une simple consultation peut être effectuée conformément à l'art. 22 al. 1 LSCPT auprès du service de surveillance de la correspondance postale et des télécommunications (service SCPT). Ces informations peuvent également être obtenues par voie d'édition (art. 265 CPP), en particulier lorsque le fournisseur étranger qui offre ses services au sens de l'art. 18 al. 1 let. b CCC en Suisse n'est pas soumis à la LSCPT. La demande d'informations par l'intermédiaire du service SCPT constitue uniquement une règle de procédure ; ni le CPP, ni la LSCPT, ni l'ordonnance y relative ne prévoient que les informations qui ne sont pas communiquées par l'intermédiaire du service SCPT ne peuvent être utilisées. Une consultation de données d'inventaire présuppose qu'il existe un soupçon d'infraction (crime, délit ou contravention) commise via Internet (art. 22 al. 1 LSCPT), que les informations demandées sont susceptibles d'être pertinentes pour l'enquête ou d'avoir une valeur probante et que la proportionnalité est respectée. Aucun recours ordinaire n'est admissible contre une consultation de données d'inventaire ; notamment, la mise sous scellés (art. 248 CPP) n'est pas applicable, car il n'est pas possible de déterminer à l'avance dans quelle mesure les données d'inventaire demandées pourraient être soumises à une interdiction de saisie au sens de l'art. 264 CPP. Les fournisseurs sont soumis à une obligation de renseigner ; s'ils refusent, une amende d'ordre ou une amende au sens de l'art. 292 CP peut leur être infligée (pour autant qu'ils en aient été informés au préalable), ou des mesures de contrainte peuvent être prises (par analogie avec l'art. 265, al. 3 et 4, CPP). Pour les fournisseurs étrangers qui offrent leurs services en Suisse, la menace d'une sanction pénale au sens de l'art. 292 CP devrait également être admissible, mais les mesures de contrainte visant à obtenir les données relatives à l'existence d'une

communication devraient être demandées à l'État concerné dans le cadre de l'entraide judiciaire.

Pour les données relatives au contenu et à la connexion, qui peuvent toutes deux être exigées en vertu de l'art. 18, al. 1, let. a, CPP, il convient ensuite de distinguer : **les données relatives au contenu** qui peuvent être pertinentes à des fins de preuve doivent être éditées en vertu de l'art. 265 CPP, pour autant qu'elles soient stockées (« in storage ») au moment de la décision et qu'elles ne se trouvent pas encore en cours de transmission (« in traffic »). Sont pertinentes en pratique, par exemple, les données relatives au contenu des opérateurs de messagerie électronique, comme le compte de messagerie électronique d'une adresse « @bluewin.ch » chez Swisscom. La remise des données relatives au contenu est subordonnée à l'existence d'un soupçon suffisant d'une infraction pénale, à la pertinence potentielle des enregistrements remis pour la procédure pénale et au respect du principe de proportionnalité. La décision de production peut être assortie d'une interdiction de communication conformément à l'art. 73, al. 2, CPP, ce qui a pour effet que le fournisseur de services n'est pas autorisé à informer le titulaire du compte jusqu'à nouvel ordre. Les titulaires et autres personnes habilitées peuvent former un recours contre une décision de production en demandant la mise sous scellés (art. 248 CPP), pour autant qu'ils puissent faire valoir leur propre intérêt au secret. Le fournisseur dispose certes formellement du droit de demander la mise sous scellés, mais il ne peut pas le faire à la place de ses clients et il ne pourra guère invoquer ses propres interdictions de saisie au sens de l'art. 264 CPP. Pour les **données de connexion ou marginales** (cf. n. 26), le ministère public ne doit pas ordonner la production, mais rendre une décision en vertu de l'art. 273 CPP, qui est soumise à des exigences plus strictes : (1) il doit exister un soupçon grave d'un crime ou d'un délit ; (2) la gravité de l'infraction doit justifier la surveillance ; (3) les mesures d'enquête prises jusqu'alors doivent être restées infructueuses ou les investigations seraient sinon vouées à l'échec ou rendues excessivement difficiles (art. 273 al. 1 en relation avec l'art. 269 al. 1 CPP). La décision doit en outre être approuvée par le tribunal des mesures de contrainte (art. 274 CPP), faute de quoi les preuves recueillies sont absolument inutilisables (art. 277, al. 2, CPP). L'autorisation du tribunal des mesures de contrainte peut être contestée par la personne surveillée, le cas échéant également par le fournisseur d'accès, par voie de recours au sens des art. 393 ss CPP (art. 279, al. 3, CPP). 28

BIBLIOGRAPHIE

Betschmann Simon, Randdatenerhebung im Fernmeldeverkehr gemäss Art. 273 StPO, AJP 2019, S. 358 ff.

Donatsch Andreas/Lieber Viktor/Summers Sarah/Wohlers Wolfgang (Hrsg.), Schulthess Kommentar zur Schweizerischen Strafprozessordnung, 3. Aufl., Zürich 2020 (zit. SK-Bearbeiter/in, Art. ... StPO N. ...).

Graf Damian K., Corona- und Crypto-Leaks – die Strafverfolgung bewegt sich nicht im rechtsfreien Raum, Gastkommentar, NZZ vom 17.2.2023, abrufbar unter https://www.nzz.ch/meinung/was-darf-die-staatsanwaltschaft-die-corona-und-crypto-leaks-ld.1725348, besucht am 31.3.2025 (zit. Crypto-Leaks).

Graf Damian K., Kommentierung zu Art. 32 CCC, in: Graf Damian K. (Hrsg.), Onlinekommentar, Übereinkommen über die Cyberkriminalität (Cybercrime Convention), abrufbar unter https://onlinekommentar.ch/de/kommentare/ccc32, besucht am 31.3.2025 (zit. OK).

Forster Marc, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs, in: Festgabe Schweizerischer Juristentag 2015, Zürich 2015, S. 615 ff.

Hansjakob Thomas, Die Erhebung von Daten des Internetverkehrs – Bemerkungen zu BGer 6B_656/2015 vom 16.12.2016, forumpoenale 4 (2017), 252 ff. (zit. Erhebung).

Hansjakob Thomas, Überwachungsrecht der Schweiz, Kommentar zu Art. 269 ff. StPO und zum BÜPF, Zürich/Basel/Genf 2017 (zit. Überwachungsrecht).

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar zur Strafprozessordnung/Jugendstrafprozessordnung, 3. Aufl., Basel 2023 (zit. BSK-Bearbeiter/in, Art. ... StPO N. ...).

Roth Simon, Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess, Direkter Zugriff oder Rechtshilfe?, Jusletter vom 17.8.2015.

Schweingruber Sandra, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, Jusletter vom 10. November 2014.

Seger Alexander, «Grenzüberschreitender» Zugriff auf Daten im Rahmen der Budapest Konvention über Computerkriminalität, Praxisbericht zum Stand der Arbeiten des Europarats, Zeitschrift für öffentliches Recht 73 (2018), S. 71 ff.

Walder Stephan, Grenzüberschreitende Datenerhebung: Ist und Soll, Kriminalistik 8-9/2019, S. 540 ff.

MATÉRIAUX

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2010/813/de, besucht am 31.3.2025.

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27.2.2013, BBl 2013 2683 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2013/512/de, besucht am 31.3.2025.

Europarat, Cybercrime Convention Committee (T-CY), The Budapest Convention on Cybercrime: benefits and impact in practice, Strassburg, 13.7.2020, abrufbar unter https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, besucht am 31.3.2025 (zit. T-CY, Benefits).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 10, Production orders for subscriber information (Article 18 Budapest Convention), Strassburg, 28.2.2017, abrufbar unter https://rm.coe.int/16806f943e, besucht am 31.3.2025 (zit. T-CY Guidance Note # 10).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report, Strassburg, 16.9.2016, abrufbar unter https://rm.coe.int/16806a495e, besucht am 31.3.2025 (zit. T-CY, Cloud).

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, abrufbar unter https://rm.coe.int/16800cce5b, besucht am 31.3.2025 (zit. Explanatory Report).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 25 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Miro Dangubic

PROPOSITION DE CITATION

Miro Dangubic, Commentaire de l'art. 25 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité [Cybercrime Convention]

Citation abrégée: OK-Dangubic, Art. 25 CCC N. XXX.

Titre 3 Principes généraux relatifs à l'entraide

Art. 25 Principes généraux relatifs à l'entraide

[1] Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

[2] Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux art. 27 à 35.

[3] Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. L'État requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

[4] Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux art. 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

[5] Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

TABLE DES MATIÈRES

I. Introduction 202
II. Champ d'application matériel de la CCC en matière de petite entraide judiciaire 202
A. L'infraction en tant que point de rattachement 203
B. Preuves sous forme électronique comme point de rattachement 203
III. Sources juridiques dans le cadre de l'entraide judiciaire 203
A. Dispositions relatives à l'entraide judiciaire 203
B. Droit procédural subsidiaire en Suisse 204
IV. Obligation de fournir l'entraide judiciaire 204
V. Principe de l'accommodement maximal 204
VI. Formes de transmission dans le cadre de l'entraide judiciaire 205
VII. Aménagement du principe de la double incrimination 206
A. Principe de la double incrimination 206
B. Principe de la double incrimination dans le champ d'application de la CCC 206
VIII. Rupture de la réserve fiscale 207
IX. Mandat législatif aux États parties 207
A. Généralités 207
B. Mise en œuvre en Suisse 208
Bibliographie 208
Matériaux 209

I. INTRODUCTION

1 L'article 25 de la CCC regroupe sous la rubrique "Principes généraux de l'entraide judiciaire" différentes règles relatives à la petite entraide judiciaire dans le domaine d'application de la CCC. En particulier, l'article contient des dispositions concernant

- le champ d'application matériel de la CCC (al. 1),
- les sources de droit pertinentes dans la procédure d'entraide judiciaire (al. 4),
- l'obligation de fournir une entraide judiciaire mineure (al. 1),
- le principe de l'accommodement maximal (al. 1),
- les formes de transmission possibles dans le cadre de l'entraide judiciaire (al. 3),
- l'aménagement du principe de la double incrimination (al. 5) et
- la rupture de la réserve fiscale (al. 4).

2 En outre, l'art. 25 al. 2 CCC contient un mandat législatif pour les Etats parties.

3 La CCC doit compléter les traités et conventions bilatéraux ou multilatéraux existant entre les parties contractantes (en particulier la CEEJ) et accélérer et simplifier ainsi les procédures d'entraide judiciaire. Le fait qu'il s'agisse d'une convention complémentaire a un impact important sur le contenu et la densité de la réglementation relative à la petite entraide judiciaire.

II. CHAMP D'APPLICATION MATÉRIEL DE LA CCC EN MATIÈRE DE PETITE ENTRAIDE JUDICIAIRE

4 Le champ d'application matériel de la CCC pour la petite entraide judiciaire est régi par l'article 25 al. 1 CCC et comporte deux points de rattachement alternatifs : D'une part, il est possible de se rattacher à l'infraction faisant l'objet de l'enquête ("infractions relatives aux systèmes et données informatiques") et, d'autre part, aux preuves à recueillir ("preuves sous forme électronique").

A. L'infraction en tant que point de rattachement

Le champ d'application matériel s'applique d'une part s'il existe un soupçon qu'une infraction décrite aux articles 2 à 11 de la CCC a été commise. D'autre part, le champ d'application matériel s'applique aux infractions commises au moyen d'un système informatique, indépendamment de l'infraction concrètement commise. L'article 1 let. a de la CCC définit le "système informatique" comme "un dispositif ou un ensemble de dispositifs interconnectés ou liés entre eux qui, seuls ou à plusieurs, effectuent un traitement automatisé de données sur la base d'un programme". 5

Lors de l'examen prima facie de ce champ d'application matériel par les autorités d'entraide judiciaire, il convient notamment de tenir compte des éléments suivants : Certains éléments du champ d'application matériel font en principe partie des faits juridiquement pertinents qu'il s'agit d'élucider dans le cadre de l'enquête pénale étrangère ; dans certaines circonstances, les mesures d'instruction demandées visent précisément à clarifier ces points. Il n'y a donc pas lieu de poser des exigences élevées à la description de ces éléments de fait. 6

B. Preuves sous forme électronique comme point de rattachement

S'il s'agit, dans le cadre de l'entraide judiciaire en matière pénale, de recueillir des preuves présumées sous forme électronique, le champ d'application matériel de la CCC s'applique indépendamment du délit sur lequel porte l'enquête. Les preuves sous forme électronique peuvent notamment être des données. 7

III. SOURCES JURIDIQUES DANS LE CADRE DE L'ENTRAIDE JUDICIAIRE

A. Dispositions relatives à l'entraide judiciaire

Les procédures d'entraide judiciaire dans le domaine d'application de la CCC sont régies en premier lieu par les traités internationaux pertinents et par la CCC. Dans la mesure où ces traités internationaux ne règlent pas certaines questions de manière explicite ou implicite, les dispositions nationales 8

s'appliquent (art. 25 al. 4 CCC). En Suisse, l'EIMP et l'OEIMP sont déterminants pour l'entraide judiciaire en matière pénale (art. 1 al. 1 EIMP). Le principe de faveur - également ancré dans l'art. 25 al. 1 CCC - signifie que les dispositions nationales s'appliquent même si elles posent des exigences moindres en matière d'entraide judiciaire. Par conséquent, les dispositions de la CCC ne s'appliquent dans les procédures d'entraide judiciaire que si elles représentent la norme la plus favorable à l'entraide judiciaire du point de vue de l'État requérant.

B. Droit procédural subsidiaire en Suisse

9 Si les dispositions relatives à l'entraide judiciaire manquent de règles procédurales pertinentes, le CPP et la PA s'appliquent par analogie dans les procédures d'entraide judiciaire en Suisse. Le CPP est déterminant dans les procédures d'entraide judiciaire lorsque l'EIMP y renvoie directement ou en relation avec des actes de procédure pénale au sens des art. 63 ss. EIMP. Dans les autres cas, la PA sert de droit de procédure subsidiaire.

IV. OBLIGATION DE FOURNIR L'ENTRAIDE JUDICIAIRE

10 Sur la base de l'art. 25 al. 1 CCC, l'Etat requis est tenu, si toutes les conditions d'entraide sont remplies, de fournir une entraide judiciaire de faible montant lorsqu'il est sollicité par une Partie contractante. Cette obligation n'a toutefois pas pour effet de conférer à l'État requérant la qualité de partie ou de lui permettre de faire appel dans le cadre de la procédure d'entraide judiciaire. Les éventuelles divergences de vues entre États sur la question de savoir si les conditions de l'entraide judiciaire en matière pénale sont remplies et si l'entraide doit être accordée sont résolues au niveau diplomatique.

11 L'entraide judiciaire extra-conventionnelle en matière pénale ne donne pas droit à la coopération interétatique en matière pénale (cf. art. 1 al. 4 EIMP).

V. PRINCIPE DE L'ACCOMMODEMENT MAXIMAL

12 L'art. 25 al. 1 CCC oblige l'État requis à donner suite aux demandes d'entraide judiciaire relevant du champ d'application de la CCC "dans la plus large mesure possible" (principe dit de l'accommodement maximal).

Le principe de l'accommodement maximal est un principe généralement reconnu de l'entraide judiciaire en matière pénale, qui n'a pas seulement un caractère programmatique. Le principe comprend le principe de faveur mentionné ci-dessus. Dans la pratique locale, le principe de faveur s'applique à toutes les procédures d'entraide judiciaire - même s'il n'existe pas d'obligation conventionnelle à cet égard. Il signifie que le droit national ne peut pas rendre l'entraide judiciaire en matière pénale plus difficile que le droit conventionnel prioritaire, mais qu'il peut la faciliter. 13

Le principe de l'accommodement maximal se réfère en outre à l'étendue de l'entraide judiciaire à fournir. Il permet d'interpréter généreusement les mesures demandées dans une demande d'entraide et de remettre à l'autorité requérante tous les moyens de preuve potentiellement importants pour la procédure pénale étrangère - même si l'autorité requérante n'en a pas fait explicitement la demande. 14

VI. FORMES DE TRANSMISSION DANS LE CADRE DE L'ENTRAIDE JUDICIAIRE

Conformément à l'EIMP, les demandes d'entraide judiciaire adressées à la Suisse doivent en principe être adressées à l'Office fédéral de la justice sous forme de lettre écrite. En revanche, plusieurs traités européens autorisent également la communication directe entre les organes judiciaires compétents (en général les ministères publics) ainsi que des alternatives à la forme écrite de la lettre. 15

Dans le champ d'application du CCC, l'art. 25 al. 3 CCC autorise, en cas d'urgence, l'utilisation de "moyens de communication rapides, y compris la télécopie ou le courrier électronique". Cela ne s'applique pas seulement à l'établissement de demandes d'entraide judiciaire, mais à l'ensemble des échanges d'entraide judiciaire. Le sens et le but de cette disposition est d'accélérer la procédure d'entraide judiciaire et de permettre en particulier une conservation rapide des preuves afin d'éviter le risque de perte de celles-ci. Sur demande explicite de l'État requis, une demande d'entraide judiciaire doit être présentée par écrit. 16

Il y a urgence lorsque la transmission par écrit risque d'entraîner une perte de preuves. C'est notamment le cas lorsqu'il s'agit de collecter des données dans le cadre de l'entraide judiciaire. 17

18 Il n'existe pas de numerus clausus concernant les moyens de communication qui peuvent être utilisés. Dans la pratique, on utilise notamment le courrier électronique, la télécopie et les plateformes de partage de fichiers étatiques. Les demandes d'entraide judiciaire peuvent toutefois aussi être faites par téléphone.

19 Les normes de sécurité et d'authentification déterminantes découlent des ordres juridiques nationaux ou des directives et de la pratique des autorités correspondantes.

VII. AMÉNAGEMENT DU PRINCIPE DE LA DOUBLE INCRIMINATION

20 L'art. 25 al. 5 CCC règle l'aménagement du principe de la double incrimination.

A. Principe de la double incrimination

21 Le principe de la double incrimination est un principe classique de la coopération internationale. Il signifie que l'entraide judiciaire en matière pénale n'est accordée que pour des infractions qui sont punies à la fois par le droit de l'État requérant et par le droit de l'État requis. Le principe de la double incrimination fait partie de l'ordre public en Suisse et a été garanti dans tous les traités bilatéraux et (avec des réserves) dans les conventions multilatérales d'entraide judiciaire - y compris pour le champ d'application de la CCC.

B. Principe de la double incrimination dans le champ d'application de la CCC

22 Si, dans le cadre de la procédure d'entraide judiciaire, des mesures nécessitant une contrainte procédurale doivent être appliquées, le principe de la double incrimination s'applique dans le champ d'application de la CCC. Il existe toutefois des exceptions à ce principe.

23 Selon les principes généraux, la punissabilité selon le droit de l'État requérant - même dans le champ d'application de la CCC - ne doit en principe pas être examinée dans la procédure d'entraide judiciaire locale, sous réserve des cas d'abus manifestes.

En ce qui concerne la question de la double incrimination selon le droit suisse, l'autorité d'exécution examine si l'ensemble des faits reproduits dans la demande d'entraide judiciaire peut à première vue être subsumé sous une norme pénale suisse. L'art. 25 al. 5 CCC stipule d'une part qu'il suffit que les faits décrits dans la demande d'entraide judiciaire puissent être subsumés sous une seule infraction du droit suisse - il n'est pas nécessaire d'examiner plus avant si d'autres éléments constitutifs de l'infraction pourraient être remplis en plus. D'autre part, elle stipule que la double incrimination ne présuppose pas des normes pénales identiques dans l'Etat requérant et dans l'Etat requis. Le contenu réglementaire de l'al. 5 correspond donc déjà à la pratique en vigueur en Suisse. 24

VIII. RUPTURE DE LA RÉSERVE FISCALE

Traditionnellement, de nombreuses sources de droit - tant nationales qu'internationales - contiennent ce que l'on appelle une réserve fiscale. Par exemple, l'art. 3 al. 3 EIMP stipule que l'entraide judiciaire accessoire est également exclue en principe dans les procédures pour réduction de taxes fiscales. 25

La deuxième phrase de l'art. 25 al. 4 CCC doit garantir que d'éventuelles réserves fiscales ne fassent pas obstacle à l'entraide judiciaire dans le domaine d'application de la CCC, si des infractions au sens des art. 2 à 11 CCC font l'objet d'une enquête. Comme les infractions décrites aux articles 2 à 11 de la CCC ne sont pas des infractions fiscales, la pertinence pratique de cette disposition devrait être plutôt faible. On pourrait tout au plus penser à des constellations de concours idéal : l'auteur commet, par un seul acte ou par un acte unique et cohérent, à la fois une infraction fiscale non susceptible d'entraide judiciaire et une infraction au sens des articles 2 à 11 CCC. Dans ce cas, la réserve fiscale serait toujours rompue. 26

IX. MANDAT LÉGISLATIF AUX ÉTATS PARTIES

A. Généralités

L'art. 25 al. 2 de la CCC oblige les États parties à s'assurer, lors de l'élaboration de leur ordre juridique national, qu'il existe des instruments nationaux permettant de mettre en œuvre les dispositions des art. 27 à 35 de la CCC. 27

Cette norme constitue donc en premier lieu un mandat législatif de droit international.

28 L'obligation s'adresse en principe au pouvoir législatif et présuppose une action active de l'État partie - si le droit national ne satisfait pas (encore) aux prescriptions. Les États parties qui disposent déjà des instruments juridiques nécessaires n'ont pas besoin de légiférer.

B. Mise en œuvre en Suisse

29 Les dispositions des articles 27 à 35 de la CCC doivent être qualifiées de self-executing selon la compréhension locale. En ce qui concerne leur applicabilité et leur mise en œuvre au niveau national, le législateur a estimé qu'il était nécessaire d'agir uniquement en ce qui concerne les articles 30 et 33 de la CCC.

30 Afin de mettre en œuvre l'art. 30 CCC (Transmission immédiate de données de trafic sécurisées) et l'art. 33 CCC (Entraide judiciaire pour la collecte de données de trafic en temps réel), l'art. 18b EIMP a été introduit dans la loi par l'arrêté fédéral du 18 mars 2011 avec la mention marginale "Données électroniques".

BIBLIOGRAPHIE

Böhi Simon, Kommentierung zu Art. 18*b* IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Dangubic Miro, Parteistellung und Parteirechte bei der rechtshilfeweisen Herausgabe von Kontoinformationen, forumpoenale 2018, S. 112–117.

Dangubic Miro/Clerc Yves, Art. 80dbis – ein Überblick, forumpoenale 2022, S. 287–292.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, Internationale Rechtshilfe, 2. Aufl., Zürich et al. 2015.

Donatsch Andreas/Godenzi Gunhild/Tag Brigitte, Strafrecht I, Verbrechenslehre, 10. Aufl., Zürich 2022.

Garré Roy, Kommentierung zu Art. 35 IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Graf Damian K., in: Ackermann Jürg-Beat (Hrsg.), Wirtschaftsstrafrecht der Schweiz, Hand- und Studienbuch, 2. Aufl., Bern 2021.

Graf Damian K., Kommentierung zu Art. 32 CCC, in: Graf Damian K. (Hrsg.), Onlinekommentar, Übereinkommen über die Cyberkriminalität (Cybercrime Convention), abrufbar unter https://onlinekommentar.ch/de/kommentare/ccc32, besucht am 21.11.2023.

Heimgartner Stefan, Kommentierung zu Art. 64 IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Heimgartner Stefan/Niggli Marcel Alexander, Kommentierung zu Einführung IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Kocher Martin, Kommentierung zu Art. 3 IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Popp Peter, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel et al. 2001.

MATÉRIAUX

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2010/4697.pdf, besucht am 21.10.2023 (zit. Botschaft 2010).

Explanatory Report to the Convention on Cybercrime, European Treaty Series – No. 185, Budapest, 23.XI.2001, abrufbar unter https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b, besucht am 21.10.2023 (zit. Explanatory Report).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 27 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Jan Reinhardt

PROPOSITION DE CITATION

Jan Reinhardt, Commentaire de l'art. 27 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Reinhardt, art. 27 CCC N. XXX.

Titre 4

Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Art. 27 Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

[1] En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des par. 2 à 9 du présent

article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2 a. Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;

b. Les autorités centrales communiquent directement les unes avec les autres;

c. Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;

d. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4 Outre les conditions ou les motifs de refus prévus à l'art. 25, par. 4, l'entraide peut être refusée par la Partie requise:

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b. si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités

6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.

7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9 a. En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.

b. Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).

c. Lorsqu'une demande a été formulée en application de le let. a du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité

d. Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

e. Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des

raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

TABLE DES MATIÈRES

I. Généralités 216
II. Rapport avec d'autres dispositions 216
III. Prescriptions en matière d'entraide judiciaire 218
A. Création d'autorités (al. 2) 218
B. Prescriptions relatives aux modalités d'exécution (al. 3) 219
C. Objections à l'exécution 221
1. Motifs supplémentaires de refus (al. 4) 221
2. Report de l'entraide judiciaire (al. 5) 222
3. Condition comme condition minimale pour le refus et le report (al. 6) 223
D. Obligation d'informer (al. 7) 223
E. Confidentialité (al. 8) 224
F. « Procédure accélérée » (al. 9) 226
IV. Protection juridique 227
Bibliographie 228
Matériaux 229

I. GÉNÉRALITÉS

1 L'art. 27 CCC complète le principe général de l'entraide juridique prévu à l'art. 25, al. 1, CCC et garantit un **cadre institutionnel minimal** pour l'entraide juridique mineure. Cette disposition évite que deux parties contractantes doivent recourir à l'entraide juridique non conventionnelle et sert ainsi le principe de l'efficacité prévu à l'art. 25, al. 1, CCC.

2 Outre l'obligation de désigner certaines autorités, la norme contient une **obligation plus détaillée d'exécuter les demandes d'entraide judiciaire**. En ce sens, elle est auto-exécutable selon la conception moniste suisse. Toutefois, comme dans le cas de l'entraide judiciaire non conventionnelle selon l'EIMP, les mesures individuelles faisant l'objet de la demande doivent trouver leur fondement dans le droit procédural national. Il découle en outre de l'art. 25, al. 2, CCC que les États contractants doivent adapter leur ordre juridique de manière à ce qu'il ne s'oppose pas à la procédure prévue aux articles de la section. Cela n'a pas été jugé nécessaire au regard de l'art. 27 CCC.

II. RAPPORT AVEC D'AUTRES DISPOSITIONS

3 L'art. 27 CCC définit uniquement une procédure pour les demandes d'entraide judiciaire. La condition préalable est l'ouverture du champ d'application défini à l'art. 25, al. 1. Celui-ci comprend toutes les procédures en rapport avec les systèmes et les données informatiques ainsi que la collecte de preuves sous forme électronique, y compris pour d'autres infractions. Ce dernier point crée justement un **large champ d'application**. Le deuxième protocole additionnel à la CCC contient plusieurs renvois partiels à l'art. 27 CCC, à savoir à l'art. 3, al. 2, let. a, à l'art. 7, al. 5, let. a, à l'art. 8, al. 8, à l'art. 10, al. 7, et à l'art. 11, al. 2, let. b. La Suisse n'a toutefois ni signé ni ratifié ce protocole additionnel à ce jour.

4 L'art. 25 CCC régit, outre le champ d'application, les principes de l'entraide judiciaire selon la CCC. Ses al. 2 et 4 renvoient en priorité aux dispositions de la CCC et, à titre subsidiaire, au droit national, en Suisse principalement à l'EIMP, puis à la PA et au CPP. L'art. 27 CCC a donc, du point de vue de la CCC, **prééminence sur les normes du droit national** dans son champ d'application. La question de savoir dans quelle mesure cette prééminence

existe également du point de vue du droit national relève du droit national. Pour la Suisse, on peut partir du principe que l'art. 27 CCC a la prééminence. Compte tenu des dispositions très fondamentales et principalement organisationnelles de l'art. 27 CCC, il n'y a guère lieu de s'attendre à des conflits entre cette disposition et le droit national. Elle crée plutôt une norme minimale qui ne s'oppose pas à une réglementation détaillée et plus étendue du droit national.

L'art. 27, al. 1, phrases 1 et 2, CCC stipule, conformément au titre du quatrième titre – « Procédure pour les demandes d'entraide judiciaire **sans convention internationale applicable** » que les dispositions de cet article ne sont applicables à chaque demande d'entraide judiciaire que si, dans les relations entre l'État requérant et l'État requis, il n'existe pas de convention (bilatérale) d'entraide judiciaire ou d'accord (multilatéral) en vigueur ou si, malgré l'existence d'une convention d'entraide judiciaire, les parties conviennent d'appliquer l'article 27 CCC en tout ou en partie. Au-delà de la lettre, un autre accord limité à un domaine partiel concret ne saurait suffire. Il s'agit plutôt d'un accord général d'entraide judiciaire qui garantit également l'entraide judiciaire contractuelle (restreinte) dans le champ d'application de l'art. 25, al. 1, CCC. Si un tel contrat existe, l'art. 27 CCC n'est pas applicable, même partiellement, par exemple en ce qui concerne les motifs supplémentaires de refus prévus à l'art. 27, al. 4 CCC, sous réserve d'un accord entre les parties contractantes. Cela montre clairement que l'art. 27 CCC ne fait que normaliser une norme minimale qui ne s'oppose pas à une **obligation plus étendue des États contractants dans d'autres accords**. Il ne s'agit pas d'une disposition essentielle de la CCC comme l'art. 25 al. 4, phrase 2 CCC ou l'art. 29 CCC, qui ne sont pas flexibles selon la systématique de la convention. 5

Le champ d'application effectif de l'art. 27 CCC est limité pour la Suisse comme pour de nombreux autres États contractants. Il est tout d'abord considérablement restreint par la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959. Celle-ci prévoit une réglementation complète et exclusive entre les États membres signataires du Conseil de l'Europe. À cela s'ajoutent des traités bilatéraux d'entraide judiciaire conclus par la Suisse, notamment avec les États-Unis d'Amérique, le Canada ou le Pérou. Ces traités régissent de manière exhaustive l'entraide judiciaire en matière pénale et ne prévoient pas l'application complémentaire de l'art. 27 CCC, de sorte que celui-ci n'est pas applicable. Cette 6

réglementation est applicable pour la Suisse **principalement dans ses relations avec de nombreux États africains et latino-américains ainsi qu'entre la Suisse et le Japon**. Les États sans convention applicable ou accord bilatéral sont les suivants (état au 12 avril 2025) : Argentine, Bénin, Brésil, Cap-Vert, Costa Rica, Côte d'Ivoire, République dominicaine, Îles Fidji, Ghana, Grenade, Japon, Cameroun, Kiribati, Colombie, Maroc, Maurice, Nigéria, Panama, Sénégal, Sierra Leone, Sri Lanka, Tonga et Tunisie. Enfin, la procédure prévue par la CCC devrait également s'appliquer à l'égard du Paraguay. À cet égard, il n'existe qu'un traité d'extradition, mais pas de traité global en matière d'entraide judiciaire mineure. En ce qui concerne l'obtention et la conservation des preuves, seuls les art. 16 et 17 du traité contiennent des dispositions relatives à l'audition des témoins. En outre, le champ d'application du traité d'extradition, défini à l'art. 2, auquel les autres articles se réfèrent, est limité à certaines infractions énumérées. La liste comprend, par exemple sous la forme de la fraude visée à l'art. 2, ch. 18, du traité, une part éventuellement minime des infractions punissables en vertu des art. 2 ss CCC, ce qui n'est guère surprenant compte tenu de la date de conclusion du traité en 1906. L'art. 27 CCC devrait également s'appliquer dans les relations entre la Suisse et le Rwanda. Les art. 13 et 14 du traité d'extradition entre la Suisse et la Belgique, qui restent applicables à cet égard, ne contiennent que des dispositions rudimentaires sur l'entraide judiciaire mineure par voie diplomatique. L'objectif de l'art. 27 CCC, qui est de garantir une norme minimale effective dans son champ d'application, exige également l'application des dispositions plus étendues de cet article.

7 Les conflits de normes au sein de la CCC devraient être résolus selon les principes généraux d'interprétation, en particulier selon le principe de la *lex specialis*.

III. PRESCRIPTIONS EN MATIÈRE D'ENTRAIDE JUDICIAIRE

A. Création d'autorités (al. 2)

8 La communication habituelle dans le domaine de l'entraide judiciaire par l'intermédiaire d'autorités centrales vise à fournir à la partie requérante un **interlocuteur central** et à accélérer ainsi les poursuites pénales internationales, ce qui est particulièrement important en matière de cybercriminalité. Dans le même temps, il convient de garantir l'égalité de

traitement des demandes entrantes et sortantes. La communication par l'intermédiaire d'autorités centrales évite le recours à des canaux diplomatiques, qui serait autrement nécessaire dans le cadre de l'entraide judiciaire non conventionnelle et qui serait inefficace.

Le Conseil fédéral a désigné l'**Office fédéral de la justice** comme autorité compétente. Il n'y a donc pas de dérogation à l'art. 27, al. 2, EIMP pour les demandes d'entraide judiciaire fondées sur la CCC. La liste actuelle des autorités compétentes de tous les États contractants peut être consultée en anglais sur le site Internet du Conseil de l'Europe. 9

B. Prescriptions relatives aux modalités d'exécution (al. 3)

L'al. 3 correspond dans une large mesure à l'art. 65 EIMP et aux dispositions des traités bilatéraux d'entraide judiciaire. Cette disposition vise à garantir que les éléments de preuve obtenus dans le cadre de l'entraide judiciaire puissent être utilisés dans la procédure pénale de l'État requérant. Le droit de procédure pénale des différents États contractants diffère parfois considérablement en ce qui concerne les exigences relatives à l'obtention des preuves. On citera à titre d'exemple l'exigence générale d'assermentation des témoignages, cf. également l'art. 65, al. 1, let. a, EIMP. Si l'Etat requis, qui ne connaît pas une telle exigence, se fondait exclusivement sur son propre droit procédural, les éléments de preuve risqueraient d'être **inutilisables dans l'Etat requérant** et l'entraide judiciaire manquerait son but. En effet, l'État requis applique régulièrement son propre droit de procédure pénale, cf. art. 12 et art. 63 al. 1 EIMP. 10

Le principe de l'entraide judiciaire effective n'est toutefois pas garanti de manière absolue. Au contraire, l'exécution dans la procédure désignée par l'État requérant est soumise à la réserve de la **compatibilité avec le droit de l'État requis**, cf. également art. 65 al. 2 EIMP. Celui-ci peut donc – sans préjudice de la possibilité éventuelle de refuser l'entraide judiciaire dans son ensemble – appliquer son propre droit procédural dans la mesure où la procédure prescrite par l'État requérant est incompatible avec son droit national. Compte tenu du libellé des versions anglaise (« except where ») et française (« sauf lorsqu'elle ») ainsi que de l'objectif visé par la dérogation, celle-ci ne devrait toujours s'appliquer qu'à des prescriptions individuelles. L'État requis ne peut donc pas appliquer globalement sa procédure nationale au motif qu'une seule prescription est incompatible avec son droit. 11

Conformément au libellé précité, au principe de l'art. 25, al. 1, CCC et à l'esprit de l'art. 27, al. 6, CCC, il serait même approprié de réduire autant que possible la prescription incompatible à ce qui est encore compatible et de maximiser ainsi la probabilité que les éléments de preuve puissent être utilisés dans l'État requérant. Une solution pratique consiste à consulter les autorités compétentes au sens de l'al. 2.

12 Il est très important de distinguer entre une exécution **incompatible avec** le droit national et une exécution **simplement non prévue** par celui-ci, car le refus ne peut être fondé uniquement sur ce dernier fait. Les dispositions de rang constitutionnel, telles que celles relatives à la laïcité en matière d'exigences religieuses en matière d'assermentation, justifient en tout état de cause un refus. À l'inverse, la simple existence d'une réglementation différente dans le droit national simple ne suffit naturellement pas. Il convient de distinguer, par interprétation au cas par cas, les normes de droit simple qui s'opposent expressément à la mesure d'exécution concrète. Le facteur déterminant devrait être la question de savoir si la formalité exigée constitue une atteinte supplémentaire essentielle aux droits individuels pour laquelle il n'existe pas de base légale.

13 L'intention des États contractants semble correspondre à une application plus restrictive de l'al. 3 par rapport à l'art. 65, al. 2, EIMP. Cela ressort également du fait que le critère supplémentaire et large du préjudice important n'est pas contenu dans la CCC. En outre, l'art. 25 CCC prévoit également un régime d'entraide judiciaire plus strict pour le domaine particulièrement internationalisé de la cybercriminalité.

14 En même temps, la comparaison avec l'al. 4 let. a montre que la réduction à une simple réserve d'*ordre public* pour le pouvoir de refus limité selon l'al. 3 n'est pas voulue. La réserve doit donc être classée entre la disposition large de l'art. 65, al. 2, EIMP et un principe de *l'ordre public* pur, tel qu'il figure par exemple à l'art. 73, al. 1, de la loi allemande sur l'entraide judiciaire (IRG). En conséquence, une demande peut et doit être rejetée si son exécution implique **des atteintes importantes aux droits individuels** sans base légale et contraires à la pesée des intérêts effectuée par le législateur.

15 Dans la mesure où le droit procédural national impose **des exigences supplémentaires** à la mesure à exécuter, celles-ci doivent en principe être

respectées par les autorités exécutantes de l'État requis, cf. également art. 12, al. 1, EIMP.

C. Objections à l'exécution

1. Motifs supplémentaires de refus (al. 4)

Dans la procédure prévue à l'art. 27 CCC, c'est d'abord l'art. 25, al. 4, CCC qui s'applique. Le renvoi aux motifs de refus prévus par le droit national ou par un traité d'entraide applicable s'applique donc également à cet égard, le refus étant irrecevable *au seul* titre de la qualification d'infraction fiscale. L'art. 27, al. 4, CCC renvoie à l'art. 25, al. 4, CCC et prévoit deux motifs de refus supplémentaires : la poursuite d'**infractions politiques** et le *principe de l'ordre public***.** L'État requis peut donc invoquer ces motifs de refus même si son droit interne ne les prévoit pas. En cas d'application d'un accord international, l'art. 27 CCC n'est toutefois pas applicable en vertu de son al. 1. 16

Au regard de la systématique de la CCC, selon laquelle les motifs de refus prévus par le droit national s'appliquent régulièrement en cas d'application de l'art. 27 CCC, la valeur ajoutée pratique des motifs de refus supplémentaires n'apparaît pas clairement à première vue. Un État qui ne prévoit pas ces restrictions dans son droit national ne s'en prévaudra généralement pas non plus dans la procédure prévue par la CCC, car le refus au sens de l'al. 4 relève du pouvoir d'appréciation de l'État requis. L'importance devrait découler du fait que les États, en application du principe de l'entraide judiciaire la plus large possible, ont convenu de ne faire usage des motifs de refus prévus par le droit national qui ne sont pas mentionnés à l'al. 4 que dans des cas exceptionnels dans le champ d'application de la CCC. Dans ce contexte, l'al. 4 a un **effet clarificateur et symbolique**. La réglementation montre que les motifs de refus mentionnés restent valables en tant que reflet de la conception nationale du monde. L'accord sur la non-application d'autres motifs de refus dans les cas généraux devrait toutefois être principalement contraignant sur le plan politique, notamment parce qu'il n'a pas été repris dans le texte de la convention. 17

Pour la Suisse, outre l'EIMP, il pourrait tout au plus exister un **domaine d'application restreint** pour les motifs de déni supplémentaires en application directe de l'al. 4. En cas d'infractions politiques, le motif de déni prévu à l'art. 3, al. 1, EIMP s'applique. Il y a lieu de partir du principe que l'art. 18

27, al. 4, let. a, CCC englobe aussi bien les infractions politiques absolues que relatives. Compte tenu de la réglementation restrictive de la CCC, qui renvoie largement au droit national, et de la qualification subjective et divergente d'un acte comme politique ou non politique selon les États, il convient de s'abstenir de toute interprétation autonome. Il appartient plutôt à l'État requis de déterminer le motif de refus, sous réserve d'un abus de droit. En cas d'exclusion au sens de l'art. 3 al. 2 EIMP, il ne faut pas non plus s'attendre à un refus au titre de l'art. 27 al. 4 let. a CCC.

19 La réserve *d'ordre public* est partiellement exprimée à l'art. 2 EIMP. En tant que principe général du droit international et compte tenu de l'interprétation conforme à la Constitution de l'EIMP, en particulier de la clause générale de l'art. 2 let. d EIMP, il convient par ailleurs de partir du principe que cette disposition est déjà applicable en droit national. L'art. 27, al. 4, let. b, CCC simplifie tout au plus la motivation du refus. La réserve d'ordre public s'étend également à l'absence de garantie des normes élémentaires en matière de protection des données, pour lesquelles des exigences élevées doivent être posées. L'entraide judiciaire devrait en priorité être subordonnée à une assurance correspondante.

2. Report de l'entraide judiciaire (al. 5)

20 Al. 5, permet à l'État requis, c'est-à-dire à l'autorité compétente, de différer l'exécution de la demande d'entraide judiciaire et de déroger ainsi au **principe de l'exécution rapide** énoncé à l'art. 25, al. 1, CCC, dans le préambule de la convention et dans la possibilité d'une procédure d'urgence prévue à l'art. 27, al. 9, CCC. A contrario, il s'ensuit que si les conditions de l'al. 5 ne sont pas remplies, la demande doit être exécutée dans un délai utile. Comme il s'agit d'un moyen moins sévère de refus, il n'y a pas de délai maximal fixe. L'exécution de la demande peut être reportée aussi longtemps que les conditions de l'al. 5 sont remplies.

21 La condition préalable au report est le risque que l'exécution immédiate de la demande compromette des enquêtes ou des procédures pénales menées par l'État requis. N'est pas seulement considéré comme une entrave le fait de compromettre l'enquête, par exemple dans le cas d'une enquête secrète de longue durée menée par l'État requérant. Le **retard dans une mesure de recherche de preuves imminente** qui serait à craindre en cas de remise des éléments de preuve à l'État requérant justifie déjà le refus. Toutefois, dans

l'intérêt d'une entraide judiciaire complète et rapide, il convient de ne recourir qu'avec retenue à la possibilité offerte par l'al. 5.

Selon la systématique de l'article 27 CCC, le **refus et le report** coexistent de manière indépendante en raison de leurs conditions et conséquences juridiques différentes, de sorte que la décision de refus pourrait être reportée jusqu'à la fin du délai prévu à l'al. 5. Toutefois, une appréciation globale doit en tout état de droit être effectuée lors de la décision prise en vertu de l'al. 6 et devrait également être conforme au principe de l'entraide judiciaire effective. 22

3. Condition comme condition minimale pour le refus et le report (al. 6)

Al. 6, concrétise le principe de l'entraide judiciaire effective et complète prévu à l'art. 25, al. 1, CCC. L'État requis ne doit pas être contraint d'élaborer en détail des demandes principales et subsidiaires. Il appartient plutôt à l'État requis de **donner suite à la demande dans toute la mesure du possible et, en cas de doutes, de consulter l'État requérant**. Il en résulte tout d'abord que les objections doivent être limitées, dans la mesure du possible, aux parties dissociables de la demande. La partie non concernée doit alors être traitée sans délai. L'al. 6 mentionne une deuxième possibilité pour garantir un traitement rapide, à savoir l'exécution sous conditions. Ces conditions concernent en premier lieu l'utilisation des moyens de preuve remis dans l'État requérant. Avant la remise, des assurances correspondantes doivent être obtenues. Souvent, la condition est que les éléments de preuve ne puissent être utilisés que pour la procédure en cours et non pour d'autres procédures ultérieures. En revanche, s'il existe des doutes quant à la légalité de l'exécution dans l'État requis, il convient, dans le cadre de la consultation, d'œuvrer à une adaptation de la demande. Si cela n'est pas possible, la demande doit être rejetée en tout ou en partie ou il convient de procéder conformément à l'al. 3. Dans l'intérêt d'une entraide judiciaire efficace, il convient également de ne faire usage des droits de l'État requis prévus à l'al. 6 qu'avec retenue. 23

D. Obligation d'informer (al. 7)

Al. 7, prévoit une obligation de communication des résultats de l'exécution et des motifs d'un refus ou d'un sursis. Cette disposition vise à informer l'État 24

requérant afin qu'il puisse formuler de manière plus efficace **ses futures demandes** adressées au même État. Il n'est pas nécessaire de communiquer séparément les motifs d'une condition. Il semble que l'on parte du principe que les motifs ressortent suffisamment de la condition elle-même ou qu'ils sont examinés dans le cadre d'une consultation avec l'État requérant conformément à l'al. 6.

E. Confidentialité (al. 8)

25 L'al. 8 permet, au-delà de l'al. 3, de fixer une condition à l'exécution de la demande qui ne sert pas l'utilité de la demande dans l'État requis, mais d'autres **intérêts tactiques ou politiques liés à l'enquête**. La formulation « dans la mesure où l'exécution de la demande ne s'y oppose pas » dans la traduction allemande prête à confusion : il ressort des versions anglaise (« except to the extent necessary ») et française (« sauf dans la mesure nécessaire ») que cette demi-phrase précise la notion de confidentialité et ne limite pas en principe la possibilité d'une procédure selon l'al. 8. Au sens de l'al. 8, est notamment confidentielle une mesure qui doit nécessairement être portée à la connaissance de la personne concernée, par exemple la banque du prévenu.

26 Compte tenu de la formulation restrictive et du principe d'entraide judiciaire aussi large que possible, les lacunes structurelles effectives ne peuvent en tout état de cause être invoquées pour justifier l'impossibilité de donner suite à une demande, par exemple les problèmes de corruption au sein des autorités compétentes. L'exception devrait plutôt être interprétée conformément à l'al. 3, 2e partie, et concerner ainsi **des obstacles juridiques**. La confidentialité ne peut donc pas être respectée lorsque les mesures faisant l'objet de la demande, y compris le fait qu'elles sont fondées sur une demande d'entraide judiciaire, doivent être divulguées en vertu du droit national impératif.

27 L'intérêt de l'État requérant vise généralement à empêcher l'**accusé** d'en prendre connaissance. Il en va de même pour la personne **concernée par** la mesure, dans la mesure où celle-ci est proche de l'accusé et où la mesure peut en principe être prise de manière secrète. La confidentialité n'est en tout état de cause pas garantie lorsqu'il y a communication directe à l'accusé ou lorsque l'on peut s'attendre à ce que l'intéressé obtienne l'information. De plus, la confidentialité n'est naturellement pas garantie lorsque le fait qu'une demande a été présentée ou le contenu de cette demande est rendu public, c'est-à-dire

connu d'un nombre indéterminé de personnes qui ne sont pas liées entre elles par des caractéristiques particulières.

Cela est en contradiction avec le droit de la personne concernée par la mesure à une **protection juridique effective** : si les résultats de la mesure sont transmis à un État étranger qui n'est pas lié par le droit suisse, les conséquences d'une violation de l'EIMP ne peuvent plus être éliminées. Les droits de l'homme de l'accusé et de la personne concernée doivent être conciliés avec les intérêts légitimes de l'État requérant en matière de confidentialité. La mise en balance des intérêts opérée par l'EIMP doit être considérée comme favorable aux personnes concernées. 28

L'art. 80m EIMP régit la notification des décisions de l'autorité d'exécution et présuppose donc la **notification tant de la décision d'entrée en matière que de la décision finale**, ainsi que des éventuelles décisions incidentes. Le moment de la notification n'est pas réglementé. A l'inverse, l'art. 63 al. 2 EIMP prévoit des mesures d'entraide judiciaire mineures qui seraient compromises par une annonce préalable. Cela concerne notamment la perquisition de personnes et de locaux. En outre, l'objet de la protection juridique et donc le point de rattachement prioritaire du droit d'être entendu selon l'art. 12 EIMP en relation avec l'art. 29 PA n'est pas la décision d'entrée en matière, mais la décision finale selon l'art. 80e, al. 1, EIMP. La communication de la décision d'entrée en matière à la personne concernée en même temps que la décision finale est donc admissible. 29

Cela garantit temporairement la confidentialité de l'existence et du contenu de la demande pour les mesures qui, de par leur nature, ne peuvent être portées à la connaissance de la personne concernée, comme l'audition. Toutefois, conformément à l'art. 80d en relation avec l'art. 80l al. 1 EIMP, il convient d'attendre l'**entrée en force de la décision finale** avant de transmettre les résultats de la mesure à l'État requérant. Une transmission anticipée, qui préserve la confidentialité à l'égard de la personne concernée à plus long terme, n'est possible que dans les conditions très strictes prévues à l'art. 80d^{bis} EIMP, qui exige notamment qu'il s'agisse d'un cas de criminalité organisée ou de terrorisme. Dans ce cas, la communication à la personne concernée est reportée conformément à l'art. 80d^{bis} al. 5 EIMP, mais doit être effectuée a posteriori. La confidentialité totale vis-à-vis de la personne concernée quant à l'existence d'une demande ne peut donc en aucun cas être garantie. 30

31 Si la personne concernée apprend l'existence de la mesure – par la notification d'une décision ou par un autre moyen –, elle bénéficie des droits prévus à l'art. 80b, al. 1, EIMP, à savoir le **droit de consulter le dossier** et le droit de **participer aux actes d'exécution**. Cela compromet la confidentialité du contenu de la demande d'entraide judiciaire. À cet égard, l'art. 80b al. 2 let. a et b EIMP offre toutefois la possibilité d'accéder à la demande de confidentialité concernant le contenu de la demande.

32 En vertu de l'art. 80n al. 1 EIMP, la personne concernée est en outre en principe habilitée à **informer** son mandant ou son client, qui est généralement le prévenu, de la mesure d'entraide judiciaire. La confidentialité ne peut alors plus être garantie à son égard non plus. L'art. 80n al. 1, 2e partie de la phrase, EIMP permet toutefois à l'autorité compétente d'interdire sous peine de sanctions l'information du mandant ou du client, ce qui est parfois le cas pour les décisions de remise de documents à des banques (art. 73 al. 2 CPP en relation avec l'art. 292 CP). La confidentialité est ainsi garantie, du moins d'un point de vue juridique.

33 La confidentialité peut donc être garantie sous certains aspects grâce à différentes réglementations particulières. Il n'existe toutefois pas de réglementation générale permettant de traiter les demandes d'entraide judiciaire de manière confidentielle avec la même efficacité que les mesures prises au niveau national. On peut se demander si cela suffit dans tous les cas pour satisfaire au **mandat d'adaptation de l'art. 25, al. 2, CC**.

34 La deuxième phrase laisse à l'État requérant la décision finale quant au traitement non confidentiel lorsque l'État requis ne peut garantir la confidentialité.

F. « Procédure accélérée » (al. 9)

35 L'al. 9 prévoit, pour les « cas urgents », la transmission des demandes sans participation directe des autorités centrales au sens de l'al. 2. La communication s'effectue soit directement entre les autorités d'exécution (let. a et d), soit par l'intermédiaire d'Interpol (let. b). La Suisse a toutefois fait usage de la possibilité prévue à la let. e et a décidé que les demandes entrantes doivent être adressées – conformément au libellé de la convention « pour des raisons d'efficacité » – **exclusivement à l'autorité centrale**, à savoir l'Office fédéral de la justice. Les autorités d'exécution en Suisse sont

ainsi déchargées du traitement immédiat des demandes entrantes. Pour les États étrangers requérants, la simplification réside (uniquement) dans le fait qu'ils ne doivent pas communiquer par l'intermédiaire de leur autorité centrale. Une autorité étrangère subordonnée peut adresser une demande à l'Office fédéral de la justice ou la transmettre à celui-ci par l'intermédiaire d'Interpol.

L'art. 27 CCC a pour but d'établir entre les États contractants une procédure minimale allant au-delà de l'entraide judiciaire non conventionnelle. En aucun cas, l'État requérant ne doit être défavorisé par rapport à une procédure fondée sur l'EIMP. Les demandes au titre de l'art. 27 CCC peuvent donc également être transmises par les **voies de communication prévues à l'art. 29 EIMP**. Cela inclut une procédure selon l'art. 29, al. 2, 2e alternative, EIMP, selon lequel la demande ne doit pas être adressée directement à l'autorité subordonnée, mais une copie peut lui être transmise au moins en même temps que la demande adressée à l'Office fédéral de la justice. 36

L'al. 9, let. e, ne contient **aucune réserve de réciprocité**. Les autorités suisses subordonnées peuvent donc, en vertu de la CCC, transmettre directement les demandes émanant d'autorités subordonnées d'autres États, pour autant que ces derniers n'aient pas fait de déclaration au sens de l'al. 9, let. e. Cela ne correspond toutefois pas à la procédure habituelle en Suisse (sous réserve des dispositions des traités internationaux). 37

IV. PROTECTION JURIDIQUE

Pour le citoyen concerné par les mesures faisant l'objet de la demande, les voies de recours sont régies par le droit **national de l'État requis**, conformément à l'art. 25, al. 4, CCC. Si la Suisse est requise, il convient donc, conformément à l'art. 21 EIMP, de désigner un conseil juridique et la décision finale peut faire l'objet d'un recours conformément à l'art. 80e EIMP. Si la Suisse demande l'entraide judiciaire à un autre État, la protection juridique contre les mesures en tant que telles est régie par le droit procédural de cet État. La personne concernée ne peut former un recours contre la demande suisse que dans les conditions prévues à l'art. 25, al. 2, EIMP, qui ne sont pas remplies dans le champ d'application de l'art. 27 CCC. 38

L'art. 27 CCC est contraignant entre l'État requérant et l'État requis et crée, lorsque les conditions sont remplies, une **obligation d'exécuter la demande** 39

d'entraide judiciaire. L'exécution s'effectue conformément à l'art. 45 CCC, qui prévoit en premier lieu une solution au niveau diplomatique et, à titre subsidiaire, une décision rendue par une instance à déterminer entre les parties, à savoir le Comité européen pour les problèmes criminels (CDPC), un tribunal arbitral ou la Cour internationale de justice.

BIBLIOGRAPHIE

Dangubic Miro, Kommentierung zu Art. 25 CCC, in: Graf Damian K. (Hrsg.), Onlinekommentar, Übereinkommen über die Cyberkriminalität (Cybercrime Convention), abrufbar unter https://onlinekommentar.ch/de/kommentare/ccc25, besucht am 5.4.2024.

Dangubic Miro/Stelzer-Wieckowska Marta, Kommentierung zu Art. 80b IRSG, in: Staffler Lukas/Glassey Maria Ludwiczak (Hrsg.), Onlinekommentar zum Bundesgesetz über internationale Rechtshilfe in Strafsachen, abrufbar unter https://onlinekommentar.ch/de/kommentare/irsg80b, besucht am 27.2.2025.

Donatsch Andreas/Heimgartner Stefan/Simonek Madeleine, Internationale Rechtshilfe, 3. Aufl., Zürch 2024.

Gercke Marco, Kommentierung zum Übereinkommen über die Cyberkriminalität, in: Grützner Heinrich/Pötz Paul-Günther/Kress Claus/Gazeas Nikolaos/Brodowski Dominik, Internationaler Rechtshilfeverkehr in Strafsachen, 3. Aufl., Heidelberg 2022 (zit. Grützner/Pötz/Kress/Gazeas/Brodowski-Gercke).

Gless Sabine, Überblick über die Rechtshilfe in Strafsachen, in: Schomburg Wolfgang/Lagodny Otto, Internationale Rechtshilfe in Strafsachen, 6. Aufl., München 2020 (zit. Schomburg/Lagodny-Gless).

Heimgartner Stefan/Niggli Marcel Alexander, Kommentierung zu Art. 80b IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan, Basler Kommentar Internationales Strafrecht, Basel 2015 (zit. BSK-Heimgartner/Niggli).

Meyer Frank, Ergänzende Kommentierung Schweiz, in: Ambos Kai/König Stefan/Rackow Peter, Rechtshilfe in Strafsachen, 2. Aufl., Baden-Baden 2020 (zit. Ambos/König/Rackow-Meyer).

Popp Peter, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel 2001.

Trautmann Sebastian, Kommentierung zu Art. 27 CCC, in: Schomburg Wolfgang/Lagodny Otto, Internationale Rechtshilfe in Strafsachen, 6. Aufl., München 2020 (zit. Schomburg/Lagodny-Trautmann).

MATÉRIAUX

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2010/4697.pdf, besucht am 5.4.2024 (zit. Botschaft 2010).

Explanatory Report to the Convention on Cybercrime, European Treaty Series – No. 185, Budapest, 23.XI.2001, abrufbar unter https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b, besucht am 5.4.2024 (zit. Explanatory Report).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 28 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Julian Mausbach

PROPOSITION DE CITATION

Julian Mausbach, Commentaire de l'art. 28 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Mausbach, art. 28 CCC N. XXX.

Art. 28 Confidentialité et restriction d'utilisation

[1] En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande:

a. à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou

b. à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au par. 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au par. 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

TABLE DES MATIÈRES

I. Orientation 234
II. Champ d'application (art. 28, al. 1) 235
III. Conditions restrictives (art. 28, al. 2) 236
IV. Impossibilité de satisfaire aux conditions (art. 28, al. 3) 237
V. Informations sur l'utilisation (art. 28, al. 4) 237
Matériaux 238

I. ORIENTATION

1 L'article 28 vise à garantir l'entraide judiciaire tout en imposant **des restrictions à l'utilisation des informations ou des matériels.** La partie requise est ainsi en mesure de ne fournir des informations ou des matériels particulièrement sensibles qu'à titre protégé. Cette protection peut aller jusqu'à limiter l'utilisation des informations à la finalité pour laquelle l'entraide a été accordée ou à définir le cercle des destinataires en interdisant la diffusion des informations ou des matériels fournis au-delà des autorités de poursuite pénale de la partie requérante. En ce sens, l'art. 28 doit être compris comme une norme de médiation classique qui, d'une part, est soumise à l'objectif fondamental de l'entraide judiciaire et, d'autre part, aux intérêts légitimes de la protection (des données) des informations et du matériel concernés.

2 L'approche de médiation est garantie par le fait que l'article 28 prévoit une **obligation de confidentialité**. En vertu de celle-ci, l'autorité destinataire doit traiter de manière confidentielle les informations qu'elle a reçues d'un autre État. Cela signifie que les informations ne peuvent être rendues publiques ou transmises à des tiers non autorisés.

3 Il existe en outre le **principe de la limitation de la finalité**. Selon ce principe, l'État destinataire ne peut utiliser les informations qu'aux fins pour lesquelles elles ont été initialement transmises. Cela signifie que les informations ne peuvent être utilisées à d'autres fins ou dans d'autres procédures sans le consentement de l'État qui les a transmises.

4 Ce principe est complété par le fait que les **dérogations à la limitation de la finalité** sont elles-mêmes soumises à l'exigence du consentement. Si l'État destinataire a l'intention d'utiliser les informations à des fins autres que celles couvertes par la limitation de la finalité, il doit obtenir l'accord de l'État qui les a transmises. Cela garantit que le contrôle de l'utilisation des informations reste entre les mains de l'État qui les a initialement fournies.

5 L'article 28 peut ainsi être considéré comme un élément central de la coopération internationale en matière de lutte contre la cybercriminalité. Il garantit que les informations échangées entre États sont traitées de manière confidentielle et utilisées uniquement aux fins prévues. L'article 28 crée ainsi une base pour un échange international d'informations dans un climat de

confiance et favorise le respect des directives nationales et internationales en matière de protection des données.

II. CHAMP D'APPLICATION (ART. 28, AL. 1)

L'art. 28 ne s'applique que s'il n'existe **aucun traité d'entraide judiciaire** ou accord fondé sur des dispositions légales uniformes ou réciproques entre la partie requérante et la partie requise. Les conventions et traités d'entraide judiciaire existants, notamment, en matière d'obtention de preuves, la Convention du 8 novembre 1990 relative au blanchiment d'argent, à l'identification, au gel et à la confiscation des produits du crime, la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 ou le deuxième protocole additionnel du 8 novembre 2001 à la Convention européenne d'entraide judiciaire en matière pénale doivent être respectés au regard de l'al. 1 et ont pour conséquence que l'art. 28 est supplanté par ceux-ci dans bon nombre de procédures d'entraide judiciaire. 6

Si un tel traité ou accord est en vigueur, ses dispositions relatives à la confidentialité et aux restrictions d'utilisation s'appliquent en lieu et place de l'art. 28. Cela vaut en tout état de cause, à moins que les parties n'aient expressément convenu d'appliquer l'art. 28, al. 2 à 4. Pour la plupart des procédures d'entraide judiciaire auxquelles participent les autorités suisses, il y a lieu de partir du principe que l'entraide judiciaire au sens de l'al. 1 est régie par les conventions et les traités d'entraide judiciaire correspondants. 7

La question de savoir s'il existe, et le cas échéant sous quelle forme, un accord entre la Suisse et d'autres Etats non parties aux accords d'entraide judiciaire précités qui exclut l'applicabilité de l'art. 28, établit ses propres règles de confidentialité ou se réfère à l'art. 28 al. 2 à 4, doit être examinée au cas par cas en fonction de la législation du pays concerné. La liste des traités bilatéraux et multilatéraux dans le domaine de l'entraide judiciaire pénale internationale tenue par l'Office fédéral de la justice est utile à cet égard. 8

S'il existe une réglementation entre les parties, celle-ci s'applique exclusivement. Les chevauchements avec d'autres traités d'entraide judiciaire bilatéraux et multilatéraux existants et avec des accords similaires sont ainsi évités grâce à la disposition claire de l'al. 1, de sorte que les autorités compétentes peuvent s'en tenir dans la pratique à la réglementation habituelle 9

et qu'il n'est pas nécessaire de trancher la question de la relation entre des accords concurrents, voire contradictoires.

III. CONDITIONS RESTRICTIVES (ART. 28, AL. 2)

10 L'al. 2 permet à la Partie contractante requise de poser deux types de conditions. Elle peut tout d'abord fournir les informations ou les documents à condition qu'ils restent **confidentiels** si et dans la mesure où la demande ne peut être satisfaite autrement (let. a ; comparable à l'identité confidentielle d'un informateur).

11 En outre, la condition peut être posée que les informations ou documents transmis ne peuvent être utilisés **à des fins autres que celles visées dans la demande** (let. b).

12 La restriction de l'utilisation des informations et documents transmis doit être expressément demandée par la Partie contractante requise. Cela doit d'ailleurs s'appliquer de la même manière à la condition de traitement confidentiel, comme il ressort déjà du libellé de la norme lorsqu'elle mentionne que la transmission est subordonnée à une condition et qu'une action de la partie requise est donc attendue.

13 En l'absence de déclaration expresse de la condition, la partie requérante n'est donc soumise à aucune restriction de ce type.

14 La deuxième condition, en particulier, reflète également à l'art. 28 le principe de spécialité ancré à l'art. 67 EIMP, qui revêt une importance capitale dans la pratique. Selon ce principe, les documents et renseignements transmis ne peuvent être utilisés dans l'État requérant que pour des procédures relatives à des infractions pour lesquelles l'entraide judiciaire n'est pas admissible. En Suisse, cette interdiction s'étend également et en particulier aux infractions qui, selon la conception suisse, ont un caractère politique, militaire ou fiscal.

15 Dans le cadre des négociations sur la Convention sur la cybercriminalité, **deux exceptions** à la possibilité de restreindre l'utilisation ont été reconnues. Elles sont donc implicitement contenues dans les dispositions de l'alinéa et ont elles-mêmes un effet restrictif dans la mesure où elles ne prévoient pas de restriction d'utilisation.

16 La première restriction découle des principes fondamentaux du droit de nombreux États, qui exigent que les informations et le matériel constituant

des preuves à décharge d'un accusé **soient divulgués à la défense ou à une autorité judiciaire.** Si les informations ou le matériel mis à disposition constituent de telles preuves, on ne saurait donc attendre ni exiger qu'il y ait violation des principes fondamentaux du droit.

De manière analogue, une restriction ne s'étend pas non plus aux **procédures judiciaires publiques.** Les éléments transmis dans le cadre de la procédure d'entraide judiciaire et destinés à être utilisés dans une procédure judiciaire qui est normalement publique ne peuvent faire l'objet d'une restriction d'utilisation correspondante. 17

IV. IMPOSSIBILITÉ DE SATISFAIRE AUX CONDITIONS (ART. 28, AL. 3)

L'al. 3 impose à la partie requérante l'obligation de réagir immédiatement à une condition si elle ne peut y satisfaire. La partie requérante doit **immédiatement informer** la partie requise de cette circonstance. Il appartient alors à cette dernière d'examiner et de décider si elle souhaite néanmoins fournir les informations, en connaissance de l'impossibilité de satisfaire à la condition, c'est-à-dire en fin de compte sans condition. À cet égard, on peut exiger et présupposer le respect des principes de l'entraide judiciaire, ce qui signifie, au regard de la décision, que la partie requise est en droit, dans un souci de transparence, d'utiliser la marge d'appréciation dont elle dispose également dans cette optique. 18

Si, concernant une condition, il n'est pas immédiatement communiqué qu'elle ne peut être remplie, cette condition est, comme dans le cas d'une acceptation expresse de la condition, en vigueur en tant que condition obligatoire. 19

V. INFORMATIONS SUR L'UTILISATION (ART. 28, AL. 4)

L'al. 4 constitue un **niveau de contrôle**. Il permet à la partie qui transmet des informations ou des documents de se faire une idée de la manière dont les informations et les documents mis à disposition sous réserve d'une condition énoncée à l'al. 2 ont été utilisés. Pour garantir cela, la partie requérante peut exiger de la partie requise qu'elle fournisse des informations sur l'utilisation des informations ou des documents. Celles-ci doivent être suffisamment détaillées et complètes pour permettre de vérifier le respect des conditions. 20

21 En fin de compte, cela sert non seulement à contrôler la partie requérante, mais aussi à garantir que la partie requise puisse respecter les obligations qui lui incombent, en particulier celle de veiller à ce qu'il n'y ait pas de violation de l'art. 67 EIMP.

MATÉRIAUX

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, BBl 2010 4697 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2010/813/de, zuletzt besucht am 19.2.2025 (zit. Botschaft CCC).

Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001, https://rm.coe.int/16800cce5b, zuletzt besucht am 19.2.2025 (zit. Explanatory Report).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 29 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Simon Bächtold

PROPOSITION DE CITATION

Simon Bächtold, Commentaire de l'art. 29 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité [Cybercrime Convention]

Citation abrégée: OK-Bächtold, art. 29 CCC N. XXX.

Section 2 Dispositions spécifiques

Titre 1 Entraide en matière de mesures provisoires

Art. 29 Conservation rapide de données informatiques stockées

[1] Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de

l'accès par un moyen similaire, de la saisie ou de l'obtention par unmoyen similaire, ou de la divulgation desdites données.

2 Une demande de conservation faite en application du par. 1 doit préciser:

a. l'autorité qui demande la conservation;

b. l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent;

c. les données informatiques stockées à conserver et la nature de leur lien avec l'infraction;

d. toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique;

e. la nécessité de la mesure de conservation; et

f. le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3 Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux art. 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5 En outre, une demande de conservation peut être refusée uniquement:

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b. si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6 Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7 Toute conservation effectuée en réponse à une demande visée au par. 1 sera valable pour une période d'au moins 60 jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

TABLE DES MATIÈRES

I. Introduction 243
A. Poursuite pénale multinationale fondée sur la division du travail en matière de cybercriminalité 243
B. Importance pratique et articles apparentés 243
II. Condition de la double incrimination (art. 29 al. 3 et 4 CCC), exclusion des poursuites politiques (art. 29 al. 5 let. a CCC) et violation de l'ordre public (art. 29 al. 5 let. b CCC) 245
III. Sécurisation et collecte de données à l'étranger 246
A. Faire une demande de préservation 246
1. L'autorité requérante (let. a.) 246
2. L'infraction qui fait l'objet de l'enquête ou de la procédure pénale et un bref exposé des faits (let. b.) 247
3. Les données informatiques stockées qui doivent être sauvegardées et le lien entre celles-ci et l'infraction (let. c.) 247
4. Toutes les informations disponibles pour déterminer le dépositaire des données informatiques stockées ou l'emplacement du système informatique (let. d.) 248
5. La nécessité de la sauvegarde (let. e.) et l'intention de la partie contractante de présenter une demande d'entraide judiciaire (let. f.). 248
B. Transmission et traitement de la demande de préservation 248
C. Délimitation avec l'Information Request 249
D. Procédure au moyen d'une demande d'entraide judiciaire 250
E. Meilleures pratiques pour les demandes d'entraide judiciaire adressées aux États-Unis 251
IV. Exécution des demandes de préservation par les autorités suisses 253
A. Déroulement de la procédure et compétences 253
B. Mise en œuvre par le biais du droit suisse 253
Bibliographie 257
Matériaux 257

I. INTRODUCTION

A. Poursuite pénale multinationale fondée sur la division du travail en matière de cybercriminalité

Les criminels utilisent **Internet** pour commettre des infractions, principalement pour deux raisons. D'une part, pour rester anonyme. D'autre part, pour adapter leur modèle commercial criminel à moindre coût, c'est-à-dire pour atteindre un grand nombre de victimes potentielles (en particulier la cyber-escroquerie). A cela s'ajoutent les délits informatiques au sens strict du terme, qui ne sont pas concevables dans le monde analogique (p. ex. piratage, attaques DDOS, etc.). 1

Conformément à la nature d'Internet en tant que réseau de communication mondial, la cybercriminalité a toujours lieu **au niveau international**. Les groupes criminels organisés agissent généralement à l'échelle mondiale, ou du moins - dans une perspective suisse - à l'échelle européenne, voire, dans certains cas, à l'échelle d'une région linguistique (p. ex. l'espace germanophone). Il en résulte qu'aucun État ne peut lutter seul contre la cybercriminalité. Les cyberenquêtes doivent presque toujours être menées au niveau international ou présentent des aspects transfrontaliers. Dans le cas d'enquêtes importantes et coûteuses, on parle de poursuite pénale internationale avec division du travail. Le contraste avec la poursuite pénale (suisse) ne pourrait pas être plus clair. En raison de la compétence primaire des cantons en matière de poursuite pénale, de très nombreuses ressources sont encore perdues dans notre pays pour clarifier la compétence nationale. Une image nationale de la situation concernant les phénomènes de cybercriminalité n'existe, au mieux, qu'à l'état d'ébauche. 2

Celui qui enquête dans le domaine cybernétique ne peut généralement pas passer à côté de l'art. 29 CCC (Preservation Request / saisie immédiate de données) en dehors du domaine des infractions mineures. 3

B. Importance pratique et articles apparentés

L'art. 29 CCC compte, avec l'art. 32 let. b CCC, parmi les dispositions les plus pertinentes de la Convention sur la cybercriminalité dans la pratique, du moins du point de vue des autorités de poursuite pénale. 4

5 La Preservation Request doit résoudre le problème suivant : les données électroniques sont volatiles et souvent stockées à l'étranger, mais les procédures d'entraide judiciaire sont régulièrement très longues. Du point de vue de la poursuite pénale, la situation est encore aggravée par le fait que de nombreux pays ne connaissent pas la "conservation des données préalables", ce qui peut conduire à la perte de données pertinentes pour l'enquête avant même qu'une demande d'entraide judiciaire ne puisse être déposée. Les demandes de préservation doivent donc permettre de **saisir** provisoirement, de manière simple et rapide, des données pertinentes pour la poursuite pénale à l'étranger, afin que l'Etat requérant ait le temps d'obtenir les données par la voie de l'entraide judiciaire.

6 Contrairement à l'Information Request selon l'art. 32 let. b CCC, qui peut être formulée à bas seuil et sans inconvénients ni frais pour l'Etat requérant, l'Etat requérant qui se réfère à l'art. 29 CCC s'engage à demander ultérieurement les données saisies à l'étranger également par le biais d'une **demande d'entraide judiciaire**. Une demande d'entraide judiciaire est liée à une certaine charge de travail pour le ministère public requérant, de sorte que ce dernier ne formulera pas de demandes de préservation à la légère.

7 La question de la **nature juridique** d'une Preservation Request se pose régulièrement. C'est par exemple le cas lorsque, après le dépôt d'une plainte pénale, il n'est pas encore clair s'il existe des soupçons initiaux suffisants pour ouvrir une procédure pénale (art. 309 al. 1 let. a CPP). Ce n'est que dans ce cas que les mesures de contrainte du ministère public sont possibles et justifiées. Si la demande de préservation n'était pas une mesure de contrainte, il serait possible que la police en fasse une de son propre chef, ce qui serait à saluer du point de vue de l'intention, car une sauvegarde des données devrait être d'autant plus efficace qu'elle est effectuée rapidement. La Convention sur la cybercriminalité elle-même ne répond pas à la question de la nature juridique, qui est régie par le droit de l'État sollicité (art. 25 al. 4 CCC). La réponse peut donc être différente. Pour la Suisse, on considère que la police ne peut en principe pas faire de demande de préservation sans l'accord du ministère public, car ce dernier s'engage alors à déposer ultérieurement une demande d'entraide judiciaire internationale (ce qui n'est possible que si une procédure pénale est ouverte). De même, la demande de sauvegarde immédiate des données entraîne une saisie temporaire des enregistrements, ce qui constituerait une mesure de contrainte dans le contexte national. Dans

les faits, une demande de préservation doit donc être traitée de la même manière qu'une **mesure de contrainte dans le cadre d'une procédure pénale**. En conséquence, une demande de préservation doit en principe être ordonnée par le ministère public, l'exécution pouvant être déléguée à la police. Dans les affaires nationales, une saisie temporaire par la police est exceptionnellement autorisée lorsqu'il y a "péril en la demeure" et que le ministère public ne peut pas être informé à temps (même oralement) (art. 263 al. 3 CPP). Dans de tels cas exceptionnels, la police peut également formuler des demandes de manière autonome conformément à l'article 29 CCC.

Il convient également de mentionner l'article 16 de la CCC, qui exige des Etats membres qu'ils créent les conditions législatives et organisationnelles nécessaires pour que les demandes de préservation des Etats étrangers puissent être satisfaites conformément à l'article 29 de la CCC. Dans le cadre de la mise en œuvre de la Convention, la Suisse a décidé de ne pas adopter de nouveau droit de procédure pénale à cet égard (cf. ci-après, n. 32). 8

II. CONDITION DE LA DOUBLE INCRIMINATION (ART. 29 AL. 3 ET 4 CCC), EXCLUSION DES POURSUITES POLITIQUES (ART. 29 AL. 5 LET. A CCC) ET VIOLATION DE L'ORDRE PUBLIC (ART. 29 AL. 5 LET. B CCC)

La Convention sur la cybercriminalité s'efforce de promouvoir au mieux la coopération internationale en matière de poursuite pénale des délits informatiques. C'est pourquoi la convention elle-même ne contient pas d'exigence de double incrimination, mais laisse les Etats parties libres de fournir une assistance même si seul l'Etat requérant incrimine une infraction correspondante (art. 29 al. 3 CCC). Les États parties sont libres d'émettre une réserve lors de la ratification, selon laquelle la double incrimination est une condition préalable. Dans ce cas, l'Etat requis peut refuser une demande de préservation s'il est déjà établi à ce moment-là que les données demandées à des fins de préservation ne pourront pas être communiquées par le biais de l'entraide judiciaire (art. 29 al. 4 CCC). Sur les 70 États qui ont ratifié la convention, 23 ont émis une réserve correspondante, dont la Suisse et les États-Unis d'Amérique. Comme les Etats-Unis ou leurs Etats fédéraux ne connaissent pas d'infraction pénale analogue à nos **délits d'atteinte à** 9

l'honneur, l'entraide judiciaire est toujours exclue à cet égard et, par conséquent, aucune Preservation Request n'est acceptée.

10 Indépendamment de la question de la double incrimination, la Convention sur la cybercriminalité exclut la Preservation Request pour les poursuites pénales à motivation politique (persécution) (art. 29 al. 5 let. a CCC), ce qui devrait aller de soi du point de vue suisse. Il en va de même lorsque la partie requise estime que l'exécution de la demande est de nature à porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels (art. 29 al. 5 let. b CCC).

III. SÉCURISATION ET COLLECTE DE DONNÉES À L'ÉTRANGER

11 Du point de vue suisse, l'art. 29 CCC est surtout pertinent pour la collecte de données informatiques à l'étranger (cf. n. 12 ss. ci-après). Mais cet article s'applique également aux demandes adressées à la Suisse par des États étrangers (voir ci-après, n. 31 ss).

A. Faire une demande de préservation

12 Le texte de la Convention lui-même donne des instructions assez détaillées sur la manière de formuler une demande de préservation. Les exigences suivantes sont expressément mentionnées :

1. L'autorité requérante (let. a.)

13 Dans la pratique, il s'agira régulièrement d'un **ministère public** (cf. aussi ci-dessus, n. 7). Du point de vue de la convention, rien ne s'oppose toutefois à ce que - en étroite concertation avec la direction de la procédure du ministère public (qui doit ensuite présenter la demande d'entraide judiciaire) - la police puisse déjà présenter une Preservation Request. Comme il s'agit de saisir à temps des données volatiles, cela peut même être judicieux. La mise en œuvre de la demande de préservation, c'est-à-dire sa qualification juridique, est régie par le droit national de l'Etat requis (art. 25 al. 4 CCC). Dans de nombreux Etats requis, la mise en œuvre de la demande de préservation (saisie de données sur le lieu de stockage) sera qualifiée de mesure de contrainte, de sorte qu'il n'est pas rare qu'une demande - ou du moins une

(co)signature - d'un procureur soit exigée. Dans l'ensemble, le traitement est très hétérogène.

2. L'infraction qui fait l'objet de l'enquête ou de la procédure pénale et un bref exposé des faits (let. b.)

Il s'agit ici de permettre à l'Etat requis de savoir si la **double incrimination** est réalisée (cf. supra, n. 9) et si la demande, qui peut tout à fait impliquer des efforts considérables, est proportionnée (rapport fin/moyens). Pour les phénomènes courants, une description de deux ou trois phrases suffit néanmoins à satisfaire à cette exigence. 14

3. Les données informatiques stockées qui doivent être sauvegardées et le lien entre celles-ci et l'infraction (let. c.)

Il convient de préciser quelles données doivent être concrètement sauvegardées (p. ex. données d'enregistrement, fichiers journaux/données marginales ou même données de contenu, en indiquant si possible et judicieusement les formats de fichiers). Mais il faut surtout justifier *pourquoi* ces données ont effectivement un **lien avec** les faits qui fondent le **soupçon**. Ce critère ressemble à ce que l'on appelle la pertinence potentielle des preuves dans le contexte d'une perquisition nationale selon l'art. 246 CPP (selon lequel "il y a lieu de présumer" que les enregistrements concernés contiennent des informations qui peuvent être saisies) ; ici, les données doivent seulement, mais tout de même, "pouvoir avoir de l'importance" ou ne pas paraître "manifestement inappropriées". Les recherches de preuves (*fishing expeditions*) sont mal vues. Ce critère est pris très au sérieux et une justification minutieuse est indiquée. Il ne faut pas oublier que dans d'autres pays, la compétence de saisir et/ou de remettre des données n'appartient pas au ministère public, mais doit être ordonnée par un tribunal des mesures de contrainte. Ainsi, dans les relations pratiques avec les Etats-Unis, le Department of Justice doit s'adresser à un tribunal pour faire ordonner la remise des données à un fournisseur de services par le biais d'un mandat de perquisition. Cela requiert une présentation substantielle et (selon les circonstances) étayée par les documents essentiels (en anglais) du lien avec le délit. La densité de la motivation va ici bien au-delà de ce à quoi les ministères publics suisses sont habitués dans le cadre du droit de procédure pénale national. Les autorités américaines consultent tout de même l'autorité 15

requérante, conformément à la pratique, si le degré de matérialité de la demande n'est pas encore suffisant, et donnent la possibilité de motiver plus précisément la Preservation Request.

4. Toutes les informations disponibles pour déterminer le dépositaire des données informatiques stockées ou l'emplacement du système informatique (let. d.)

16 En règle générale, on désigne ici simplement l'**entreprise** à laquelle la ressource d'adressage concrète est attribuée. Par exemple Google pour les adresses électroniques @gmail, Meta (pour Facebook, Instagram et WhatsApp), etc.

5. La nécessité de la sauvegarde (let. e.) et l'intention de la partie contractante de présenter une demande d'entraide judiciaire (let. f.).

17 La demande doit explicitement déclarer que la demande est **nécessaire** (au sens de la subsidiarité et de la proportionnalité) et confirmer que l'autorité requérante a l'intention de donner suite à la demande de préservation au moyen d'une commission rogatoire.

B. Transmission et traitement de la demande de préservation

18 Indépendamment du libellé de la Convention sur la cybercriminalité, il existe dans la pratique **deux voies** par lesquelles une demande de préservation peut ou doit être formulée. La voie typique est le réseau 24/7, conformément au texte de la convention (art. 35 CCC). Chaque Etat signataire s'est engagé à gérer un point de contact prêt à recevoir les demandes de préservation 24 heures sur 24 et 7 jours sur 7. En Suisse, ce rôle est assumé par l'Office fédéral de la justice en collaboration avec l'Office fédéral de la police (fedpol).

19 Pour des raisons d'efficacité (éviter les ruptures de médias, automatisation), de nombreux grands fournisseurs de services de communication basés sur Internet ont toutefois décidé d'exploiter leurs propres systèmes de demandes d'application de la loi (Law Enforcement Request Systems, LERS), par le biais desquels les autorités de poursuite pénale peuvent saisir directement leurs demandes de manière standardisée et en suivre l'évolution, sans devoir faire appel à d'autres autorités étatiques (p. ex. Office fédéral de la justice / Département de la justice). Il est judicieux, et c'est ce qui a été mis en œuvre

dans certains cantons, qu'un service central au sein de la police ou du ministère public gère les accès à tous les **portails LERS** disponibles, établisse et administre les Preservation et Information Requests sur mandat des directions de procédure. Cela permet de centraliser et d'évaluer les expériences faites avec les différents fournisseurs de services et de mettre à la disposition des directions des procédures des interlocuteurs compétents pour discuter à l'avance des chances de succès des demandes correspondantes.

Les autorités de poursuite pénale ont également la possibilité d'envoyer leurs demandes par courriel (crypté et authentifié) à l'**Office fédéral de la police** (fedpol). Les demandes y sont examinées, complétées si nécessaire par des demandes de précisions, traduites et transmises à l'autorité compétente à l'étranger. De manière générale, l'anglais est la langue recommandée pour les Preservation Requests dans le monde entier. Il est également possible de demander au service de coordination de fedpol si d'autres autorités de poursuite pénale suisses ont déjà envoyé la même Preservation Request, ce qui peut fournir des informations précieuses en vue de la coordination des enquêtes en cours (ou la possibilité d'adresser une demande d'élection de for à l'autre canton). 20

C. Délimitation avec l'Information Request

En quoi la Preservation Request se distingue-t-elle de l'Information Request selon l'art. 32 let. b CCC ? A ce sujet, nous renvoyons tout d'abord au commentaire de l'article 32 CCC. En bref, la demande d'information concerne la **remise volontaire** de données à un État partenaire de la CCC directement par le fournisseur de services. Dans la pratique, le "caractère volontaire" concerne le fournisseur de services et seulement indirectement l'utilisateur/le client du service. Les utilisateurs prévoient régulièrement dans leurs conditions d'utilisation qu'une transmission de données aux autorités de poursuite pénale est possible ; dans le cas concret, les clients concernés ne sont plus consultés. Le caractère volontaire du côté des utilisateurs est relatif dans la mesure où, sans le consentement aux conditions d'utilisation (et donc à la transmission de données aux services répressifs), de nombreux services ne peuvent tout simplement pas être utilisés. 21

Bien que la Convention sur la cybercriminalité ne connaisse pas cette restriction, une demande d'information ne peut, selon le droit national des Etats partenaires concernés, comprendre en règle générale que des données 22

d'enregistrement (également appelées "données de base" ou "subscriber information") conformément à l'art. 18 al. 3 let. b CCC (p. ex. nom, date de naissance, adresse, nom d'utilisateur, adresse de facturation, adresses e-mail, adresse IP lors de l'enregistrement) et des données périphériques ("traffic data", p. ex. l'historique IP), mais en règle générale **pas de données de contenu** ("content data"). Le terme "données de contenu" désigne le contenu d'une communication, c'est-à-dire par exemple un message, un post, des fichiers média, etc. Les données d'enregistrement sont de loin les plus fréquentes. Souvent, les demandes d'information et de préservation sont faites en même temps, car il n'est pas certain quelles données les fournisseurs de services mettent volontairement à disposition.

23 Dans la pratique, les demandes d'information sont formulées de manière beaucoup plus simple, car elles n'obligent pas le ministère public à présenter une demande d'entraide judiciaire. Une telle demande n'est d'ailleurs pas nécessaire, puisque la remise des données est volontaire et que le fournisseur de services y répond directement. La **volonté de coopération** des fournisseurs de services dépend fortement du type d'infraction. Les services sont particulièrement disposés à coopérer en cas de délits sexuels, en particulier au détriment d'enfants. Les délits contre le patrimoine sont plus problématiques. En bas de l'échelle se trouvent les délits contre l'honneur, pour lesquels la coopération échoue régulièrement, ne serait-ce qu'en raison de l'exigence de la double incrimination (cf. ci-dessus, n. 9 et n. 14).

D. Procédure au moyen d'une demande d'entraide judiciaire

24 Comme nous l'avons déjà mentionné à plusieurs reprises et comme le texte de la convention l'indique explicitement, le ministère public s'engage, par la Preservation Request, à demander les données saisies par la voie de l'entraide judiciaire. Il existe certainement des cas où il s'avère après coup que des données initialement sauvegardées sont devenues entre-temps obsolètes. Le fait de **renoncer à une demande d'entraide judiciaire** n'a pas non plus de conséquences directes (il n'y a par exemple pas de frais). On s'attend toutefois généralement à ce que les ministères publics respectent cette obligation de droit conventionnel afin de ne pas mettre en péril la bonne coopération entre les États signataires.

25 La conservation des données s'effectue **pendant au moins 60 jours** (cf. art. 29 al. 7 CCC). La durée concrète est indiquée dans la confirmation écrite de la

Preservation Request et est généralement plus longue. La plupart du temps, l'autorité requérante peut également faire une demande de prolongation de délai. Dans le délai imparti, la demande d'entraide doit être formellement déposée.

E. Meilleures pratiques pour les demandes d'entraide judiciaire adressées aux États-Unis

En raison de leur grande importance pratique, les meilleures pratiques pour les demandes d'entraide judiciaire adressées aux États-Unis sont abordées ci-après. Les explications suivantes se fondent sur le "Practical Guide for Requesting Electronic Evidence Across Borders", publié par l'UNODC, le CTED et l'IAP, ainsi que sur notre propre expérience. 26

Les demandes d'entraide judiciaire adressées à des autorités étrangères dans des affaires de cybercriminalité doivent contenir les informations suivantes : 27

- Langue de la demande : les demandes d'entraide judiciaire doivent idéalement être saisies directement en anglais, sinon elles doivent être traduites ;
- Faits : ils doivent être présentés brièvement mais dans les grandes lignes, en indiquant le lieu de l'infraction (ou le lieu du résultat), l'heure exacte de l'infraction et la manière dont elle a été commise ;
- Eventuel modus operandi : doit être décrit en détail ;
- Désignation juridique de l'acte, y compris les articles de loi applicables in extenso ;
- Motifs de la demande, en indiquant notamment le lien entre la procédure menée et les mesures demandées ;
- Les preuves recherchées ou les actes demandés doivent être décrits avec précision (p. ex. remise des extraits de compte concernant le compte X pour la période A à B, demande de documents auprès du fournisseur d'accès Y, d'où ressortent les données d'enregistrement et les logfiles concernant l'ID distant 12345678 pour la période entre A et B, etc ;)
- des explications sur l'éventuelle demande de préservation (Preservation Request) déjà formulée, tous les numéros de référence communiqués à la suite de la demande de préservation devant être mentionnés dans la

demande (CCIPS ainsi que numéros de référence de fedpol, de l'autorité de police étrangère requise et du ministère public étranger requis).

28 Pour obtenir les données de contenu des fournisseurs de services américains, le Department of Justice doit obtenir un mandat de perquisition auprès d'un tribunal, conformément au droit américain. L'obstacle du niveau de preuve est la "*cause probable*". Cela signifie que le tribunal doit être convaincu que le compte d'utilisateur en question contient probablement encore des preuves liées à un délit (à moins que les données n'aient déjà été provisoirement saisies sur la base d'une Preservation Request). Il est en outre nécessaire de disposer d'une base de preuves solide pour supposer qu'une infraction a été ou sera commise et que les preuves de l'infraction se trouveront sur le compte d'utilisateur demandé. Les sources des indices présentés doivent être dignes de confiance (par exemple, rapports de police, sources privées dignes de confiance). Des indices centraux doivent être présentés. Si des indices sont présentés, ils doivent être traduits en anglais. En résumé, il faut expliquer pourquoi le titulaire du compte est une cible de l'enquête, pourquoi on suppose que le compte d'utilisateur en question appartient à cette personne et quels sont les moyens de preuve que l'on espère obtenir de ce compte d'utilisateur.

29 La demande d'entraide judiciaire doit être envoyée soit par la voie diplomatique via l'Office fédéral de la justice, soit - si cela a été convenu et prévu - par voie de transmission directe au ministère public à l'étranger. Le guide de l'entraide judiciaire de l'Office fédéral de la justice contient des informations plus détaillées sur les voies de transmission concrètes.

30 Remarque :

- Pour les demandes d'entraide judiciaire dans les cas de cybercriminalité, il convient d'inscrire en plus la CCC comme base juridique (si le pays de destination a ratifié la convention).
- La présentation des faits, la subsomption des faits sous les éléments constitutifs de l'infraction ainsi que la mise en évidence des motifs de la demande sont l'alpha et l'oméga d'une demande d'entraide judiciaire internationale.
- Des informations détaillées sur l'entraide judiciaire sont disponibles dans le guide de l'entraide judiciaire de l'Office fédéral de la justice, avec des modèles dans différentes langues et un index des pays.

- Une demande d'entraide judiciaire faisant suite à une Preservation Request déposée doit être effectuée dès que possible, au plus tard dans le délai de prosecution (art. 29 al. 7 CCC).

IV. EXÉCUTION DES DEMANDES DE PRÉSERVATION PAR LES AUTORITÉS SUISSES

A. Déroulement de la procédure et compétences

Tous les Etats ayant ratifié la Convention sur la cybercriminalité ont indiqué laquelle de leurs autorités fait office de point de contact central pour les Etats requérants ("24/7 network", art. 35 CCC). Selon la déclaration de la Suisse, il s'agit en premier lieu de l'Office fédéral de la justice. Toutefois, c'est la Police judiciaire fédérale (fedpol) qui est compétente pour les questions relatives à la Convention sur la cybercriminalité, en particulier pour les demandes de préservation (l'Office fédéral de la justice transmet les demandes correspondantes à fedpol). Fedpol reçoit chaque année environ **200 demandes** de l'étranger, qu'il transmet à son tour aux corps de police cantonaux pour traitement. 31

B. Mise en œuvre par le biais du droit suisse

Le processus de traitement d'une demande de conservation étrangère en Suisse n'est **pas réglé par la loi**. Il est remarquable de constater à quel point le message relatif à la mise en œuvre de la Convention sur la cybercriminalité ne s'est pas penché sur les questions procédurales et pratiques. Il est seulement mentionné que les Etats parties ne sont pas tenus de créer d'autres instruments juridiques en plus de la saisie et de l'édition. 32

Le droit de procédure pénale suisse ne connaît **pas les "Preservation Orders"** au sens de la Convention sur la cybercriminalité. Un Preservation Order serait une décision des autorités à l'égard d'un fournisseur de services de tenir des données à disposition pendant une certaine période (typiquement dans le sens d'un Back Up). Comme cet instrument n'est pas prévu dans le CPP, la disponibilité à long terme des données doit être garantie d'une autre manière, ce qui ne peut se faire raisonnablement qu'au moyen d'une édition (art. 265 CPP). Comme les polices cantonales n'ont pas la compétence d'éditer des données, elles doivent à leur tour transmettre les 33

demandes correspondantes qu'elles reçoivent de fedpol au ministère public compétent, qui rend finalement une ordonnance d'édition. Alors que le code de procédure pénale ne connaît pas de base pour les Preservation Orders, la conservation des données prescrite par la loi a été mise en œuvre de manière comparable dans le domaine des télécommunications. Ainsi, ce sont les fournisseurs de services de télécommunication eux-mêmes qui doivent conserver les données d'enregistrement et les données marginales de communication de leurs clients pour une durée de 6 mois à l'intention des autorités de poursuite pénale (art. 21 al. 2, art. 22 al. 2 et art. 26 al. 5 LSCPT).

34 Cette conception suisse de la Preservation Request selon l'art. 29 CCC est relativement éloignée de l'esprit de la Convention, qui voulait une mesure rapide, simple et impliquant le moins de restrictions possibles pour toutes les parties. Le processus que nous venons d'exposer implique au moins trois autorités et l'entreprise destinataire, donc de nombreuses interfaces, ce qui entraîne des retards et augmente inévitablement le risque d'erreurs. Une décision d'édition, liée à la livraison physique ou numérique et à la conservation de quantités de données - parfois très importantes - représente en outre une **charge considérable** pour les fournisseurs de services et les autorités responsables de la conservation des données. Au niveau international, la question de savoir si les États qui n'ont pas introduit de Preservation Orders au sens de la Convention et qui se contentent d'ordonnances d'édition (comme la Suisse) remplissent les exigences de la Convention fait l'objet d'un débat. Si la majorité semble répondre par l'affirmative, des critiques subsistent néanmoins, notamment en ce qui concerne les obstacles juridiques plus élevés (pas en Suisse), la durée plus longue de la procédure et le risque éventuellement accru que les personnes concernées apprennent l'existence de la mesure, ce qui peut faire échouer le but de l'enquête.

35 L'exécution de demandes de préservation étrangères en Suisse ne fait pas encore partie d'une procédure d'entraide judiciaire formelle et ne constitue pas non plus une mesure préventive au sens de l'EIMP (ou d'autres bases du droit de l'entraide judiciaire). Elle se situe en amont d'une éventuelle procédure d'entraide judiciaire. Dans les faits, chaque Preservation Request ne devrait de loin pas être suivie d'une demande formelle d'entraide judiciaire. La Preservation Request trouve son fondement dans la Convention sur la cybercriminalité elle-même (qui, dans la mesure où elle est

suffisamment concrète, est directement applicable dans le système moniste de la Suisse). L'exécution de la Preservation Request en l'occurrence n'est pas suffisamment précise, raison pour laquelle il faut - comme mentionné plus haut - recourir aux institutions juridiques du droit de procédure pénale national, c'est-à-dire au code de procédure pénale (p. ex. art. 265 CPP, édition) ainsi qu'à la LSCPT et à ses ordonnances (p. ex. art. 38 OSCPT, IR_8_IP (NAT) : titulaires d'adresses IP). Ceci, toujours dans le but de respecter au mieux l'esprit de la Convention sur la cybercriminalité (prévention rapide, simple et efficace de la perte de preuves). Cela signifie également que les ordonnances d'édition émises en exécution d'une Preservation Request doivent être assorties d'une **interdiction de communication** au destinataire de l'édition, afin de ne pas compromettre le succès de l'enquête (art. 29 al. 6 CCC ; art. 73 al. 2 CPP en relation avec. art. 292 CP ; cf. par analogie également art. 11b al. 2 let. c EIMP et art. 80b al. 2 let. a EIMP). La conséquence en est que les personnes concernées ne peuvent pas encore recourir contre l'édition elle-même au moment de son exécution, faute d'en avoir connaissance. Dès qu'une procédure formelle d'entraide judiciaire est ouverte (si), les détenteurs de données (les clients concernés du service) doivent être informés de leur droit d'apposer des scellés (art. 9 EIMP en relation avec l'art. 248 al. 2 CPP). En revanche, si aucune demande d'entraide judiciaire n'est reçue dans un délai de 60 jours conformément à l'art. 29 al. 7 CCC et à un éventuel avertissement/délai supplémentaire, les données doivent être irrévocablement effacées faute de base légale pour une conservation plus longue.

Selon la situation juridique actuelle, le fournisseur de services lui-même a un droit propre d'apposer des scellés lors de l'édition en tant que détenteur des données (cf. art. 248 al. 1 CPP). L'apposition de scellés par le **fournisseur de services** pourrait toutefois entraîner des dépenses inutiles, à savoir lorsqu'une procédure de levée des scellés coûteuse doit être menée et que l'État requérant renonce ensuite à la procédure d'entraide judiciaire. A cela s'ajoute le fait que l'édition n'affecte souvent pas les propres intérêts secrets du fournisseur de services. Ce serait pourtant une condition préalable à une demande de scellement valable, car il n'est pas possible de demander le scellement à la place d'un tiers (par exemple le titulaire d'un compte). Si des données sont collectées par des fournisseurs de services qui, en raison de la nature de leur service, doivent régulièrement compter avec des données protégées par le secret, la question se pose d'autre part de savoir si le 36

ministère public qui exécute la Preservation Request (qui rend l'ordonnance d'édition) ne devrait pas déjà procéder d'office à l'apposition de scellés au moment de l'édition. Dans les deux cas, le ministère public devrait, pour exécuter la Preservation Request, déposer une demande de levée des scellés dans les 20 jours (art. 248 al. 3 CPP), à un moment où le détenteur des données ne devrait pas encore avoir connaissance de la Preservation Request et ne devrait donc pas être impliqué dans la procédure de levée des scellés (sans compter qu'il n'a généralement pas de domicile de notification en Suisse).

37 Afin de ne pas compromettre le succès de l'enquête et d'éviter des temps morts inutiles, la seule procédure cohérente dans le contexte de la convention sur la cybercriminalité serait que les scellés/décellés ne soient appliqués que dans le cadre de la procédure formelle d'entraide judiciaire. En tout état de cause, le scellement ne peut être possible que lorsque la collecte de données en tant que telle est terminée. On pense par exemple aux collectes de données qui résultent d'une seule demande de préservation, mais qui nécessitent plusieurs étapes successives sur le territoire national, par exemple plusieurs demandes de renseignements adressées au service OCTF (1. détermination de la ressource d'adressage à partir de l'adresse IP, 2. détermination du titulaire du raccordement à partir de la ressource d'adressage).

38 La question se pose de savoir si le droit suisse permettrait d'obliger les fournisseurs de services à simplement conserver certaines données, même en dehors du champ d'application de la LSCPT, au lieu de les fournir. Cela permettrait d'atténuer bon nombre des problèmes d'édition évoqués précédemment et serait donc à encourager. Une véritable **augmentation de l'efficacité** pourrait toutefois être obtenue si l'exécution des demandes de conservation étrangères était centralisée au niveau de la Confédération (fedpol), ce pour quoi il n'existe actuellement aucune base dans le code de procédure pénale (cf. art. 22 ss CPP *e contrario*). Une base juridique comparable se trouve en revanche déjà aujourd'hui à l'art. 18 al. 2 EIMP, selon lequel l'Office fédéral de la justice peut lui-même ordonner des mesures de sûreté provisoires s'il y a péril en la demeure.

BIBLIOGRAPHIE

Bommer Felix/Goldschmid Peter, Kommentierung zu Art. 265 StPO, in: Niggli Heer/Wiprächtiger (Hrsg.), Schweizerische Strafprozessordnung, Strafprozessrecht I + II, 3. Aufl., Basel 2023.

Graf Damian K., Praxishandbuch zur Siegelung, StPO inkl. revidierter Bestimmungen – VStrR – IRSG – MStP, Bern 2022.

Thormann Oliver/Brechbühl Beat, Kommentierung zu Art. 248 StPO, in: Niggli Heer/Wiprächtiger (Hrsg.), Schweizerische Strafprozessordnung, Strafprozessrecht I + II, 3. Aufl., Basel 2023.

MATÉRIAUX

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2010/813/de, besucht am 24.1.2024.

Council of Europe, The 24/7 Network established under the Convention on Cybercrime (known as the Budapest Convention), What is the 24/7 Network?, abrufbar unter: https://www.coe.int/en/web/cybercrime/24/7-network-new-, zuletzt besucht am 24.1.2024 (zit. CoE 24/7).

Cybercrime Convention Committee (T-CY), Assessment report, Implementation of the preservation provisions of the Budapest Convention on Cybercrime, Supplementary report, 15/16.06.2015, abrufbar unter: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b, zuletzt besucht am 24.1.2024 (zit. T-CY, Preservation Assessment).

Europarat, Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Strassburg, 3.12.2014, abrufbar unter: https://rm.coe.int/16802e726c, besucht am 17.10.2023 (zit. T-CY, Assessment Report).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report, Strassburg,

16.9.2016, abrufbar unter: https://rm.coe.int/16806a495e, besucht am 17.10.2023 (zit. T-CY, Cloud).

Europarat, Cybercrime Convention Committee (T-CY), The Budapest Convention on Cybercrime: benefits and impact in practice, Strassburg, 13.7.2020, abrufbar unter: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, besucht am 17.10.2023 (zit. T-CY, Benefits).

Opinion of the T-CY on the competent authority for issuing a preservation request under Articles 29 and 35 Budapest Convention, 28.11.2017, abrufbar unter: https://rm.coe.int/t-cy-2017-18-opinion-article29-/168076cf95, zuletzt besucht am: 19.1.2024 (zit. T-CY, Competent Authority).

Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185), Status as of 09/03/2024, abrufbar unter: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0, besucht am 9.3.2024 (zit. Reservations and Declarations).

United Nations Office on Drugs an Crime (UNDOC), Sharing Electronic Resources and Laws on Crime (SHERLOC), The Practical Guide for Requesting Electronic Evidence across Borders, für Strafbehörden abrufbar unter: https://sherloc.unodc.org/cld/en/st/evidence/practical-guide.html, besucht am 27.09.2023, zuletzt besucht am 24.01.2024 (zit. Practical Guide for Requesting Evidence).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 32 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Damian K. Graf

PROPOSITION DE CITATION

Damian K. Graf, Kommentierung zu Art. 32 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Citation abrégée: OK-Graf, N. XXX zu Art. 32 CCC.

Art. 32 Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie:

a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre

État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

TABLE DES MATIÈRES

I. Généralités 262
A. Introduction, historique, objectif et critique 262
B. Fondement de droit international public : les principes de territorialité et de souveraineté (art. 31 CCC) ainsi que leur violation (art. 32 CCC) 266
C. Matériaux et interprétation 269
D. Nature juridique 269
E. Champ d'application 270
F. Pertinence pratique 274
II. Accès à des données accessibles au public ("open source") stockées dans un autre État contractant (let. a) 274
A. Données accessibles au public 274
B. Nature juridique : qualification d'atteinte aux droits fondamentaux ? 276
C. Conditions d'un accès autorisé aux données selon le droit de procédure pénale suisse 279
III. Accès à d'autres données stockées dans un autre État contractant (let. b) 280
A. Consentement légal et volontaire de la personne légalement habilitée à transmettre les données 280
1. Autorisation de transmission 280
2. Consentement 282
B. Conséquence d'un consentement juridiquement valable 284
C. Conditions d'un accès autorisé aux données selon le droit de procédure pénale suisse 285
IV. Conservation des preuves au-delà de l'article 32 de la CCC selon le principe d'accès 288
V. Conséquences de la violation du droit à la souveraineté étrangère 292
VI. Nécessité d'une réforme 293
Bibliographie 294
Matériaux 300

I. GÉNÉRALITÉS

A. Introduction, historique, objectif et critique

1 Compte tenu de l'augmentation constante du transfert de la communication vers les services Internet (tels que le courrier électronique, les médias sociaux et la téléphonie par Internet) ainsi que de l'évolution technologique du stockage local vers le "cloud computing", l'objectif d'enquête des autorités de poursuite pénale a également changé. Leur travail devient de plus en plus complexe en raison de ce déplacement des preuves vers le monde numérique. Cette complexité s'explique d'une part par le fait que les données sont de nature volatile, qu'elles peuvent être déplacées sans problème au-delà des frontières (ce qui peut aussi se faire automatiquement, par exemple pour mieux exploiter les systèmes informatiques) et qu'elles peuvent être cryptées. D'autre part, les principaux fournisseurs de services Internet dont on ne peut plus se passer (comme Google, Facebook ou Meta, WhatsApp, X ou Microsoft) opèrent généralement depuis l'étranger (surtout les États-Unis) et proposent leurs services aux personnes physiques et morales en Suisse à partir de là, tandis que les données de leurs utilisateurs sont stockées à l'étranger. Il en résulte que les autorités d'enquête doivent régulièrement porter leur attention au-delà des frontières nationales, même dans des affaires internes. Dans les États membres de l'UE, plus de 50 % des enquêtes pénales font déjà l'objet d'une demande transfrontalière visant à obtenir des données électroniques. Cela pose quelques défis aux autorités de poursuite pénale, notamment en termes de droit international public, car la collecte extraterritoriale de preuves constitue prima vista une atteinte à la souveraineté de l'autre État (voir ci-après, n. 10 ss).

2 Dans ce contexte transfrontalier, les autorités doivent disposer de pouvoirs d'intervention effectifs leur permettant de garantir les éléments de preuve nécessaires aux procédures pénales nationales. L'entraide judiciaire, en tant que mécanisme traditionnel de coopération internationale, est considérée comme inefficace et lente, en particulier lorsqu'il s'agit de données volatiles ou de données qui peuvent être déplacées, effacées ou manipulées sans effort particulier. En règle générale, les enquêteurs ne savent pas non plus dans quel État les données sont stockées ou, selon le fournisseur de services Internet, dans quel État les données sont conservées, ce qui ne leur permet souvent pas

de juger, au moment de l'accès, s'ils franchissent la "frontière numérique de l'État", ni de savoir dans quel État l'entraide judiciaire doit être demandée - et même si les enquêteurs ont identifié un État, ils ont besoin d'un minimum d'informations (par exemple un mot de passe ou une adresse IP) pour justifier une demande d'entraide judiciaire prometteuse. un compte d'utilisateur ou une adresse IP), ce qui peut également s'avérer difficile dans certains cas.

La nécessité d'une conservation transfrontalière des preuves a été reconnue dès les années 90 et le 11 septembre 1995 - à une époque où les possibilités techniques actuelles n'étaient encore qu'esquissées dans certains ouvrages de vulgarisation - le Conseil de l'Europe a adopté la recommandation n° R (95) 13 sur les problèmes de procédure pénale liés aux technologies de l'information. Son paragraphe 17 se lit comme suit : "Le pouvoir d'étendre une recherche à d'autres systèmes informatiques devrait également être applicable lorsque le système est situé dans une juridiction étrangère, à condition qu'une action immédiate soit requise. Afin d'éviter d'éventuelles violations de la souveraineté des États ou du droit international, il convient d'établir une base juridique sans ambiguïté pour de telles recherches et captures étendues. Il y a donc un besoin urgent de négocier des accords internationaux sur la manière, le moment et l'étendue de telles recherches et incitations". En application de cette recommandation, des négociations ont ensuite été entamées en vue d'une convention sur la cybercriminalité. L'accélération de la coopération internationale ainsi que l'octroi éventuel de pouvoirs transfrontaliers, au mépris du principe de souveraineté, ont fait partie des thèmes centraux. 3

L'art. 32 de la Convention sur la cybercriminalité ("CCC") finalement adopté autorise, en violation de la souveraineté des Etats, l'accès à des données stockées dans d'autres Etats parties dans deux constellations, sans qu'une demande d'entraide judiciaire adressée aux autorités de l'autre Etat soit nécessaire : d'une part, lorsque des données accessibles au public sont concernées (let. a), et d'autre part, lorsque la personne autorisée a donné son consentement à l'accès (let. b). En d'autres termes, l'article 32 CCC permet dans ces cas une saisie directe de données stockées à l'étranger, sans qu'il soit nécessaire d'obtenir au préalable le consentement de l'État concerné et sans qu'il soit nécessaire de passer par la voie (semée d'embûches) de l'entraide judiciaire avant ou après la collecte. Le lest administratif disparaît totalement, car l'autre État ne doit pas être informé de la collecte des preuves. Si les conditions de l'art. 32 CCC ne sont pas remplies, notamment si l'ayant droit 4

ne coopère pas, ou si une collecte n'est pas possible techniquement ou ne peut être mise en œuvre pour d'autres raisons, il faut, en application de l'art. 31 CCC, recourir à titre subsidiaire à la voie ordinaire de l'entraide judiciaire, le cas échéant en liaison avec une demande de conservation immédiate des preuves au sens de l'art. 29 CCC, si une perte de preuves risque de se produire.

5 L'article 32 de la CCC n'a fait l'objet d'aucune remarque lors de la procédure de consultation et du processus législatif de mise en œuvre de la CCC en Suisse, malgré les notions sujettes à interprétation qu'il contient et l'atteinte à la souveraineté qu'il implique.

6 L'orientation de l'art. 32 CCC n'a pas échappé à la critique ailleurs, d'une part en raison de la suppression de la protection des droits fondamentaux garantie par la souveraineté territoriale qui en découle, sans même que les autorités nationales ne soient informées de telles atteintes aux droits fondamentaux. L'article 32 de la CCC autorise ainsi des actes de souveraineté étrangers incontrôlés sur le territoire national, ce qui porte atteinte aux droits constitutionnels des personnes concernées et des tiers, est disproportionné et délicat, en particulier pour les États dont la situation des droits de l'homme est trouble. La facilitation de l'administration des preuves dans le cadre de la procédure pénale qui découle de l'article 32 CCC est devenue incontournable dans la poursuite d'infractions à composante numérique : notre vie - et donc celle des personnes suspectées - est devenue numérique et se déroule de plus en plus souvent en dehors de l'espace numérique attribuable au territoire suisse. Certes, la plupart des appareils électroniques disposent encore aujourd'hui d'une mémoire locale propre, souvent généreuse, qui peut être saisie, perquisitionnée (art. 246 CPP) et confisquée (art. 263 CPP) sur la base des règles générales de la procédure pénale, pour autant que l'appareil puisse être saisi en Suisse. La tendance est cependant à l'abandon du stockage local au profit de solutions basées sur le cloud ou dislocales, dont le lieu de stockage se situe quelque part dans le monde, ou en tout cas seulement pour une petite partie en Suisse (à l'exception d'industries particulières comme les banques et le conseil). De même, la communication se fait aujourd'hui régulièrement par le biais de médias sociaux et de services Internet comparables, dont le contenu n'est parfois même plus stocké localement sur l'appareil personnel. En permettant aux autorités de poursuite pénale nationales d'un Etat contractant de demander directement aux fournisseurs

de services Internet étrangers la remise de données en évitant la voie de l'entraide judiciaire (cf. ci-après, n. 48, 55), l'art. 32 CCC garantit au moins partiellement que la recherche matérielle de la vérité ne devienne pas totalement illusoire en cas d'infractions ayant une composante numérique.

D'autre part, les milieux de la poursuite pénale en particulier considèrent l'article 32 CCC comme trop restrictif : l'article 32 CCC représente, en tant que " plus petit dénominateur commun ", un compromis finalement peu révolutionnaire. Les discussions sur l'admissibilité de l'obtention de preuves transfrontalières allant au-delà de l'article 32 CCC ont échoué en raison du manque de consensus au sein du Conseil de l'Europe. Les discussions qui se sont poursuivies depuis lors n'ont pas non plus permis de trouver un consensus, bien que la majorité des Etats considère le transfert de preuves au-delà des frontières nationales comme l'un des principaux défis de la poursuite pénale au niveau territorial. Le IIe Protocole additionnel à la Convention sur la cybercriminalité, adopté le 12 mai 2022 et déjà ratifié par deux États et signé par 40 autres États (état : octobre 2023), ne fait pas exception à la règle. Le Protocole additionnel à la Convention sur la cybercriminalité ("ZP II-CCC") n'a pas été un grand succès - mais il devrait tout de même permettre de demander directement et de manière contraignante à des prestataires de services à l'étranger, sans passer par l'entraide judiciaire, de fournir des informations sur l'enregistrement des noms de domaine et des données d'inventaire (art. 6 et 7 ZP II-CCC). La Suisse n'a pas encore signé ou ratifié le PA II-CCC, ce qui, selon des sources de l'Office fédéral de la justice, ne devrait pas se faire dans un avenir proche - d'une part parce que la nouvelle réglementation touche à nouveau au principe de souveraineté, et d'autre part parce que des discussions sont en cours sur ce thème au niveau des Nations Unies, et qu'il faut attendre qu'elles aboutissent. En effet, les discussions relatives à une convention des Nations unies sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles ("traité des Nations unies sur la cybercriminalité") en sont à un stade avancé. Le projet actuel, soutenu par la majorité, ne prévoit toutefois pas de collecte transfrontalière de preuves, raison pour laquelle il ne semble pas approprié d'attendre la signature et la ratification du PC II-CCC. 7

Le règlement (UE) 2023/1543 récemment adopté dans l'UE concernant les mandats européens d'obtention de preuves et les mandats européens de conservation des preuves électroniques dans le cadre des procédures pénales 8

et de l'exécution des peines privatives de liberté à l'issue de ces procédures, va un peu plus loin que l'article 32 de la CCC. 2023 ("règlement e-Evidence"), selon lequel les autorités judiciaires d'un État membre peuvent demander des preuves électroniques directement à un fournisseur de services d'un autre État membre (art. 1 al. 1 du règlement e-Evidence) et les fournisseurs de services sont légalement tenus d'éditer les données dans les 10 jours ou dans le délai imparti (art. 10 du règlement e-Evidence). L'art. 32 CCC mise en revanche sur le caractère volontaire des fournisseurs de services étrangers - s'ils ne répondent pas ou pas entièrement à la demande, la voie de l'entraide judiciaire doit être empruntée, même en cas de refus de coopération arbitraire, opaque ou infondé. Certes, l'art. 18 al. 1 let. b CCC prévoit au moins que le fournisseur de services Internet qui offre ses services "sur le territoire de la partie contractante" doit fournir sur demande les données existantes en rapport avec ces services. Le Tribunal fédéral ne permet toutefois pas d'ordonner la production de données sur la base de l'art. 18 al. 1 CCC à un fournisseur d'accès étranger ou considère qu'une telle décision est tout au plus légale si elle est adressée à sa filiale suisse, pour autant que celle-ci possède ou contrôle les données.

9 La critique des limitations de l'art. 32 CCC, exprimée surtout dans les milieux des poursuites pénales, s'est quelque peu atténuée en Suisse. En effet, le fait que la communauté internationale n'ait pas encore trouvé de solution consensuelle n'a pas empêché le Tribunal fédéral (sans doute pour des considérations de praticabilité, même si c'est au mépris du principe de souveraineté) d'autoriser également des collectes de preuves transnationales de données sans le consentement des personnes autorisées en recourant implicitement au principe dit de l'accès (cf. ci-après, n. 63 ss).

B. Fondement de droit international public : les principes de territorialité et de souveraineté (art. 31 CCC) ainsi que leur violation (art. 32 CCC)

10 Le principe de territorialité constitue une limite à l'action de l'Etat qui échappe à la souveraineté du droit international public. Il ne sert pas seulement à limiter l'applicabilité du droit pénal national à des faits étrangers - il existe bien sûr des exceptions - mais limite également l'action de l'Etat à son propre territoire. L'accomplissement d'actes officiels sur le territoire étranger n'est certes pas totalement interdit. Mais dans la mesure où un tel

comportement n'est pas expressément autorisé par des accords internationaux (d'entraide judiciaire), des traités bilatéraux ou du moins des autorisations ad hoc, il constitue une atteinte inadmissible à la souveraineté de l'État et peut, le cas échéant, être sanctionné en conséquence selon le droit étranger. Les actes officiels non autorisés sur le territoire étranger sont également sanctionnés par le droit suisse (art. 299 CP ; cf. également art. 271 CP). Les preuves recueillies en violation du principe de territorialité ne peuvent en outre pas, le cas échéant, être utilisées dans la procédure pénale nationale (cf. ci-après, n. 69 ss).

En particulier, les "actes arbitraires ayant un caractère de contrainte et d'intervention sur le territoire d'autrui" violent la souveraineté de l'Etat et sont donc contraires au droit international. Ainsi, dans la mesure où il n'est pas fait appel à l'entraide judiciaire de l'Etat étranger, les arrestations de personnes à l'étranger par des fonctionnaires suisses sont tout aussi interdites que les interrogatoires, les visites sur place ou l'exécution directe de jugements. Selon le Tribunal fédéral, il en va de même pour l'envoi de citations à comparaître à des prévenus domiciliés à l'étranger, qui ne doivent pas être assorties de menaces de contrainte et doivent donc être conçues comme de simples invitations. Il apparaît donc clairement que les autorités de poursuite pénale ne peuvent pas recueillir physiquement des preuves à l'étranger ou y effectuer des actes de procédure sans passer par la voie de l'entraide judiciaire ou sans que de tels actes soient explicitement autorisés par un accord. Les perquisitions arbitraires ou la saisie et la fouille d'appareils électroniques ou de documents sur le territoire d'un autre Etat sont donc sans aucun doute interdites. 11

Il n'en va pas autrement des situations de recherche de preuves dans lesquelles les autorités pénales ne se trouvent certes pas physiquement sur le territoire étranger, mais procèdent en Suisse à des actes d'enquête qui ont des répercussions sur la souveraineté territoriale étrangère. Il s'agit par exemple de l'observation de personnes sur la rive allemande du Rhin par des policiers suisses depuis Schaffhouse, tout comme l'interrogatoire vidéo d'un prévenu se trouvant à l'étranger par un tribunal suisse. Un tel comportement viole également le droit international, car il équivaut dans ses effets à un acte de souveraineté directement sur le territoire d'un Etat étranger. 12

L'accès à des systèmes informatiques à l'étranger à partir d'un site en Suisse et donc la saisie de données stockées à l'étranger doivent également être 13

qualifiés de tels actes de souveraineté extraterritoriaux. La communauté internationale revendique également sa souveraineté en ce qui concerne les installations de traitement de données stationnées sur son propre territoire et les données qui y sont stockées. Les pouvoirs de perquisition nationaux ne peuvent pas légitimer de telles atteintes à des droits de souveraineté étrangers. Cela a été reconnu par le Tribunal fédéral (voir toutefois ci-après, n. 63 ss.) et se reflète en particulier dans les discussions (intensives) sur le contenu et le développement de la CCC.

14 Dès qu'il est question de porter atteinte à la souveraineté d'un Etat étranger, celui-ci doit par conséquent donner son consentement, soit en fournissant l'entraide judiciaire sur demande individuelle, soit en accordant à des partenaires internationaux, par traité ou ad hoc, le droit d'agir en conséquence. Des exemples d'abandon partiel de la souveraineté de la Suisse se trouvent dans les accords avec les pays voisins sur la "poursuite" policière ou, de manière limitée, dans le contexte de la Convention sur la cybercriminalité. En effet, la création de l'art. 32 CCC a permis de renoncer à la nécessité d'une demande d'entraide judiciaire dans deux constellations : D'une part, l'accès à des données informatiques stockées et accessibles au public est autorisé, quel que soit le lieu géographique où se trouvent les données (let. a). D'autre part - et de manière très large par rapport à d'autres accords d'entraide judiciaire - une Partie contractante peut, selon l'article 32 let. b CCC, "accéder à des données informatiques stockées qui se trouvent sur le territoire d'une autre Partie contractante au moyen d'un système informatique situé sur son territoire ou recevoir ces données si elle obtient le consentement légal et volontaire de la personne légalement autorisée à lui transmettre les données au moyen de ce système informatique". Cela légitime non seulement une demande directe auprès de fournisseurs d'accès étrangers pour la remise d'informations, mais aussi l'accès en main propre des autorités par le biais de comptes d'utilisateurs existants (voir ci-après, n. 55). En d'autres termes, la CCC définit de manière contraignante pour les Etats parties dans quelles circonstances les autorités peuvent accéder directement à des données se trouvant à l'étranger (i.e. dans les conditions de l'art. 32 CCC) et quand elles sont tenues de déposer une demande formelle d'entraide judiciaire (dans tous les autres cas ; art. 31 CCC). Il en ressort que l'accès à des données étrangères est considéré comme une atteinte fondamentale à la souveraineté, indépendamment du fait que les membres des autorités de poursuite pénale ne se trouvent pas physiquement sur le territoire étranger

lors de telles mesures de conservation des preuves. Dans le cadre de l'élaboration de la CCC, il s'est précisément avéré "qu'aucun consensus n'a pu être atteint sur des règles plus larges concernant les conditions dans lesquelles un accès unilatéral d'un État à des données se trouvant dans un autre État contractant peut avoir lieu sans l'autorisation de ce dernier".

C. Matériaux et interprétation

Les termes utilisés par l'article 32 de la CCC et les constellations qu'ils couvrent n'ont été que partiellement précisés dans le Rapport explicatif sur la CCC - en substance le "message" du Conseil de l'Europe sur la CCC -, ce qui comporte le risque que les autorités des États contractants les interprètent différemment. Il semble toutefois qu'il s'agisse d'une décision délibérée. Toujours est-il qu'un groupe de travail sur l'accès transfrontalier aux données ("T-CY Transborder Group") du Comité des Parties ("Cybercrime Convention Committee", "T-CY") a émis le 3.12.2014 une note d'orientation ("Guidance Note") sur l'accès transfrontalier aux données au titre de l'art. 32 CCC, qui peut être utilisée comme aide à l'interprétation. Les conditions de l'art. 32 CCC - par exemple la question de savoir qui est habilité à donner le consentement selon l'art. 32 let. b CCC - doivent toutefois être déterminées en dernier ressort selon le droit interne (cf. ci-après, n. 41 s.) ; sur ce point, une définition nationale et donc d'éventuelles divergences d'opinion entre les États contractants sont inévitables. 15

Selon le Conseil fédéral, la disposition doit être interprétée de manière restrictive "afin de contrecarrer le risque d'abus en contournant l'entraide judiciaire ou en portant atteinte à la sphère privée de tiers". Toutefois, si l'on tient compte de l'effet recherché par l'article 32 de la CCC - l'accélération de la procédure ou la simplification de l'administration des preuves -, cela laisse une marge de manœuvre pour des interprétations proches et adaptées à la pratique. 16

D. Nature juridique

L'art. 32 CCC est une norme de droit international public "self-executing" qui s'applique directement dès sa ratification. Les parties contractantes accordent ainsi aux autres États contractants le droit d'accéder directement aux données sur leur territoire en contournant la voie de l'entraide judiciaire. En d'autres termes, la disposition normalise une "renonciation à la procédure nationale 17

dans l'État requis". Les autorités de poursuite pénale des Etats contractants peuvent se fonder directement sur l'art. 32 CCC, que ce soit dans le cadre de la procédure pénale nationale pour légitimer l'obtention de preuves correspondantes à l'étranger (tout en continuant à devoir respecter les règles de procédure nationales, cf. ci-après, n. 56) - l'art. 32 CCC ne constitue pas à cet égard une mesure de contrainte originale - ou qu'elles puissent invoquer, dans leurs relations avec l'Etat contractant concerné, l'absence d'atteinte illicite à la souveraineté étrangère. Par rapport à l'EIMP, les dispositions de la CCC priment en tout cas sur celles de l'EIMP (art. 1 al. 1 EIMP).

E. Champ d'application

18 L'art. 32 CCC autorise la saisie de données informatiques stockées dans un autre État contractant.

19 Selon l'art. 1 let. b CCC, sont considérées comme données informatiques toutes les représentations "de faits, d'informations ou de concepts sous une forme appropriée au traitement par un système informatique, y compris un programme qui peut déclencher l'exécution d'une fonction par un système informatique". L'article 32 de la CCC couvre donc l'accès aux données relatives au stock, au trafic ou à la marge, ainsi qu'au contenu, qui sont soit stockées, soit en cours de transmission au moment de l'accès. En raison de sa qualification juridique en tant qu'ensemble de données électroniques, les crypto-actifs peuvent par exemple être saisis en application de l'art. 32 let. b CCC, dans la mesure où les personnes habilitées donnent leur autorisation.

20 L'art. 32 CCC se réfère expressément au lieu de stockage des données concrètement envisagées (art. 32 let. b CCC : "[...] données informatiques stockées qui se trouvent sur le territoire d'une autre Partie contractante" ; cf. également art. 31 CCC : "[...] qui sont stockées au moyen d'un système informatique se trouvant sur le territoire de la Partie contractante requise"). Dans le cas de données stockées en plusieurs endroits, c'est l'endroit où se trouve l'ensemble des données qui doit être concrètement saisi qui est déterminant. Par conséquent, un accès en application de cette disposition n'est autorisé que si la CCC est applicable au lieu de stockage des données. Comme aucun des 68 Etats parties n'a émis de réserve à l'art. 32 CCC, l'examen peut se limiter à la question de savoir si l'Etat du lieu de stockage concerné est partie à la Convention sur la cybercriminalité, c'est-à-dire s'il l'a signée et ratifiée.

L'art. 32 CCC ne s'applique pas aux situations purement nationales : Si les données sont stockées localement sur un terminal ou un serveur se trouvant en Suisse et y ayant été saisi, c'est le droit national suisse qui s'applique à cet égard (en premier lieu les art. 246, 263 et 265 CPP, pour les données marginales voir l'art. 273 CPP). C'est également le cas lorsque des données étrangères se trouvent, au moment de l'accès, dans la mémoire intermédiaire de l'appareil saisi ici. Si l'appareil est utilisé comme "clé" ou "porte d'entrée" pour accéder à des services dont les données sont stockées à l'étranger (p. ex. cloud, webmail, etc.), sans que celles-ci soient stockées localement sur l'appareil, il s'agit d'une soustraction de données transnationale et l'art. 32 CCC doit être respecté (cf. toutefois n. 63 ss. ci-après). Le droit national suisse s'applique également lorsque des fournisseurs d'accès étrangers ont des filiales ou des partenaires suisses qui stockent les données en Suisse. Dans ce cas, l'accès peut se faire auprès de ces derniers. Toutefois, les centres de données n'en font généralement pas partie, car les données qu'ils stockent sont souvent cryptées et ne peuvent guère être lues sans la collaboration ou la collecte forcée des personnes autorisées à consulter les données. Il faut alors demander aux personnes étrangères la remise des données ou des clés, soit en application de l'art. 32 let. b CCC, soit subsidiairement par le biais de l'entraide judiciaire. L'art. 32 let. b CCC est également applicable lorsque des filiales ou des partenaires nationaux de fournisseurs d'accès étrangers sont enjoints par le ministère public de remettre des données qu'ils ont stockées à l'étranger. Il est correct de ne pas demander à une personne nationale, sous la menace, de fournir aux autorités de poursuite pénale à l'étranger des moyens de preuve disponibles, même s'il s'agit de données auxquelles elle a un droit d'accès. Le Tribunal fédéral a estimé qu'une ordonnance de production de documents au sens de l'art. 265 CPP adressée à une filiale suisse d'un fournisseur de services Internet était admissible si elle disposait d'une possibilité et d'une autorisation d'accès ("pouvoir de disposition, en fait et en droit, sur ces données"). Cela ne va pas à l'encontre de ce qui vient d'être dit, étant donné que l'ordre de production ne constitue pas encore une mesure de contrainte et que, dans ce contexte, il peut être compris et apprécié comme une demande de remise volontaire au sens de l'article 32 de la CCC. 21

En ce qui concerne les États tiers qui n'ont pas adhéré à la Convention, il faut partir du principe que la souveraineté de l'État y interdit tout accès en ligne à des données (non publiques, voir ci-après, n. 35) et que seule la voie de l'entraide judiciaire entre donc en ligne de compte. 22

23 Il est certes évident de se baser sur le lieu de stockage, car les Etats peuvent également invoquer le principe de souveraineté en ce qui concerne l'infrastructure informatique se trouvant sur leur territoire. Le problème est qu'au moment de l'accès, il n'est pas rare que ni l'autorité de poursuite pénale, ni la personne autorisée à consulter les données, ni même le détenteur des données, ne sachent où les données sont stockées à tout moment. Ainsi, les fournisseurs de services Internet ne stockent parfois pas les données de leurs clients dans leur pays d'origine, mais ailleurs. Le lieu de stockage peut également changer au fil du temps en raison de restructurations techniques ou de transferts vers d'autres sites (moins chers). En tout état de cause, il n'est souvent pas possible de déterminer avec certitude le lieu de stockage au moment de la consultation des données. La question se pose donc de savoir comment traiter le cas standard dans lequel l'autorité de poursuite pénale ne peut pas déterminer, au moment de la saisie envisagée, si les données sont stockées dans un Etat partie à la CCC, dans un Etat tiers ou même dans son propre pays. La documentation relative à l'art. 32 CCC n'aborde pas cette question de manière exhaustive ; la T-CY Guidance Note prévoit seulement, mais tout de même, que dans les situations où le lieu de stockage est inconnu ou incertain, les Parties doivent évaluer elles-mêmes la légitimité de l'accès à la lumière du droit national, des principes pertinents du droit international ou en tenant compte des relations internationales ("[...] Parties may need to evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations"). En cas d'emplacement inconnu, la question suivante se pose : Si l'applicabilité de l'article 32 de la CCC exigeait la connaissance certaine que le lieu de stockage se trouve dans un État contractant, l'article 32 let. b de la CCC perdrait sa signification et la sécurisation des données en nuage serait réduite à l'absurde. "La seule possibilité d'un emplacement dans un pays tiers ne peut pas non plus déclencher une obligation d'entraide judiciaire, d'autant plus qu'il n'est pas du tout établi à quel pays il faut s'adresser pour cela". Des clarifications détaillées sur le lieu de stockage sont souvent impossibles avant l'accès ou prennent trop de temps - certes : s'il n'y a pas d'urgence et que le lieu de stockage peut être déterminé techniquement sans effort particulier, on devrait s'y efforcer. Compte tenu de l'idée d'accélération de la CCC, il ne serait pas indiqué d'attendre jusqu'à ce que la connaissance soit sûre, surtout s'il y a un risque de perte de preuves. S'il devait s'avérer après coup que le lieu de stockage se

trouvait effectivement dans un Etat tiers, il faudra demander une autorisation ultérieure d'accès aux données par le biais de l'entraide judiciaire (voir ci-après, n. 71).

En ce qui concerne les grands fournisseurs de médias sociaux, la situation est encore un peu plus compliquée. Ceux-ci ont leur siège principal aux Etats-Unis, mais leur siège européen se trouve souvent en Irlande et, selon leurs propres indications (qui ne sont pas forcément correctes au vu du U.S. Cloud Act), ils n'ont accès aux données des clients européens et suisses qu'à partir de l'Irlande (ce que les fournisseurs justifient par le règlement européen du 27.4.2016 sur la protection des données ["DSGVO"]), les données étant à leur tour régulièrement stockées dans d'autres Etats (p. ex. en Suède). L'Irlande n'a toutefois pas encore ratifié la CCC. La question se pose donc de savoir si les demandes au sens de l'art. 32 let. b CCC pour des données européennes à l'intention des filiales irlandaises sont autorisées et si les données collectées sont utilisables. La Suède doit-elle être considérée comme un lieu de stockage possible, même si les données peuvent éventuellement y être consultées, mais qu'elles sont cryptées et donc inutilisables ? Ou faut-il s'adresser à la société mère américaine, qui doit se procurer les données auprès de sa filiale européenne ? Dans la pratique, le caractère explosif de cette question est atténué par le fait que les demandes de renseignements peuvent être adressées par le biais des "Law Enforcement Portals" mis à disposition par les fournisseurs de services Internet - la société du groupe à partir de laquelle les fournisseurs mettent les données demandées à la disposition des autorités ou la manière dont ils se sont organisés en interne est laissée à leur appréciation et ne doit pas faire l'objet d'un examen plus approfondi, d'autant plus que les autorités de poursuite pénale n'ont de toute façon pas la possibilité de vérifier où les données éditées ont été effectivement stockées et quelle société du groupe y a précisément eu accès. 24

Compte tenu de toutes ces difficultés, le lieu de stockage n'a guère de sens en tant que critère déterminant. De lege ferenda, il conviendrait donc de renoncer au critère de rattachement du lieu de stockage pour l'art. 32 CCC et de le rattacher plutôt au siège ou au lieu de séjour de la personne qui a légalement accès aux données. Alternativement (conformément au règlement e-Evidence de l'UE et à l'art. 18 al. 1 let. b CCC), on peut aussi se contenter du fait que l'entreprise concernée offre ses services dans l'État concerné. 25

F. Pertinence pratique

26 L'article 32 de la CCC est devenu un outil indispensable pour la poursuite de la criminalité avec une composante numérique. Les autorités de poursuite pénale suisses s'appuient régulièrement sur l'art. 32 CCC, que ce soit par la collecte d'informations de source ouverte ("OSINF") en application de l'art. 32 let. a CCC, ou par l'accès aux données en cas de communication volontaire des données de connexion par la personne suisse habilitée à traiter les données conformément à l'art. 32 let. b CCC, ou en particulier par des demandes directes ("Information Requests") adressées à des fournisseurs de services Internet étrangers pour la communication de données d'inventaire, de données marginales ou de données de contenu (sachant que dans la pratique, seules les données d'inventaire et les données marginales sont le plus souvent fournies et que pour les données de contenu, il faut passer par la voie de l'entraide judiciaire, le cas échéant en combinaison avec une "Preservation Request" selon l'art. 29 CCC). Les chiffres des demandes directes de renseignements sont remarquables : au cours du premier semestre 2022, Google a reçu à lui seul plus de 422 000 demandes directes, dont 1 357 émanant d'autorités de poursuite pénale suisses, dont 90 % ont été acceptées. Les fournisseurs d'accès n'ont toutefois pas de comptes à rendre s'ils refusent une demande ; ils peuvent fixer eux-mêmes les conditions d'une remise, les modifient régulièrement et, en outre, les conditions varient considérablement d'un fournisseur à l'autre. Cela est acceptable dans le régime actuel, puisque l'article 32 de la CCC est basé sur le volontariat.

II. ACCÈS À DES DONNÉES ACCESSIBLES AU PUBLIC ("OPEN SOURCE") STOCKÉES DANS UN AUTRE ÉTAT CONTRACTANT (LET. A)

A. Données accessibles au public

27 Dans le secteur du renseignement, la collecte et l'exploitation d'"informations en source ouverte" sont désignées par le terme "OSINT" ("Open Source Intelligence"). L'utilisation de données accessibles au public est également devenue une méthode d'enquête utile et non invasive dans le domaine de la répression. Cette tendance est soutenue par l'industrie technologique, qui a développé des outils permettant d'automatiser la collecte des données au lieu

de les rassembler manuellement : Par exemple, en mettant à disposition un logiciel permettant d'extraire de Facebook toutes les informations accessibles au public et de les représenter sous forme d'arbres de relations et sur l'axe du temps, ou des aides techniques permettant de suivre le flux d'argent des crypto-monnaies (dont la blockchain est accessible au public). L'utilisation de l'intelligence artificielle n'est plus une utopie.

Les données sont publiques lorsqu'elles sont librement accessibles via un système de traitement des données et qu'elles ne sont pas soustraites à l'accès général par des mesures de sécurité particulières. Il suffit qu'elles soient rendues accessibles à un cercle indéterminé d'utilisateurs, même si un login est nécessaire, "mais que celui-ci est en principe accordé à chaque utilisateur lorsqu'un formulaire d'inscription correspondant a été rempli". Un système peut également n'être que partiellement public. En revanche, les données qui "ne sont accessibles qu'au moyen d'une interface d'un terminal se trouvant dans l'objet de la recherche - non accessible au public" ne sont pas "open source". 28

Sont considérées comme données accessibles au public, à titre d'exemple et dans le sens d'une énumération non exhaustive, les médias de masse librement accessibles (presse écrite [même si elle est protégée par un paywall], radiodiffusion), toutes les informations trouvables sur Internet (Clearnet ainsi que Darknet), les applications basées sur le Web (comme Google Earth), les informations sur la blockchain visible par le public (par ex. pour le bitcoin), les données accessibles au public sur le site web d'une entreprise ou d'une administration, les webcams librement accessibles, une liste de diffusion ouverte à toute personne intéressée, les données librement disponibles sur une plateforme de partage, l'extraction de données techniques à partir d'un serveur web, la détermination d'informations sur les domaines via des bases de données "WhoIs", des renseignements sur les débiteurs, le registre foncier, le registre du commerce et le contrôle de l'habitant accessibles librement ou contre paiement à l'étranger ou des enregistrements disponibles de procédures pénales, administratives et civiles, l'observation de chats publics, de forums Internet ouverts et de réseaux sociaux activés publiquement (l'utilisation de données publiques, de photos et de relations sur Facebook, d'informations à partir de X, Instagram, LinkedIn, etc.). Un post dans un groupe fermé (forum en ligne, Facebook ou autre) peut également être qualifié de public dans le cas de groupes comptant un grand nombre de 29

membres ou dont l'accès est de fait illimité, à moins que le cercle de personnes ne soit délimité de manière précise et que les personnes soient personnellement liées entre elles. De même, ne peuvent plus être qualifiés de publics "les groupes d'utilisateurs fermés dans lesquels les administrateurs du site vérifient l'identité des utilisateurs au cas par cas et où un enquêteur n'aurait accès qu'en simulant une légende, par exemple".

30 Selon les circonstances, non seulement les données de contenu (données personnelles ou autres), mais aussi les données de base (par exemple les informations d'enregistrement des bases de données "WhoIs") ou (rarement) les données marginales peuvent être publiques et donc être collectées en application de l'article 32 let. a CCC.

31 Pour la qualification de données accessibles au public, il importe peu que les données aient été publiées sans autorisation ou avec le consentement de la personne autorisée à traiter les données. Si la publication a eu lieu de manière illégale (par exemple en raison d'une violation des obligations légales de confidentialité), les données sont utilisables dans la procédure pénale nationale si elles auraient pu être obtenues légalement par les autorités de poursuite pénale et si une pesée des intérêts plaide en faveur de leur utilisation. Pour le premier critère, il convient donc de déterminer si les données auraient hypothétiquement pu être saisies même si elles n'avaient pas été publiques - c'est-à-dire si elles auraient pu être obtenues dans le cadre de l'art. 32 let. b CCC ou par la voie de l'entraide judiciaire.

B. Nature juridique : qualification d'atteinte aux droits fondamentaux ?

32 La question est de savoir dans quelle mesure la collecte et l'exploitation de données accessibles au public doivent être qualifiées d'atteinte aux droits fondamentaux et, par conséquent, de mesure de contrainte au sens de l'article 196 CPP. La réponse à cette question est essentielle, d'une part pour déterminer dans quelle mesure il est possible d'accéder à des données publiques situées dans un Etat tiers, et d'autre part parce que, dans l'affirmative, il doit exister une base légale suffisamment concrète (art. 197 al. 1 let. a CPP). Cette dernière condition est déjà remplie par l'art. 95 CPP (collecte de données personnelles).

Selon l'art. 196 CPP, les mesures de contrainte sont des actes de procédure des autorités pénales qui servent entre autres à conserver des preuves, dans la mesure où elles portent atteinte aux droits fondamentaux des personnes concernées. L'art. 196 CPP ne présuppose donc pas nécessairement la contrainte (contrairement au libellé ["mesure de contrainte"]), mais se fonde plutôt de manière décisive sur la question de savoir si la mesure doit être considérée comme une atteinte aux droits fondamentaux des personnes concernées. Outre le droit à la liberté personnelle et la garantie de la propriété, la protection de la sphère privée selon l'art. 13 Cst. et l'art. 8 CEDH, ou plus concrètement le droit à l'autodétermination en matière d'information qui y est ancré, est au premier plan. Parmi les atteintes à ce droit constitutionnel, on peut citer les écoutes téléphoniques, la collecte de données de télécommunication, le prélèvement et l'analyse d'ADN et d'empreintes digitales, l'observation (y compris la surveillance systématique par des détectives privés), les enregistrements vidéo par la police, la mise en place d'un IMSI-catcher et la recherche en ligne protégée par mot de passe ou la saisie de messages échangés par chat. 33

En ce qui concerne la surveillance automatisée de la circulation, le Tribunal fédéral a déclaré une fois que la protection de la sphère privée ne se limitait pas aux locaux privés, mais s'étendait également au domaine public privé ; l'art. 13 Cst. couvre également les faits de la vie ayant un contenu personnel qui se produisent dans l'espace public. Avec la Cour constitutionnelle fédérale allemande, l'accès aux "contenus de communication et informations disponibles sur Internet, qui s'adresse à tout le monde ou du moins à un cercle de personnes non délimité", ne peut pas encore être caractérisé, à juste titre, comme une atteinte au droit à l'autodétermination en matière d'information. Les contenus qui, sur les blogs, les forums ou les médias sociaux, sont réservés à un certain cercle d'utilisateurs et s'adressent donc à un environnement marqué par des relations personnelles ou une confiance particulière, relèvent de la sphère privée au sens de l'art. 13 al. 1 Cst. et leur consultation doit être considérée comme une atteinte aux droits fondamentaux. Les données qui sont accessibles à tout utilisateur d'Internet sans condition préalable ou qui peuvent être consultées par tous les utilisateurs enregistrés sur une plate-forme (indépendamment d'une relation de proximité avec la personne qui fournit les informations) ne peuvent plus être considérées comme "privées", quel que soit leur contenu. Les informations qui sont déjà connues du public ne présentent plus, à juste titre, 34

d'intérêt digne de protection (à l'exception du "droit à l'oubli" en matière de protection des données).

35 Si l'accès à des données accessibles à tous n'est pas une mesure de contrainte, cela signifie en même temps que l'art. 32 let. a CCC n'est pas de nature constitutive, mais purement déclaratoire : si l'accès à des sources publiques ne viole pas la souveraineté de l'État en l'absence d'exercice d'une contrainte proprement dite, il n'est pas non plus nécessaire de conclure un accord interétatique. Par conséquent, les données accessibles au public provenant d'États tiers qui n'ont pas ratifié la CCC peuvent également être consultées sans problème. Ce dernier point est parfois justifié par le fait que l'accès transnational aux "open source data" relève du droit international coutumier, de tels actes d'enquête étant considérés comme incontestés.

36 Même si l'on ne suivait pas ce raisonnement dans l'absolu, l'interception de données volontairement divulguées - par exemple des contenus de communication dans les médias sociaux - ne pourrait en tout cas pas être caractérisée comme une atteinte aux droits fondamentaux. En effet, en décidant délibérément de partager des informations personnelles, les personnes concernées renoncent à leur autodétermination en matière d'information en ce qui concerne ces données spécifiques ou, en d'autres termes, elles ont précisément exercé leur autodétermination en matière d'information en les mettant à disposition dans le domaine public. Il en va de même pour les traces de données publiques laissées par des apports personnels, comme les transactions effectuées avec le bitcoin, qui peuvent être retracées sur la chaîne de blocs publique. Par ailleurs, les données qui ne peuvent pas être directement attribuées à une personne déterminée ne sont pas protégées par les droits fondamentaux. Il s'agit par exemple de l'utilisation de "Google Earth" ou de données techniques divulguées par un serveur web. Par conséquent, la collecte et l'analyse d'informations personnelles non divulguées volontairement peuvent être considérées comme des mesures de contrainte ; dans ce cas, on pourrait légitimement faire valoir que les personnes concernées n'ont aucun contrôle sur les informations les concernant qui sont disponibles sur Internet. Toutefois, même dans ce cas, il faudrait tenir compte du fait qu'OSINT est une intervention relativement peu invasive et donc proportionnée, puisqu'elle se limite aux informations qui peuvent être consultées par tout un chacun sans restriction d'accès spécifique.

C. Conditions d'un accès autorisé aux données selon le droit de procédure pénale suisse

L'accès à des données "open source" est autorisé pour n'importe quelle infraction (crime, délit ou contravention), dans la mesure où la collecte de preuves disponibles sous forme électronique est utile à leur poursuite (cf. art. 25 al. 1 et art. 14 al. 2 let. c CCC). Dans la mesure où le droit cantonal en matière de police le permet, il est également possible d'accéder à des informations publiques dans le cadre d'une activité policière préventive. 37

En raison de l'absence d'atteinte aux droits fondamentaux, les enquêtes "open source" ne doivent pas être considérées comme des mesures de contrainte au sens des art. 196 ss CPP (cf. supra, n. 32 ss). En conséquence, ni les dispositions formelles et matérielles relatives à la perquisition (art. 246 ss CPP) ni celles relatives au séquestre (art. 263 CPP) ne sont applicables. "OSINF" ou "OSINT" est plutôt considéré comme une collecte de preuves autorisée sur la base de l'art. 95 CPP au sens de l'art. 139 al. 1 CPP. 38

Le fait que des membres des autorités de poursuite pénale se connectent sous une fausse identité dans les médias sociaux ou dans un chat pour avoir accès aux contenus qui y sont publiés ne doit pas être considéré comme une recherche secrète (art. 298a CPP) ou une investigation secrète (art. 285a CPP), car aucun contact direct n'est établi avec la personne visée. Il en irait autrement si l'enquêteur envoyait activement une demande d'amitié ou autre à la personne visée afin de pouvoir également prendre connaissance de ses contributions (privées) ou s'il obtenait frauduleusement l'accès à un chat ou à un forum non accessible à tous en créant une légende. 39

La valeur probante des données disponibles publiquement doit être examinée en détail dans le cadre de la libre appréciation des preuves (art. 10 al. 2 CPP). Diverses considérations jouent un rôle à cet égard, en premier lieu l'origine de la preuve, son authenticité et sa fiabilité, le rapport de son auteur avec les parties à la procédure, mais aussi et surtout le fait que la source soit anonyme ou connue, d'autant plus que les doutes sont grands en cas d'origine inconnue et que les données sont relativement faciles à manipuler. Il est également important que les données soient sécurisées selon l'état actuel de la technique, car les métadonnées permettent de tirer d'éventuelles conclusions sur la valeur probante ; la simple réalisation de captures d'écran ne suffira pas. 40

III. ACCÈS À D'AUTRES DONNÉES STOCKÉES DANS UN AUTRE ÉTAT CONTRACTANT (LET. B)

A. Consentement légal et volontaire de la personne légalement habilitée à transmettre les données

1. Autorisation de transmission

41 L'article 32 de la CCC ne règle que l'admissibilité de l'accès aux données en droit international ; "les dispositions nationales à l'aune desquelles la transmission de données doit être évaluée, c'est-à-dire selon lesquelles il convient de décider si le consentement à la transmission a été donné légalement par une personne habilitée à le faire, ne sont pas affectées par la convention". Le Conseil de l'Europe a renoncé à définir plus précisément la notion d'autorisation de transmission dans la CCC. Le rapport explicatif précise à cet égard que la personne qui peut donner son consentement "peut varier en fonction des circonstances, de la nature de la personne et du droit applicable concerné".

42 La question de savoir qui est "légalement autorisé à transmettre les données [...]" est déterminée par le droit interne de l'État requérant, c'est-à-dire celui dans lequel l'enquête est menée. Cela semble également judicieux parce qu'une localisation précise des données avant l'accès n'est souvent pas possible, ou pas sans grands efforts. Il serait en outre impraticable et incompatible avec l'idée d'accélération de la CCC d'exiger des autorités suisses qu'elles vérifient la situation d'autorisation pour chaque État contractant séparément avant de pouvoir procéder à une sauvegarde des données.

43 L'autorisation de transmettre des données est nécessaire. Est nécessaire, mais aussi suffisant, le consentement d'une personne légalement autorisée à les divulguer aux autorités de poursuite pénale. L'autorisation peut être de nature légale ou obligatoire.

44 Contrairement au message, l'existence du consentement "d'une personne se trouvant sur le territoire national" n'est pas une condition supplémentaire ; l'art. 32 let. b CCC ne connaît pas de critère restrictif de ce type, qui serait en outre contraire à l'esprit et au but de la convention.

Le rapport explicatif et le message citent comme exemples de personnes susceptibles de donner leur consentement les personnes qui ont stocké leur courrier électronique auprès d'un fournisseur de services dans un autre Etat ou d'autres données à l'étranger. Dans la littérature, le client qui loue l'espace de stockage est désigné comme personne autorisée pour les données stockées sur des serveurs en nuage, la banque pour les données relatives aux transactions financières, l'employeur pour le compte de messagerie professionnel et, pour les personnes morales, les personnes déclarées compétentes en interne, le conseil d'administration (SA) ou la direction (Sàrl) en l'absence de telles réglementations internes ; les administrateurs ou autres personnes autorisées à accéder aux données ne devraient pas avoir cette autorisation. 45

Un aspect qui n'est pas abordé de manière exhaustive dans le Rapport explicatif est la question de savoir si le consentement doit toujours être donné par les personnes concernées (propriétaires des données) ou si l'autorisation d'autres instances qui traitent les données personnelles (en premier lieu le fournisseur de services Internet en tant que détenteur des données) suffit. L'extension aux fournisseurs de services Internet est considérée d'un œil critique, car ces derniers ne feraient qu'exercer la garde des données et ne seraient donc pas en position de pouvoir donner un consentement juridiquement valable. 46

La question du droit de transmission doit être considérée dans le contexte plus large du fait qu'en Suisse, selon la situation juridique actuelle, il n'existe pas de droit similaire à la propriété sur les données : Le droit de propriété selon l'art. 641 CC s'étend uniquement à la "chose", par laquelle la doctrine entend "un objet corporel, distinct des autres et susceptible d'être maîtrisé en fait et en droit". Les données étant des biens immatériels, il n'est pas possible de créer une propriété au sens de l'art. 641 CC (mais il est possible de créer une propriété sur des installations de traitement de données ou des supports de données). De même, le droit d'auteur s'étend uniquement aux créations intellectuelles à caractère individuel sous forme de données et ne s'applique qu'exceptionnellement. Le droit de la protection des données reconnaît néanmoins un droit d'accès aux données, en tout cas en ce qui concerne les données personnelles, pour lesquelles l'art. 25 de la loi fédérale sur la protection des données du 25.9.2020 ("LPD", RS 235.1) prévoit un droit d'accès. L'art. 28 LPD accorde en outre aux personnes concernées, si 47

certaines conditions sont remplies, le droit à la remise et à la transmission de données personnelles (portabilité des données), pour autant qu'elles aient communiqué ces données aux responsables. En outre, les données personnelles "ne peuvent être collectées que dans un but précis et identifiable par la personne concernée ; elles ne peuvent être traitées que de manière compatible avec ce but" (art. 6 al. 3 LPD). La remise de données personnelles aux autorités de poursuite pénale constitue à cet égard une forme de traitement de données (cf. art. 5 let. d LPD). Cela signifie que : La personne autorisée peut consentir à la transmission par la personne traitant les données.

48 C'est pourquoi la Suisse, à l'instar d'autres Etats contractants, admet le consentement des fournisseurs de services Internet comme conséquence de leur relation de droit privé avec la personne concernée, lorsque les fournisseurs de services se sont réservés un droit de transmission aux autorités étrangères de poursuite pénale dans leurs conditions générales d'utilisation ou leurs directives d'utilisation des données. La majorité des fournisseurs de services Internet prévoient dans leurs accords d'utilisation que les données peuvent être transmises non seulement en présence d'une décision judiciaire valable, mais aussi sur simple demande des autorités de poursuite pénale ou que les fournisseurs coopèrent avec les autorités de poursuite pénale. Dans ces cas, la transmission est conforme à la loi.

2. Consentement

49 Le fait qu'un fournisseur d'accès étranger concerné soit en principe autorisé à donner son consentement à une remise directe de données ne suffit pas encore (selon le libellé clair de l'art. 32 let. b CCC) pour un accès transfrontalier : Il convient plutôt d'examiner plus avant si l'autorité de poursuite pénale requérante a obtenu un "consentement légitime et volontaire" juridiquement valable.

50 Comme nous l'avons vu, est habilitée à donner son consentement la personne morale ou la personne physique capable de discernement qui, en vertu d'une autorisation légale ou obligatoire, peut disposer des données et y donner accès à des tiers (cf. également n. 43 ss. ci-dessus). Lorsque plusieurs personnes sont autorisées à transmettre des données, l'autorisation d'une seule personne suffit. Si, par exemple, l'autorisation est donnée par le titulaire du compte, aucun consentement supplémentaire n'est nécessaire de la part de l'entreprise étrangère prestataire de services. Inversement, il suffit que le

fournisseur d'accès étranger transmette les données en se fondant sur une autorisation correspondante du client dans les conditions générales d'utilisation (concernant le consentement par les fournisseurs de services Internet, cf. ci-dessus, n. 46 ss).

Conformément aux principes généraux de la procédure pénale, le consentement peut soit être déclaré expressément (aucune exigence de forme n'est applicable), soit être implicite. Ce dernier cas de figure se produit notamment lorsque la personne sollicitée par les autorités de poursuite pénale - par exemple un fournisseur de services ou le titulaire du compte concerné - fournit les données sur demande. 51

Cela signifie en même temps que des "demandes d'informations" correspondantes peuvent être faites à l'étranger, et ce sans que cela soit qualifié d'acte illicite dans un Etat étranger. Dans la pratique, les demandes directes aux fournisseurs d'accès étrangers sont devenues un standard international, qui peuvent soit être saisies sur des portails de poursuite pénale exploités par les fournisseurs d'accès, soit, dans le cas d'autres fournisseurs d'accès (plus petits), être transmises par la voie policière (via Interpol). Divers accords internationaux autorisent en outre la notification directe de documents officiels à l'étranger, du moins en principe, à commencer par l'art. 52 al. 1 de la Convention d'application de l'accord de Schengen du 19.6.1990 ("CAAS"). Or, cette disposition prévoit que chaque État peut ou doit faire une déclaration sur les documents qui peuvent être envoyés aux personnes se trouvant sur son territoire. Il convient donc en principe d'examiner séparément pour chaque État contractant si et, dans l'affirmative, dans quelle mesure une notification directe est autorisée. Dans la mesure où les destinataires sont informés que toute coopération est volontaire et qu'aucune conséquence négative directe n'est liée à un refus de coopération, on ne voit pas dans quelle mesure on peut y voir une violation de la souveraineté territoriale étrangère et donc un cas d'application de l'article 52, al. 1, CAAS - il s'agit de simples invitations sans menace de contrainte et sans conséquences négatives liées à un éventuel refus de coopération. Il ne serait guère judicieux que la réglementation d'exception de l'art. 32 let. b CCC permette d'accroître l'efficacité de la difficile voie de l'entraide judiciaire formelle, mais que celle-ci soit en même temps torpillée par l'exigence de devoir clarifier, par cette même voie de l'entraide judiciaire formelle, la disposition des personnes 52

concernées à coopérer volontairement. L'article 32, let. b, de la CCC prime sur l'article 52 de la CAAS.

53 Le consentement doit être libre ; la personne concernée ne doit pas être trompée ou contrainte à fournir des données. Il existe certes souvent une situation de pression indirecte, car le ministère public pourrait, en cas de refus, exiger la saisie et la transmission des données concernées dans le cadre de l'entraide judiciaire. Cela ne suffit toutefois pas à entraver la formation de la volonté. Il en va de même, par exemple, dans le cas d'une situation de détention où le prévenu pourrait se sentir subjectivement contraint, en raison des circonstances, de coopérer et de mettre à disposition les données enregistrées à l'étranger afin d'être libéré le plus rapidement possible de sa détention. Toutefois, même une telle situation de pression générale ne l'empêche pas de donner un consentement conforme à la loi. En revanche, la menace concrète d'éventuels autres inconvénients est interdite. De même, une personne domiciliée en Suisse ne peut pas être contrainte, sous la menace, de produire des données enregistrées à l'étranger auxquelles elle a accès. Elle peut toutefois être invitée à le faire par une ordonnance de production (art. 265 CPP).

54 Enfin, le consentement peut être révoqué à tout moment, la révocation n'étant valable qu'ex nunc. Une révocation après la sauvegarde des données n'est donc pas pertinente.

B. Conséquence d'un consentement juridiquement valable

55 Si la personne habilitée à disposer de ses données de connexion à des services Internet étrangers dérivés les divulgue volontairement ou consent à une perquisition en ligne, les autorités de poursuite pénale ont la possibilité, en application de l'art. 32 let. b CCC, d'accéder directement aux informations en utilisant les données d'accès et de les saisir. De même, toute personne privée est libre de mettre à la disposition des autorités de poursuite pénale une copie de ses propres données stockées auprès d'un fournisseur d'accès étranger (par exemple des e-mails ou des messages de chat). Il est également admissible que les autorités de poursuite pénale demandent directement à un fournisseur de services Internet domicilié à l'étranger de leur remettre des données (cf. ci-dessus, n. 48, 51 s.).

C. Conditions d'un accès autorisé aux données selon le droit de procédure pénale suisse

L'accès à des données non publiques en Suisse n'est pas possible sans conditions. S'il s'agit de données relatives au contenu, les données doivent être saisies (par exemple par une ordonnance de production [art. 265 CPP] ou à l'occasion d'une perquisition [art. 244 CPP]), perquisitionnées (art. 246 CPP) et ensuite saisies si elles sont pertinentes pour la preuve (art. 263 CPP). Pour les données relatives au trafic, une collecte rétroactive des données marginales (art. 273 CPP) doit être ordonnée et approuvée par le tribunal des mesures de contrainte (art. 274 CPP). L'art. 32 let. b CCC ne constitue pas une mesure autonome de conservation ou de collecte de preuves qui primerait sur les conditions nationales. Cette disposition règle uniquement le fait qu'il est possible de renoncer à une procédure d'entraide judiciaire en présence d'un consentement juridiquement valable. L'accès aux données, même s'il est transnational, constitue donc une mesure de contrainte nationale qui doit satisfaire aux exigences de la législation nationale. La saisie de données à l'étranger doit donc - en plus du consentement décrit - remplir comme condition nécessaire les mêmes conditions que si les données avaient été enregistrées en Suisse. Une "Information Request" adressée à un fournisseur d'accès à Internet doit donc être qualifiée de décision d'édition au sens de l'art. 265 CPP. 56

Il s'ensuit tout d'abord que l'ouverture d'une enquête pénale au sens de l'art. 309 al. 1 CPP et donc un soupçon suffisant sont en principe présupposés, une procédure pénale qui n'est pas encore formellement ouverte étant automatiquement réputée ouverte par la saisie de données (art. 309 al. 1 let. b CPP). Dans la procédure d'enquête policière indépendante, il n'est pas possible de se fonder sur l'art. 32 let. b CCC. Les services de renseignement ne peuvent pas non plus s'y référer. 57

La CCC sert à recueillir des preuves d'une infraction disponibles sous forme électronique (cf. art. 25 al. 1 et art. 14 al. 2 let. c CCC). Le soupçon suffisant peut donc en principe s'étendre à n'importe quelle infraction, pour autant qu'il existe au moins le soupçon criminologique que celle-ci a été commise avec un moyen technique. La gravité de l'infraction n'a pas d'importance : l'accès transnational aux données est en principe ouvert aux crimes, aux délits 58

et aux contraventions (dans les cas mineurs, la proportionnalité de l'accès aux données peut toutefois être discutée).

59 Pour saisir des données de contenu, il faut qu'il y ait lieu de supposer qu'elles contiennent des informations susceptibles d'être saisies (art. 246 CPP). Selon l'art. 263 al. 1 let. a CPP, les objets appartenant à un prévenu ou à un tiers peuvent être saisis, notamment s'ils sont utilisés comme moyens de preuve. Pour la saisie et la perquisition d'enregistrements, il suffit donc d'une pertinence potentielle des preuves, qui est donnée lorsque les données "peuvent être importantes" pour l'élucidation des infractions reprochées ou qu'elles ne semblent pas "manifestement inappropriées". La jurisprudence n'est pas très exigeante à cet égard. Enfin, la saisie et la perquisition doivent être proportionnées (art. 197 al. 1 let. c et d CPP) et donc appropriées, nécessaires et adéquates. La proportionnalité peut être discutable, notamment dans le cadre de la poursuite de contraventions. D'un point de vue formel, la saisie et la perquisition doivent en règle générale être ordonnées par le ministère public dans un ordre écrit (art. 241 al. 1 CPP). En revanche, pour la collecte de données de stock, la seule condition est qu'il existe un soupçon qu'une infraction a été commise via Internet (art. 22, al. 1, de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication du 18.3.2016 ["LSCPT" ; RS 780.1]).

60 Si l'historique/les données log IP ou d'autres données marginales sont collectées à l'étranger, la question se pose de savoir si le ministère public peut rendre ces enregistrements disponibles de sa propre compétence ou si une autorisation doit être demandée au tribunal des mesures de contrainte en application de l'art. 273 al. 2 CPP. Le Tribunal fédéral a un jour retenu que l'art. 273 CPP ne permettait qu'une collecte rétroactive des données marginales de la correspondance par télécommunication "à l'égard des fournisseurs de services de télécommunication ou des fournisseurs d'accès à Internet soumis au droit suisse et domiciliés en Suisse". Il a ainsi exclu son applicabilité aux situations internationales, avec pour conséquence que la collecte ne devrait pas nécessiter l'autorisation du tribunal des mesures de contrainte ; en d'autres termes, l'art. 32 let. b CCC "permet un échange international facilité de données marginales". Dans un autre arrêt, le Tribunal fédéral a toutefois rejeté une demande d'autorisation du ministère public au motif que les conditions de l'art. 32 let. b CCC n'étaient pas remplies en l'espèce, ajoutant que l'accès transfrontalier direct aurait dû être autorisé par

le tribunal des mesures de contrainte conformément à l'art. 273 CPP. Plus encore, il a expressément constaté dans un autre jugement que même les historiques IP consultés auprès de fournisseurs étrangers devaient être soumis à l'autorisation du tribunal des mesures de contrainte et que, comme cela n'avait pas été fait dans le cas concret, les informations issues de ces consultations étaient absolument inutilisables. Le fait que le Tribunal fédéral se soit penché ici sur l'art. 273 CPP peut sembler compréhensible à première vue si l'on considère la nature juridique de l'art. 32 let. b CCC, qui déclare uniquement que l'accès transnational est autorisé par le droit international public, mais qui ne touche pas aux dispositions nationales, précisément en ce qui concerne la compétence de collecter des données. Il faut toutefois tenir compte du fait que les dispositions relatives à la collecte rétroactive de données secondaires ne sont pas activées uniquement par le type de données à collecter (données relatives au trafic ou données secondaires), mais que les données doivent être collectées auprès d'un fournisseur de télécommunications ou être protégées par le secret des télécommunications (art. 321ter CP et art. 43 de la loi sur les télécommunications du 30.4.1997 ["LTC" ; RS 784.10]). Le secret des télécommunications ne s'applique toutefois (dans la mesure où cela nous intéresse ici) qu'aux fournisseurs qui proposent un accès à Internet ou une transmission par télécommunication. Les fournisseurs de services Internet ou les fournisseurs de services de communication dérivés qui n'offrent pas d'accès à Internet, mais uniquement des services fournis via Internet ("over-the-top services"), ne sont pas considérés comme des fournisseurs de télécommunications. C'est pourquoi la saisie de données secondaires auprès de telles entreprises n'est pas soumise à autorisation, ni en Suisse ni à l'étranger. Au contraire, une décision d'édition à l'attention du fournisseur de services Internet est suffisante (art. 265 CPP). Par conséquent, si des historiques IP et d'autres données secondaires sont collectés à l'étranger sur la base de l'art. 32 let. b CCC auprès de fournisseurs de services autres que de télécommunication, il n'est pas nécessaire de demander l'autorisation du tribunal des mesures de contrainte.

La question se pose enfin de savoir dans quelle mesure les autres conditions de l'entraide judiciaire, notamment les motifs de refus et la nécessité d'une double incrimination, s'appliquent également à l'art. 32 let. b CCC. L'art. 25 al. 4 CCC prévoit, sous le titre 3 ("Principes généraux de l'entraide judiciaire"), que, sauf disposition contraire expresse de la CCC, "l'entraide judiciaire est soumise aux conditions prévues par le droit de la Partie requise ou par les 61

traités d'entraide judiciaire applicables, y compris les motifs pour lesquels la Partie requise peut refuser de coopérer". Or, l'art. 32 let. b CCC permet un accès direct avant l'entraide judiciaire ; une "demande" à l'autre Etat contractant, telle que celle qui est à la base de l'art. 25 al. 4 CCC, n'est justement pas nécessaire ici. L'accès volontaire ne requiert donc pas de double incrimination et ne nécessite pas le respect d'autres conditions qui s'appliqueraient autrement dans la procédure d'entraide judiciaire. Cet assouplissement se justifie d'une part par le caractère volontaire des personnes qui donnent leur consentement et d'autre part par la nature juridique de l'art. 32 let. b CCC, qui prolonge le bras territorial des autorités de poursuite pénale, alors qu'il s'agit toujours d'une mesure nationale de conservation des preuves. Si la tentative de saisie des enregistrements sur la base de l'art. 32 let. b CCC échoue, il faut bien sûr suivre la voie ordinaire de l'entraide judiciaire, pour laquelle les limitations correspondantes s'appliquent à nouveau.

62 La personne concernée ne peut pas s'opposer à la saisie directe en tant que telle ou à la demande du fournisseur d'accès ; elle dispose néanmoins d'un moyen de recours contre la perquisition, à savoir l'apposition de scellés (art. 248 CPP), dans la mesure où elle peut rendre vraisemblable une interdiction de séquestre (art. 264 CPP). L'apposition de scellés a pour effet que les autorités de poursuite pénale ne peuvent provisoirement pas perquisitionner les enregistrements jusqu'à ce que le tribunal des mesures de contrainte se soit prononcé sur l'admissibilité de la collecte des données et de la perquisition.

IV. CONSERVATION DES PREUVES AU-DELÀ DE L'ARTICLE 32 DE LA CCC SELON LE PRINCIPE D'ACCÈS

63 En friction avec le principe de territorialité, qui se fonde sur le lieu de stockage des moyens de preuve et donc, dans le cas des données, sur le lieu physique de stockage, le Tribunal fédéral autorise un accès même en l'absence de consentement, et ce indépendamment de l'endroit où les données sont stockées au moment de l'accès ; ce qui est déterminant, c'est que les données puissent être consultées depuis la Suisse : "Celui qui utilise, par le biais d'un accès Internet situé en Suisse, un service Internet dérivé proposé par une entreprise étrangère n'agit pas à l'étranger. Même le simple fait que les données électroniques du service Internet dérivé en question

soient gérées sur des serveurs (ou supports de stockage en nuage) à l'étranger ne permet pas de considérer une recherche en ligne effectuée depuis la Suisse conformément à la loi comme un acte d'instruction illicite sur le territoire étranger (au sens de la pratique exposée) [...]".

L'objet de l'évaluation était l'accès au compte Facebook d'une personne accusée de trafic qualifié de stupéfiants, dont les données d'accès avaient été rendues disponibles par les autorités de poursuite pénale. Le ministère public a alors fait examiner le compte Facebook en utilisant les données de connexion déterminées et a saisi des messages de discussion pertinents pour la preuve. Le lieu de stockage de ces données n'était pas - et n'est toujours pas - situé en Suisse. Dans l'arrêt cité, le Tribunal fédéral a retenu qu'il était possible d'accéder directement aux comptes de prévenus ou de tiers auprès de services Internet étrangers si les conditions générales d'une perquisition selon le CPP suisse sont remplies et si les enquêteurs agissent "à partir d'ordinateurs, de serveurs et d'infrastructures informatiques situés en Suisse", c'est-à-dire s'ils restent physiquement en Suisse. 64

La pratique a accueilli cette jurisprudence avec gratitude. Elle ne s'applique pas seulement à Facebook, mais à une multitude de services suisses et étrangers tels que les fournisseurs d'hébergement, les services de communication, les services de cloud computing, les fournisseurs d'externalisation de données, les forums de discussion, les plateformes d'échange de documents, les portails d'achat et les fournisseurs de services de messagerie. Les cryptoactifs détenus dans un hot wallet peuvent également être saisis (c'est-à-dire habituellement transférés sur un wallet de l'autorité de poursuite pénale) en application de cette jurisprudence. La jurisprudence du Tribunal fédéral prend également de plus en plus d'importance. La tendance générale pour les appareils électroniques est l'abandon du stockage individuel au profit de la sauvegarde dans le cloud. Aujourd'hui, les téléphones portables en particulier sont souvent utilisés par les utilisateurs pour différents services uniquement comme "clés", les données concernées n'étant plus stockées sur l'appareil physique. Si un téléphone portable ou une tablette est saisi lors d'une perquisition ou d'une arrestation par la police et qu'il s'avère que les données ne sont pas stockées sur l'appareil, mais dans le cloud, ou si des applications de services de communication ou de fournisseurs de messagerie web se trouvent sur l'appareil, toutes ces données peuvent être saisies sur la base de la jurisprudence du Tribunal fédéral. Cette procédure est facilitée 65

dans la pratique par le fait que les utilisateurs, pour des raisons de commodité, enregistrent souvent leurs données de connexion aux services Internet dans le gestionnaire de mots de passe ou dans un navigateur Internet, ou utilisent le même mot de passe pour différents services. De même, lors de perquisitions dans des entreprises, on constate de plus en plus souvent que celles-ci n'hébergent ou ne stockent plus elles-mêmes leurs données au siège ou au lieu de la direction, mais qu'elles ont externalisé le traitement et la conservation des données à des prestataires de services externes. Dans de telles situations, l'arrêt du Tribunal fédéral cité est également utile, car il autorise également la sauvegarde des données dans de tels cas.

66 Dans l'arrêt cité, le Tribunal fédéral a implicitement invoqué le "principe d'accès". Selon ce principe, pour les données informatiques, on ne se base pas sur l'emplacement du support de données sur lequel les informations sont enregistrées, mais sur la personne qui a accès aux données importantes pour la procédure et à partir de quel endroit. La maîtrise des données revient à la personne qui dispose de l'autorisation d'accès et non à celle qui est physiquement en possession du support de données. C'est ce qu'avancent certains auteurs pour justifier le fait que la perquisition et la saisie en Suisse de données enregistrées à l'étranger par les autorités suisses ne constituent pas une violation de la souveraineté. En d'autres termes, l'admissibilité de l'accès en ligne doit dépendre uniquement de la légalité de l'acte d'enquête national.

67 Or, si l'on accède à des sources étrangères non accessibles au public, notamment protégées par un mot de passe ou par d'autres barrières, cela a des répercussions importantes sur le territoire étranger ("numérique"). C'est pourquoi l'accès par les autorités d'enquête à des données à l'étranger est considéré à plusieurs reprises comme une atteinte à la souveraineté de l'État concerné ; de tels moyens de preuve ne peuvent être obtenus que par le biais de l'entraide judiciaire internationale ou par voie directe, uniquement si les conventions internationales le prévoient explicitement. En effet, le principe d'accès ne change rien aux effets des accès en ligne de l'État sur la souveraineté étrangère, où se produit le véritable succès de la mesure. Certes, l'absence d'intervention physique des fonctionnaires sur le territoire étranger ne devrait pas encore dépasser les limites fixées par l'article 299 CP. Toutefois, en ce qui concerne l'intensité de l'intervention, elle ne cède en rien aux activités d'enquête physiques équivalentes (la fouille du support de

données à l'étranger par des fonctionnaires suisses), qui seraient clairement inadmissibles. De plus, la consultation en ligne déclenche des processus de traitement des données à l'étranger ; l'accès laisse des traces compréhensibles dans l'État cible. Le fonctionnaire chargé de l'enquête peut, dans le pire des cas et en fonction de la législation nationale, se rendre coupable d'intrusion non autorisée dans un système de traitement des données, de collecte non autorisée de données ou de non-respect de la souveraineté étrangère. Les enregistrements numériques de preuves effectués depuis la Suisse sont en outre clandestins pour l'État étranger, ce qui les rend encore plus dangereux de son point de vue - au vu des récents scandales des services de renseignement. Il est remarquable que, selon une étude de l'ONU, le droit national de divers Etats autorise malgré tout une sorte d'accès direct aux données enregistrées à l'étranger, alors que, selon la même étude, la part des Etats qui autorisent un tel accès direct par les autorités de poursuite pénale étrangères est nettement plus faible. Le sens du droit international semble donc être plus grand lorsque la souveraineté nationale est en jeu que lorsque l'on dépend soi-même de l'obtention de preuves à l'étranger. Quoi qu'il en soit, la convention sur la cybercriminalité autorise déjà de manière limitée l'accès direct aux données étrangères à l'art. 32 CCC ; une collecte de preuves allant au-delà - du moins dans les relations entre les États signataires - doit être considérée a contrario comme une atteinte à la souveraineté de l'État. Ce n'est pas pour rien que le Conseil de l'Europe a expressément prévu l'article 31 CCC subsidiaire intitulé "Entraide judiciaire pour l'accès aux données enregistrées". Une proposition présentée par des États membres de l'UE dans le cadre des négociations, selon laquelle une perquisition en ligne transnationale devrait être autorisée en cas d'urgence, n'a pas été reprise - on a renoncé à régler de telles situations faute de consensus. Les efforts repris depuis lors sont restés largement infructueux jusqu'à présent ; le 2e protocole additionnel à la CCC n'est pas non plus un grand succès à cet égard. L'accès transnational direct aux données sans le consentement d'une personne autorisée n'est donc toujours pas couvert par un consensus international, viole la souveraineté de l'État concerné et est donc contraire au droit international tant que les conventions bi- ou multilatérales actuelles n'ont pas évolué.

Ce résultat n'est pas satisfaisant. Premièrement, précisément lorsqu'il existe 68
un risque de perte des données sans action immédiate. Il est donc envisageable, dans des situations exceptionnelles, d'autoriser la conservation

provisoire de données au niveau transnational en cas de risque de collusion ou de perte de preuves, lorsque même une "Preservation Request" au sens de l'article 29 CCC interviendrait trop tard. Dans ce cas, les données sauvegardées devraient être conservées séparément et ne pourraient pas encore être fouillées tant que l'État contractant concerné n'aurait pas demandé une autorisation ultérieure. Deuxièmement, la critique ci-dessus part du principe qu'au moment de l'accès, les autorités de poursuite pénale ont une connaissance positive du fait que les données ne sont pas stockées dans leur propre pays. Or, il n'est souvent pas clair d'emblée où les données sont stockées, que ce soit localement sur l'appareil ou dans le nuage. Dans ces cas également, une conservation des preuves, éventuellement suivie d'une demande d'entraide judiciaire en cas de lien avec l'étranger constaté a posteriori, doit être autorisée (cf. ci-dessus, n. 23).

V. CONSÉQUENCES DE LA VIOLATION DU DROIT À LA SOUVERAINETÉ ÉTRANGÈRE

69 Si les compétences de la CCC sont outrepassées, si l'entraide judiciaire en matière pénale est contournée par l'accès direct à des supports de données étrangers et si le principe de territorialité ou de souveraineté est ainsi violé, la question de l'inexploitabilité des moyens de preuve ainsi obtenus se pose. Le contournement de la voie de l'entraide judiciaire peut en principe être dénoncé dans le cadre du procès pénal national.

70 Jusqu'à présent, les tribunaux cantonaux se sont prononcés en faveur d'une interdiction relative d'exploitation au sens de l'art. 141 al. 2 CPP, ce qui permet d'exploiter les preuves concernées dans la mesure où elles sont nécessaires pour élucider une infraction grave. On peut se demander si le principe de territorialité du droit international public et l'exigence d'emprunter la voie de l'entraide judiciaire doivent être considérés comme de simples règles de validité ou si, au vu de leur importance, il ne faut pas plutôt partir du principe d'une interdiction absolue d'exploiter les preuves (par exemple sous la forme d'une violation de l'ordre public). Le Tribunal fédéral a statué dans ce sens lorsqu'il a considéré qu'une mesure de surveillance secrète (tracker GPS et appareils d'écoute dans un véhicule avec lequel des trajets à l'étranger avaient également été effectués) était absolument inexploitable en ce qui concerne les trajets à l'étranger. Il semble toutefois possible et judicieux de reprendre le point de vue défendu en Allemagne, selon lequel la question de l'exploitabilité

dépend du fait de savoir si l'enquêteur s'est rendu compte, au moment de la collecte des données, que l'accès ne serait pas conforme au droit international. S'il n'en était pas conscient, il doit avoir la possibilité de faire exécuter une procédure formelle d'entraide judiciaire ultérieure (au sens d'une procédure d'autorisation) pour les moyens de preuve (obtenus objectivement de manière illégale), afin d'éviter l'inutilisabilité des preuves.

Cette dernière disposition s'applique notamment aux cas où l'on ne sait pas d'emblée où les données sont stockées : Si un lieu de stockage sur le territoire national ne peut être exclu, l'accès doit être autorisé pour la conservation des preuves ; une connaissance positive du lieu de stockage n'est pas une condition préalable. "La seule possibilité d'un emplacement à l'étranger ne peut pas déclencher une obligation d'entraide judiciaire, d'autant plus que dans ces cas, il n'est pas possible de déterminer quel pays sera réellement concerné". S'il devait s'avérer par la suite (par exemple suite à des plaintes de la défense) que les données saisies n'étaient pas stockées sur le territoire national ni dans un État contractant, une autorisation ultérieure devra être demandée à l'État concerné par le biais de l'entraide judiciaire. 71

VI. NÉCESSITÉ D'UNE RÉFORME

Le Conseil de l'Europe a reconnu très tôt la nécessité d'assouplir les principes territoriaux en raison de l'évolution technologique et a édicté à l'article 32 CCC une réglementation progressiste par rapport aux conventions d'entraide judiciaire traditionnelles. Les idées poursuivies plus loin étaient aussi visionnaires qu'elles n'étaient pas (encore) susceptibles de réunir une majorité en raison de l'idée de souveraineté fortement ancrée. Si la communauté internationale souhaite une poursuite pénale efficace, capable d'assumer ses tâches au 21e siècle également, il semble nécessaire et judicieux de renoncer entièrement à la souveraineté en matière de données en réseau. En effet, il ne s'agit plus seulement de la criminalité transfrontalière, qui a toujours été difficile à appréhender pour les autorités nationales de poursuite pénale, mais aussi de faits purement internes qui, en raison du déplacement des moyens de preuve au-delà des frontières nationales, ne pourront bientôt plus être élucidés, et encore moins avec un rapport coût-utilité approprié. 72

Il faut admettre qu'il semble plus prometteur de cuire des petits pains dans un premier temps : premièrement, la Suisse doit signer et ratifier le 2e protocole additionnel à la CCC le plus rapidement possible, même s'il ne s'agit pas d'un 73

grand projet. Deuxièmement, on aurait déjà fait beaucoup si, dans le contexte de l'art. 32 let. b CCC, on suivait la réalité juridique et si l'on ne se référait plus seulement au lieu de stockage, mais plutôt (aussi) au siège de la personne ayant un droit d'accès ou au fait qu'une entreprise offre ses services dans l'Etat concerné (cf. ci-dessus, n. 25). Troisièmement, la Suisse devrait s'efforcer de s'associer au système e-Evidence de l'UE (même si cela sera politiquement difficile à mettre en œuvre). Quatrièmement, les discussions récurrentes sur l'accès unilatéral aux données à l'étranger doivent être reprises et menées à terme. A l'avenir, il faudrait au moins considérer qu'un lieu d'accès en Suisse est suffisant pour que l'accès aux données ne soit plus considéré comme une atteinte à la souveraineté de l'Etat du lieu de stockage. Des mesures de protection et des garanties (p. ex. une obligation d'informer l'État concerné de l'accès, la nécessité d'une autorisation a posteriori, des exigences en matière d'État de droit et de respect des droits fondamentaux, etc.

BIBLIOGRAPHIE

Abo Youssef Omar, Smartphone-User zwischen unbegrenzten Möglichkeiten und Überwachung, ZStrR 130 (2012), S. 92 ff.

Aepli Michael, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Unter besonderer Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich, Zürich 2004.

Bangerter Simon, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht unter vergleichender Berücksichtigung der StPO, Zürich 2014.

Bär Wolfgang, Transnationaler Zugriff auf Computerdaten, ZIS 2 (2011), S. 53 ff., abrufbar unter https://www.zis-online.com/dat/artikel/2011_2_525.pdf, besucht am 17.10.2023.

Biaggini Elena, Strafrechtlicher Schutz des E-Mail-Verkehrs post mortem?, sui generis 2021, S. 321 ff., abrufbar unter https://doi.org/10.21257/sg.196, besucht am 17.10.2023.

Bonnici Jeanne Pia Mifsud et al., The European Legal Framework on Electronic Evidence: Complex and in Need of Reform, in: Biasiotti Maria Angela/Bonnici Jeanne Pia Mifsud/Cannataci Joe/Turchi Fabrizio (Hrsg.),

Handling and Exchanging Electronic Evidence Across Europe, 2018, S. 189 ff., abrufbar unter https://link.springer.com/chapter/10.1007/978-3-319-74872-6_11, besucht am 17.10.2023.

Bottinelli Nicolas, L'obtention par l'autorité pénale des données informatiques situées à l'étranger, AJP 2016, S. 1327 ff.

Brodowski Dominik, Der «Grundsatz der Verfügbarkeit» von Daten zwischen Staat und Unternehmen, ZIS 8-9/2012, S. 474 ff., abrufbar unter https://zis-online.com/dat/artikel/2012_8-9_703.pdf, besucht am 17.10.2023.

Brodowski Dominik/Eisenmenger Florian, Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden, Sachliche und zeitliche Reichweite der «kleinen Online-Durchsuchung» nach § 110 Abs. 3 StPO, ZD 2014, S. 119 ff.

Burgermeister Daniel, Beweiserhebung in der Cloud, Luzern 2015, abrufbar unter https://www.unilu.ch/fileadmin/fakultaeten/rf/institute/staak/MAS_Forensics/dok/Masterarbeiten_MAS_5/Burgermeister_Daniel.pdf, besucht am 17.10.2023.

Capus Nadja, Strafrecht und Souveränität: Das Erfordernis der beidseitigen Strafbarkeit in der internationalen Rechtshilfe in Strafsachen, Basel 2010.

Cartner Anna/Schweingruber Sandra, Strafbehörden dürfen googeln, AJP 2021, S. 990 ff.

De Busser Els, Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You, Groningen Journal of International Law 2/2 (2014): Privacy in International Law, S. 90 ff., abrufbar unter https://www.researchgate.net/publication/328962642_Open_Source_Data_and_Criminal_Investigations_Anything_You_Publish_Can_and_Will_Be_Used_Against_You, besucht am 17.10.2023.

Dombrowski Nadine, Extraterritoriale Strafrechtsanwendung im Internet, Potsdam 2011/2012.

Donatsch Andreas/Lieber Viktor/Summers Sarah/Wohlers Wolfgang (Hrsg.), Schulthess Kommentar zur Schweizerischen Strafprozessordnung, 3. Aufl., Zürich 2020 (zit. SK-Bearbeiter/in, Art. ... StPO N. ...).

Eckert Martin, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 112 (2016), S. 245 ff.

Forster Marc, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schindler Benjamin/Wildhaber Isabelle (Hrsg.), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, S. 613 ff.

Fröhlich-Bleuler Gianni, Eigentum an Daten?, Jusletter 6.3.2017.

Geiser Thomas/Wolf Stephan (Hrsg.), Basler Kommentar zum Zivilgesetzbuch II, Art. 457-977 ZGB, Art. 1-61 SchlT ZGB, 7. Aufl., Basel 2023 (zit. BSK-Bearbeiter/in, Art. ... ZGB N. ...).

Gercke Björn, Straftaten und Strafverfolgung im Internet, GA 2012, S. 474 ff.

Glassey Ludwiczak Maria, Mesures de surveillance suisses et résultats obtenus à l'étranger, Remarques à propos de l'ATF 146 IV 36, forumpoenale 5 (2020), S. 410 ff.

Gless Sabine, Beweisverbote in Fällen mit Auslandsbezug, JR 2008, S. 317 ff.

Graf Damian K. (Hrsg.), Annotierter Kommentar zum Schweizerischen Strafgesetzbuch, Bern 2020 (zit. AK-Bearbeiter/in, Art. ... StGB N. ...).

Graf Damian K., Praxishandbuch zur Siegelung, StPO inklusive revidierter Bestimmungen – VStrR – IRSG – MStP, Bern 2022 (zit. Praxishandbuch).

Graf Damian K., Strafverfolgung 2.0: Direkter Zugriff auf im Ausland gespeicherte Daten?, Jusletter IT 21.9.2017 (zit. Strafverfolgung 2.0).

Graf Jürgen-Peter (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 47. Edition, München, Stand: 1.1.2023 (zit. BeckOK-Bearbeiter/in, § ... StPO N. ...).

Grassle Christian/Hiéramente Mayeul, Praxisprobleme bei der IT-Durchsuchung, CB 2019, S. 191 ff.

Grave Carsten/Barth Christoph, Von «Dawn Raids» zu «eRaids», Zu den Befugnissen der Europäischen Kommission bei der Durchsuchung elektronischer Daten, EuZW 2013, S. 360 ff.

Hansjakob Thomas, Die Erhebung von Daten des Internetverkehrs – Bemerkungen zu BGer 6B_656/2015 vom 16.12.2016, forumpoenale 4 (2017), S. 252 ff.

Heimgartner Stefan, Die internationale Dimension von Internetstraffällen, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 117 ff. (zit. Internationale Dimension).

Heimgartner Stefan, Strafprozessuale Beschlagnahme, Wesen, Arten und Wirkungen, Zürich 2011 (zit. Strafprozessuale Beschlagnahme).

Hess-Odoni Urs, Die Herrschaftsrechte an Daten, Jusletter 17.5.2004.

Hiatt Keith, Open Source Evidence on Trial, 125 Yale Law Journal Forum (2016), S. 323 ff., abrufbar unter https://www.yalelawjournal.org/pdf/Hiatt_PDF_zxz3ufoz.pdf, besucht am 17.10.2023.

Hürlimann Daniel/Zech Herbert, Rechte an Daten, sui-generis 2016, S. 89 ff., abrufbar unter https://doi.org/10.21257/sg.27, besucht am 17.10.2023.

Karagiannis Christos/Vergidis Kostas, Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal, Information 12 (2021), 181, S. 1 ff., abrufbar unter https://www.mdpi.com/2078-2489/12/5/181, besucht am 17.10.2023.

Knauer Christoph/Kudlich Hans/Schneider Hartmut (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Band 1: §§ 1-150 StPO, 2. Aufl., München 2022 (zit. MK-Bearbeiter/in, § ... StPO N. ...).

Kohler Patrick, Rechte an Sachdaten, sic! 2020, S. 412 ff.

Largiadèr Albert, Vorladungen ins Ausland nur Einladungen?, forumpoenale 5 (2014), S. 293 f.

Marberth-Kubicki Annette, in: Auer-Reinsdorff Astrid/Conrad Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl., München 2016.

Moreillon Laurent/Parein-Reymond Aude, Petit commentaire du Code de procédure pénale, 2. Aufl., Basel 2016.

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar zum Strafrecht II, 4. Aufl., Basel 2019 (zit. BSK-Bearbeiter/in, Art. ... StGB N. ...).

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar zur Strafprozessordnung/Jugendstrafprozessordnung, 3. Aufl., Basel 2023 (zit. BSK-Bearbeiter/in, Art. ... StPO N. ...).

Obenhaus Nils, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2010, S. 651 ff.

Osula Anna-Maria, Remote search and seizure in domestic criminal procedure: Estonian case study, International Journal of Law and Information Technology 24 (2016), S. 343 ff.

Pfeffer Kristin, Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln, abrufbar unter https://eucrim.eu/articles/die-regulierung-des-grenzuberschreitenden-zugangs-zu-elektronischen-beweismitteln/, besucht am 17.10.2023.

Riedi Claudio, Auslandsbeweise und ihre Verwertung im schweizerischen Strafverfahren, Zürich 2018.

Roth Simon, Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess, Direkter Zugriff oder Rechtshilfe?, Jusletter 17.8.2015.

Ryser Dominic, «Computer Forensics», Eine neue Herausforderung für das Strafprozessrecht, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 553 ff.

Sampson Fraser, Intelligence evidence: Using open source intelligence (OSINT) in criminal proceedings, The Police Journal 90(1) 2017, S. 55 ff.

Schmid Alain/Schmidt Kirsten Johanna/Zech Herbert (Hrsg.), Rechte an Daten – zum Stand der Diskussion, sic! 11/2018, S. 627 ff.

Schmid Niklaus, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im allgemeinen, ZStrR 111 (1993), S. 81 ff.

Schomburg Wolfgang/Lagodny Otto (Hrsg.), Internationale Rechtshilfe in Strafsachen, Beck'scher Kurz-Kommentar, 6. Aufl., München 2020 (zit. Schomburg/Lagodny-Bearbeiter/in).

Schweingruber Sandra, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, Jusletter 10.11.2014.

Seger Alexander, «Grenzüberschreitender» Zugriff auf Daten im Rahmen der Budapest Konvention über Computerkriminalität, Praxisbericht zum Stand der Arbeiten des Europarats, Zeitschrift für öffentliches Recht 73 (2018), S. 71 ff.

Seitz Nicolai, Transborder Search: A New Perspective in Law Enforcement?, Yale Journal of Law & Technology 2004-2005, S. 24 ff., abrufbar unter https://yjolt.org/transborder-search-new-perspective-law-enforcement, besucht am 17.10.2023.

Singelnstein Tobias, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmassnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co., NStZ 2012, S. 593 ff.

Svantesson Dan, Preliminary Report: Law Enforcement Cross-Border Access to Data, 12.11.2016, abrufbar unter https://ssrn.com/abstract=2874238, besucht am 17.10.2023.

Unseld Lea, Internationale Rechtshilfe im Steuerrecht, Akzessorische Rechtshilfe, Auslieferung und Vollstreckungshilfe bei Fiskaldelikten, Zürich 2011.

Velasco Cristos, Cybercrime jurisdiction: past, present, future, ERA Forum (2015) 16, S. 331 ff., abrufbar unter https://rm.coe.int/16806b8a7a, besucht am 17.10.2023.

Wabnitz Heinz-Bernd/Janovsky Thomas (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl., München 2014 (zit. Wabnitz/Janovsky-Bearbeiter/in).

Walden Ian, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, Queen Mary School of Law Legal Studies Research Paper No. 7 (2011), abrufbar unter https://papers.ssrn.com/abstract=1781067, besucht am 17.10.2023.

Walder Stephan, Grenzüberschreitende Datenerhebung: Ist und Soll, Kriminalistik 8-9/2019, S. 540 ff.

Weber Amalie M., The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal 18 (2003), S. 425 ff., abrufbar unter https://lawcat.berkeley.edu/record/1118718, besucht am 17.10.2023.

Wicker Magda, Durchsuchung in der Cloud, Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, S. 765 ff.

Zerbes Ingeborg/El-Ghazi Mohamad, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015, S. 425 ff.

MATÉRIAUX

Botschaft des Bundesrates an die Bundesversammlung zu einem Bundesgesetz über internationale Rechtshilfe in Strafsachen und einem Bundesbeschluss über Vorbehalte zum Europäischen Auslieferungsübereinkommen
vom 8.3.1976, BBl 1976 II 444 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1976/2_444_430_443/de, besucht am 17.10.2023.

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2010/813/de, besucht am 17.10.2023.

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27.2.2013, BBl 2013 2683 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2013/512/de, besucht am 17.10.2023.

Botschaft zur Vereinheitlichung des Strafprozessrechts vom 21.12.2005, BBl 2006 1085 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2006/124/de, besucht am 17.10.2023.

Bundesamt für Justiz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zum erläuternden Bericht und zum Vorentwurf über die Änderung des Schweizerischen Strafgesetzbuches und des Rechtshilfegesetzes, Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, Bern, 10.4.2010, abrufbar unter https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/cybercrime-europarat.html, besucht am 17.10.2023.

Europäische Union, Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the Draft Convention on Cyber Crime held in the Council of Europe, Official Journal of the European Communities, L 142/1 vom 5.6.1999,

abrufbar unter https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1999:142:0001:0002:EN:PDF, besucht am 17.10.2023.

Europarat, Cybercrime Convention Committee (T-CY), The Budapest Convention on Cybercrime: benefits and impact in practice, Strassburg, 13.7.2020, abrufbar unter https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, besucht am 17.10.2023 (zit. T-CY, Benefits).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 3, Transborder access to data (Article 32), Strassburg, 3.12.2014, abrufbar unter https://www.ccdcoe.org/uploads/2019/09/CoE-141203-Guidance-Note-on-Transbprder-access-to-data.pdf, besucht am 17.10.2023 (zit. T-CY Guidance Note # 3).

Europarat, Cybercrime Convention Committee (T-CY), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, Transborder Access and jurisdiction: What are the options?, Strassburg, 6.12.2012, abrufbar unter https://rm.coe.int/16802e79e8, besucht am 17.10.2023 (zit. T-CY, Transborder Access).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report, Strassburg, 16.9.2016, abrufbar unter https://rm.coe.int/16806a495e, besucht am 17.10.2023 (zit. T-CY, Cloud).

Europarat, Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Strassburg, 3.12.2014, abrufbar unter https://rm.coe.int/16802e726c, besucht am 17.10.2023 (zit. T-CY, Assessment Report).

Europarat, Draft Explanatory Memorandum Regarding on Draft Recommendation No. R (95) Concerning Problems of Criminal Procedural Law Connected with Information Technology vom 31.7.1995 (zit. Explanatory Memorandum).

Europarat, Economic Crime Division, Project on Cybercrime, Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?, Discussion Paper, Strassburg, 31.8.2010, abrufbar unter https://rm.coe.int/16802fa3df, besucht am 17.10.2023 (zit. Economic Crime Division).

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, abrufbar unter https://rm.coe.int/16800cce5b, besucht am 17.10.2023 (zit. Explanatory Report).

United Nations, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes vom 21.1.2023, abrufbar unter https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf, besucht am 17.10.2023 (zit. United Nations, Consolidated Negotiating Document).

United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General vom 24.6.2013, UN Doc A/68/98, abrufbar unter https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf, besucht am 17.10.2023 (zit. Developments).

United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, Draft February 2013, abrufbar unter https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, besucht am 17.10.2023 (zit. UNODC).

COMMENTAIRE

Art. 33 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Nicolas Bottinelli / Julien Wenger

PROPOSITION DE CITATION

Nicolas Bottinelli/Julien Wenger, Commentaire de l'art. 33 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Bottinelli/Wenger, art. 33 CCC N. XXX.

Art. 33 Entraide dans la collecte en temps réel de données relatives au trafic

[1] Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du par. 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

[2] Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

TABLE DES MATIÈRES

I. Introduction 305
II. Notions 306
III. Mise en œuvre en droit suisse 310
A. L'art. 18b EIMP 310
1. Historique 310
2. Définitions 310
3. Procédure 311
4. Quelques délimitations matérielles 315
B. Distinctions 316
Bibliographie 318
Matériaux 319

I. INTRODUCTION

Figurant au chapitre III de la Convention sur la Cybercriminalité[189] intitulé « Coopération internationale », **l'art. 33 CCC** est la première des deux dispositions de la Convention traitant des obligations des Etats parties à coopérer pour la récolte et la transmission de données de communication. Cette disposition concerne les données relatives au trafic, par opposition à **l'art. 34 CCC** qui traite des données relatives au contenu de la communication. 1

La *ratio legis* de cette disposition consiste en ce que, très souvent, les enquêteurs ne peuvent être sûrs de pouvoir remonter à la source d'une communication en se fiant aux enregistrements des transmissions antérieures car des données relatives au trafic cruciales peuvent avoir été automatiquement effacées par un fournisseur de services de la filière de transmission avant de pouvoir être conservées ; il a donc été jugé nécessaire que les enquêteurs de chaque Partie puissent avoir la possibilité de se procurer en temps réel des données relatives au trafic concernant des communications transmises par un système informatique se trouvant sur le territoire d'autres Parties[190]. 2

La pratique suisse confirme ce besoin, au vu de la multiplication des plateformes de messagerie et de courriels offrant des services d'**anonymisation** non seulement par l'utilisation d'un chiffrement des données de bout en bout (*end-to-end encryption*) parfois couplé d'un chiffrement de type zéro-accès (*zero-access encryption*), mais aussi par l'absence de conservation des journaux de connexion (*logs*)[191], de telle sorte que ni une surveillance rétroactive des données relatives au trafic, ni la 3

189. RS 0.311.43 ; citée dans la suite de la contribution sous « CCC » ou « la Convention ».

190. Rapport explicatif du Conseil de l'Europe, n. 295.

191. Par « log », on entend la date et l'heure de connexion au service concerné ainsi que l'adresse IP utilisée. En Suisse, la conservation de ces données sur une période de six mois n'est obligatoire que pour les fournisseurs de services de télécommunication (art. 26 al. 5 LSCPT) ainsi qu'à certaines conditions, pour les fournisseurs de services de communication dérivés (art. 27 al. 3 LSCPT en lien avec l'art. 52 OSCPT) ; v. également arrêt du Tribunal administratif fédéral A-5373/2020 du 11 février 2021 ou encore arrêt du Tribunal fédéral 2C_544/2020 du 29 avril 2021 consécutif à l'arrêt du Tribunal administratif fédéral A-550/2019 du 19 mai 2020.

perquisition des données stockées n'est susceptible de permettre d'identifier l'utilisateur du service. L'interception en temps réel de données permet – le cas échéant via le mécanisme prévu par l'art. 30 CCC – de remonter à la source de la communication.

4 L'art. 33 al. 2 CCC prévoit l'obligation pour les Etats parties d'accorder l'entraide « au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne ». C'est donc le droit pénal matériel national (catalogue d'infractions notamment) qui définit le cadre minimum des engagements de chaque Partie. Cette solution a le mérite d'éviter l'écueil de l'établissement d'une liste d'infractions pour lesquelles l'entraide devrait être accordée dans cette constellation, ce qui, compte tenu des cultures et systèmes juridiques divers, aurait assurément engendré une levée de boucliers de nombreux Etats. A l'inverse, elle vise à encourager les Parties à accorder l'entraide la plus large possible, soit même dans des situations dans lesquelles les infractions poursuivies ne pourraient justifier une telle mesure de surveillance en procédure pénale nationale[192], solution que la Suisse n'a pas décidé d'adopter[193].

5 Au niveau du droit procédural national justement, la CCC oblige les Etats parties à adopter des mesures législatives qui se révèlent nécessaires pour habiliter ses autorités compétentes, d'une part, à collecter ou enregistrer sur son territoire, en temps réel, des données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique et, d'autre part, à contraindre les fournisseurs de services à collecter ou enregistrer eux-mêmes ces données ou à prêter assistance aux autorités pour ce faire (**art. 20 CCC**).

II. NOTIONS

6 Par « **données relatives au trafic** », la Convention entend « toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent » (art. 1 let. d

192. Rapport explicatif du Conseil de l'Europe, n. 296.
193. Cf. *infra* III.A.3.

CCC). Ces données sont produites par des ordinateurs appartenant à la chaîne de communication pour acheminer le contenu d'une communication de son origine à sa destination. Elles sont donc des auxiliaires de la communication elle-même[194]. Par « origine », on entend un numéro de téléphone, une adresse IP ou un moyen similaire d'identifier un dispositif de communication auquel un prestataire de services fournit des services. La « destination » désigne une indication comparable concernant un dispositif de communication vers lequel des communications sont transmises. L'expression « type du service sous-jacent » renvoie au type du service utilisé au sein du réseau : transfert de fichiers, courrier électronique ou messagerie instantanée[195]. En résumé, les données relatives au trafic fournissent des informations sur l'expéditeur et le destinataire ainsi que sur le moment, l'étendue, la durée, le type et l'itinéraire d'une communication[196].

La définition même des « données relatives au trafic » n'a pas été 7
expressément reprise par le législateur suisse dans le cadre de la mise en œuvre de la Convention (en particulier à l'art. 18b EIMP[197] ; cf. *infra* III.A.). Le Conseil fédéral estimait alors que la définition était suffisamment décrite par la doctrine et la pratique, à savoir : « Les données relatives au trafic comprennent notamment les ressources d'adressage de l'origine de l'accès, la date et l'heure du début et de la fin de la connexion, les données utilisées pour la procédure d'identification (login) et le type de connexion »[198]. Depuis le 1er septembre 2016[199], le droit suisse définit les « **données secondaires de télécommunication** » (art. 273 CPP renvoyant à l'art. 8 let. b LSCPT[200]) comme « les données indiquant avec qui, quand, combien de temps et d'où la personne surveillée a été ou est en communication ainsi que les caractéristiques techniques de la communication considérée ». Si cette notion de données secondaires est également applicable aux télécommunications en général[201] - et non uniquement au trafic informatique -, elle couvre la notion

194. Rapport explicatif du Conseil de l'Europe, n. 28.
195. Rapport explicatif du Conseil de l'Europe, n. 30.
196. BSK-Böhi, art. 18b EIMP, n. 4.
197. RS 351.1.
198. Message CCC, 4316 s., citant S. Bondallaz : La protection des personnes et de leurs données dans les télécommunications, n. 1821 et 1823, p. 518.
199. Date d'entrée en vigueur de la LSCPT révisée.
200. RS 780.1.
201. Cf. *infra* III.A.4.

de données relatives au trafic[202]. Cette notion s'oppose à celle de **données relatives au contenu** (cf. commentaire de l'art. 34 CCC).

8 L'art. 33 CCC vise la collecte **en temps réel** des données relatives au trafic. Il s'agit d'intercepter ces données, dès ce jour et pour le futur, au fur et à mesure de l'arrivée ou du départ des communications. Cette notion s'oppose à la récolte de données préexistantes, enregistrées, respectivement stockées sur un support informatique (serveur, *cloud*, ou autre), même lorsqu'il s'agit de données relatives au trafic de communications déjà intervenues[203]. Cette temporalité directe implique l'absence de prise sur ces données par la personne surveillée. En d'autres termes, celle-ci ne dispose typiquement pas de la possibilité de les supprimer avant leur interception. L'« **interception** » de ces données intervient en principe **auprès d'un fournisseur tiers** (fournisseur internet et/ou de téléphonie, fournisseur dérivé de télécommunication, tels que les sociétés gérant des applications de communication). A notre sens, l'art. 33 CCC ne couvre en particulier pas l'interception de données directement auprès de la personne surveillée au moyen d'un logiciel de type Cheval de Troie (*Govware*)[204]. Par contre, une interception du trafic par le biais d'un dispositif technique spécial de surveillance, de type *IMSI catcher* ne semble pas exclu (cf. *infra* III.A.3).

9 Les données interceptées doivent être « **associées à des communications spécifiées** ». L'usage du pluriel s'explique par le fait qu'il peut s'avérer nécessaire de collecter des données relatives au trafic concernant plusieurs communications pour établir l'identité de la personne à l'origine de la communication et/ou celle à laquelle celle-ci est destinée[205]. La notion de « spécifiées » signifie que la CCC n'impose pas aux Etats parties de mettre en place une surveillance et une collecte générales ou systématiques de quantité importante de données relatives au trafic[206]. Cette disposition ne saurait donc justifier une recherche indéterminée de moyens de preuve (« *fishing*

202. Message LSCPT, 2434.
203. Ces données stockées relatives au trafic ne sont pas couvertes par l'art. 33 CCC, mais par l'art. 31 CCC (entraide concernant l'accès aux données stockées) et l'art. 8 du Deuxième protocole additionnel à la CCC (ni signé ni ratifié par la Suisse).
204. Dans sa partie matérielle, la Convention distingue d'ailleurs l'interception illégale (art. 3) de l'atteinte à l'intégrité des données (art. 4) qui inclut l'introduction de codes malveillants tels que des virus ou des chevaux de Troie (cf. Rapport explicatif du Conseil de l'Europe, n. 61).
205. Rapport explicatif du Conseil de l'Europe, n. 219.
206. Rapport explicatif du Conseil de l'Europe, n. 219.

expedition »). De l'avis des auteurs, sont également « associés à une communication spécifique » au terme de cette disposition les journaux des connexions à une boite email (*logs* et IP associées). En effet, alors même que la connexion à une boîte email n'entraîne pas nécessairement l'envoi ou la réception d'une communication[207], elle en constitue un préalable nécessaire. Cette approche semble être celle retenue par le droit suisse ; en effet, comme on l'a vu, dans le Message CCC, le Conseil fédéral s'est appuyé sur une définition de la doctrine qui inclut les ressources d'adressage, y compris les dates et heures de connexion et de déconnexion[208]. L'art. 18b EIMP ne reprend d'ailleurs pas cette notion de « communications spécifiées » ce qui ouvre en particulier la voie à la collecte en temps réel et à la transmission anticipée des journaux de connexions (cf. *infra* III.A.4.).

10 Par ailleurs, les communications spécifiées doivent se dérouler **sur le territoire** d'une Partie. Cet aspect pourrait être potentiellement problématique, dès lors que l'usage de technologie de type *cloud* ne permet plus d'associer un lieu de stockage à un Etat en particulier. En pratique, le critère du lieu de stockage des données a perdu de son importance au profit de celui du lieu où se situe la personne (physique ou morale) qui dispose d'un contrôle effectif sur les données[209]. De l'avis des auteurs, l'art. 33 CCC trouve également à s'appliquer dans cette nouvelle configuration.

11 La disposition impose aux Parties de s'accorder l'entraide dans la **collecte** en temps réel de ces données. Si, à première lecture, la notion de « collecte » comprend celle de « transmission » – puisque cette collecte intervient à la demande et pour les besoins d'une autorité étrangère – nous verrons que le législateur suisse a distingué ces deux notions dans le cadre de la mise en œuvre de l'art. 33 CCC (cf. *infra* III.).

12 Enfin, la Convention ne s'applique pas en tant que telle aux télécommunications classiques (téléphonie analogique) puisque les données doivent **être transmises au moyen d'un système informatique**.

207. Typiquement, les boîtes email peuvent être utilisées comme « boîtes aux lettres mortes » pour communiquer entre utilisateurs qui disposent des droits d'accès. Les messages sont enregistrés comme brouillons, les utilisateurs les relevant à leur tour en se connectant à la boîte email.

208. Message CCC, 4316 s., citant S. Bondallaz : La protection des personnes et de leurs données dans les télécommunications, n. 1821 et 1823, p. 518.

209. Arrêt du Tribunal fédéral 1B_142/2016 consid. 3 et ATF 143 IV 21.

L'avènement de la téléphonique numérique et plus généralement la convergence des technologies des télécommunications brouille néanmoins les distinctions entre télécommunications et téléinformatique et les spécificités de leurs infrastructures. Ainsi la Convention – notamment les art. 20 et 33 CCC - s'applique à des communications spécifiées transmises au moyen d'un système informatique, la communication pouvant être transmise par le biais d'un réseau de télécommunications avant d'être reçue par un autre système informatique[210].

III. MISE EN ŒUVRE EN DROIT SUISSE

A. L'art. 18b EIMP

1. Historique

13 L'art. 18b EIMP est introduit dans le sillage de la ratification de la CCC par la Suisse[211]. Le Message CCC rappelle que les mesures de surveillance en temps réel doivent, par essence, rester inconnues des personnes surveillées ; ce postulat se concilie difficilement avec le principe de base de l'EIMP, selon lequel aucune information relevant de la sphère secrète d'une personne ne peut être transmise à l'étranger sans que celle-ci n'ait préalablement eu la possibilité de s'y opposer. L'art. 18b EIMP permet ainsi de répondre aux exigences posées par l'art. 33 CCC[212].

2. Définitions

14 Aux termes de **l'art. 18b al. 1 EIMP**, l'autorité fédérale ou cantonale chargée de traiter une demande d'entraide peut ordonner la transmission à l'étranger de données relatives au trafic informatique avant la clôture de la procédure d'entraide si les mesures provisoires font apparaître que la source de la communication faisant l'objet de la demande d'entraide se trouve à l'étranger (al. 1 let. a) ou si ces données sont recueillies par l'autorité d'exécution en vertu d'un ordre de surveillance en temps réel qui a été autorisé (art. 269 à 281 CPP ; al. 2 let. b)[213]. Si l'hypothèse de la let. a constitue la législation d'application de l'art. 30 CCC, la let. b, quant à elle, met en œuvre les

210. Rapport explicatif du Conseil de l'Europe, n. 206.
211. Message CCC, 4276.
212. FF 2010 4275, 4311 s.

engagements internationaux de la Suisse découlant de l'art. 33 CCC. Pour autant, cette disposition n'assure pas encore l'octroi de l'entraide puisque son al. 2 prohibe l'utilisation de ces données comme moyen de preuve avant que la décision sur l'octroi et l'étendue de l'entraide (art. 80d EIMP) n'ait acquis force de chose jugée[214]. La décision fondée sur l'art. 18b EIMP permettant un accès rapide aux données par l'autorité requérante est une **décision incidente**, qui ouvre ensuite la voie à la procédure d'entraide classique nécessaire selon le droit suisse. En cela, le législateur a pris soin de distinguer la collecte des données et leur accès rapide par l'autorité requérante de l'entraide elle-même, conciliant ordre juridique suisse et engagements internationaux.

3. Procédure

L'art. 18b al. 1 let. b EIMP renvoie aux art. 269 à 281 CPP et donc notamment, 15
s'agissant de surveillance de données secondaires de télécommunication, à l'art. 273 CPP. Ce dernier prévoit en particulier que seuls des graves soupçons de commission de **crimes et délits** (art. 10 al. 2 et 3 CP) permettent au ministère public d'obtenir des données secondaires de télécommunication[215].

213. Une partie de la doctrine considère que les lettres a et b de l'art. 18b al. 1 EIMP constituent des conditions cumulatives (cf. ZIMMERMANN, p. 407, n. 376) ; si le texte français est ambigu sur cette question, les versions allemande (« oder ») et italienne (« oppure ») sont explicites quant à la nature alternative de ces cas, ce que retiennent d'autres auteurs, auxquels nous nous rallions (cf. BSK-Böhi, art. 18b EIMP, n. 3 ou encore Isenring/Maybud/Quiblier, p. 446).

214. Les auteurs ne se prononcent pas sur la compatibilité de cette spécificité avec la CCC, celle-ci ne semblant pas répondre aux restrictions d'utilisation que la partie requise est en droit d'apposer aux termes de l'art. 28 CCC.

215. Cette décision du législateur concrétise la réserve consignée selon laquelle conformément à l'art. 14 par. 3 CCC, la Suisse se réserve le droit de n'appliquer les mesures mentionnées à l'art. 20 CCC qu'aux crimes et délits au sens du code pénal. Elle est satisfaisante sous l'angle de la sécurité du droit et évite ainsi des situations dans lesquelles le ministère public serait tenté d'utiliser aux fins d'une procédure nationale des données issues de l'exécution d'une demande d'entraide étrangère qui n'auraient pas pu être obtenues en procédure nationale. Elle est également plus claire et moins sujette à interprétation et discussion que la solution consistant à refuser l'entraide sur la base du principe de proportionnalité (art. 15 par. 1 et 2 CCC) lorsque les faits sous enquête à l'étranger apparaissent constitutifs d'une contravention en droit suisse (cf. Message CCC, 4314). A l'opposé, en matière d'entraide active, le principe de réciprocité devra ainsi empêcher l'autorité pénale suisse de requérir d'un Etat partie à la Convention l'obtention de données relatives au trafic pour des faits potentiellement constitutifs de contravention (art. 30 al. 1 EIMP).

Ainsi, le législateur suisse n'a pas voulu ouvrir le champ d'application de l'art. 33 CCC à des infractions qui ne permettraient pas l'application de ces mesures en droit suisse, comme le propose l'art. 33 al. 2 CCC.

16 L'art. 18b al. 1 let. b EIMP constitue une **dérogation au système classique de l'entraide** selon lequel le droit d'être entendu de la personne touchée par une mesure d'entraide doit être garanti et une ordonnance de clôture dûment notifiée et entrée en force préalablement à toute transmission de moyen de preuve à l'étranger (art. 80d EIMP). Avant l'entrée en vigueur de cette disposition, la Suisse ne pouvait fournir à l'étranger de telles données issues d'une surveillance secrète sans en avoir préalablement informé la personne touchée (pour autant que celle-ci soit domiciliée en Suisse ou y ait élu domicile ; cf. art. 80m EIMP), ce qui rendait la mesure bien souvent inutile pour la procédure étrangère, voire pouvaient mettre celle-ci en péril.

17 Désormais, après être entrée en matière (art. 80a EIMP), l'autorité d'exécution ordonnera la mesure de surveillance par l'intermédiaire du Service Surveillance de la correspondance par poste et télécommunication (Service SCPT ; art. 273 CPP en lien avec les art. 60 ss OSCPT[216]).

18 Elle devra ensuite faire autoriser la mesure par le Tribunal des mesures de contrainte dans les 24 heures à compter de l'ordre (art. 274 al. 1 CPP). A noter que, s'agissant de la condition, posée à l'art. 273 CPP, de l'existence d'un « **grave soupçon** », le Tribunal fédéral a rappelé à juste titre que selon les règles sur l'entraide judiciaire et la jurisprudence constante, les art. 14 CEEJ, 28 EIMP et 10 OEIMP[217] imposent à l'autorité requérante d'expliquer en quoi consistent ses soupçons, mais pas de les prouver ni même de les rendre vraisemblables. Sous réserve de l'interdiction des requêtes exploratoires, les soupçons de l'autorité requérante n'ont donc pas à être particulièrement graves ou précis. En effet, si le droit interne doit s'appliquer lorsqu'il est plus favorable à la coopération que le droit conventionnel, il ne saurait en revanche poser des conditions matérielles à l'entraide qui ne sont pas prévues par le droit conventionnel[218].

19 Le Tribunal des mesures de contrainte statue dans les cinq jours (art. 274 al. 2 CPP). En cas de refus de la surveillance, les documents et enregistrements collectés doivent être immédiatement détruits (art. 277 al. 1 CPP). Si

216. RS 780.11.
217. RS 351.11

l'autorisation est accordée, il faut relever que l'art. 279 CPP prévoyant la communication au prévenu ou au tiers objet de la surveillance et aménageant un droit de recours à ces derniers ainsi qu'au service de télécommunication surveillé (art. 279 al. 3 CPP) ne trouve pas application, malgré le renvoi de l'art. 18b al. 2 let. a aux art. 269 à 281 CPP. En effet, les conventions et lois applicables dans le domaine de l'entraide judiciaire internationale en matière pénale dérogent au système usuel du CPP qui ne trouve application que s'il est plus favorable à la coopération que ces conventions et lois applicables (principe de faveur)[219]. Cela a notamment pour effet que **la qualité de partie, le droit à la notification ainsi que les voies de droit sont régis par les dispositions spécifiques en matière d'entraide**[220]. Or selon l'art. 80m al. 1 EIMP, les obligations de notifier les décisions en matière d'entraide sont limitées aux personnes résidant ou ayant élu domicile en Suisse. D'éventuelles indications contraires de la part du TMC, que ce soit par rappel de la loi ou par apposition de conditions au sens de l'art. 274 al. 2 CPP seraient donc invalides, faute de compétence du TMC pour connaître de cet aspect de la procédure[221]. Il reviendra à l'autorité d'exécution, dans le cadre de la procédure d'entraide judiciaire – donc le cas échéant après la transmission anticipée prévue à l'art. 18b EIMP –, de veiller au respect de ces conventions et lois applicables et de procéder aux seules notifications prévues par l'art. 80m EIMP.

A réception des données issues de la surveillance, l'autorité d'exécution pourra rendre une **décision incidente** fondée sur l'art. 18b EIMP pour ordonner la transmission anticipée des données à l'autorité requérante. La 20

218. Arrêt du Tribunal fédéral 1C_558/2017 du 21 novembre 2017 consid. 1.2 relatif à des écoutes téléphoniques mais parfaitement transposable en matière informatique. C'est le lieu de rappeler que la CEEJ reste applicable même aux demandes d'entraide présentées dans l'une des matières traitées par la CCC. En effet, la CCC a pour but, selon son préambule, de compléter les conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, « en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale ».
219. Arrêt du Tribunal fédéral 1C_558/2017 du 21 novembre 2017 consid. 1.2.
220. Dans ce sens : arrêt du Tribunal pénal fédéral RR.2015.142-143/RR.2015.144-145 du 30 octobre 2015 consid. 5.2.2 ; arrêt du Tribunal fédéral 1C_36/2015 du 19 janvier 2015 ; arrêt du Tribunal fédéral 1C_44/2022 du 28 janvier 2022 consid. 2.2 ; avis similaire exprimé par BSK-Böhi, art. 18b EIMP, n. 30.
221. Dans ce sens : arrêts du Tribunal fédéral 1B_563/2011, 1B_631/2011 et 1B_633/2011 du 16 janvier 2012 consid. 2.3.

décision, de même que l'ordre et l'autorisation de surveillance sont communiquées à l'OFJ (art. 18b al. 3 EIMP). Si la surveillance est vouée à **durer dans le temps** et que des données sont régulièrement collectées, la décision pourra couvrir toutes les données futures issues de la surveillance autorisée de manière à permettre à l'autorité d'exécution (ou à la police le cas échéant) de transmettre les données au fur et à mesure de leur réception. En l'absence de notification à la personne touchée à ce stade et au vu des limites imposées par l'art. 18b al. 2 EIMP, une telle manière de procéder ne lèse pas les droits des parties à la procédure d'entraide et doit pouvoir être admise.

21 Il conviendra néanmoins de rappeler, à chaque transmission anticipée à l'autorité requérante, que ces données ne peuvent être utilisées comme moyens de preuve avant l'entrée en force de chose jugée de la décision sur l'octroi et l'étendue de l'entraide (art. 18b al. 2 EIMP). La protection juridique est ainsi garantie a posteriori[222]. Il est également essentiel de conserver une trace – à tout le moins sous forme de liste - des données transmises de manière anticipée afin de permettre à l'autorité d'exécution, au terme de la procédure d'entraide, de savoir précisément sur quelles données devra porter la **décision de clôture finale**.

22 En pratique, lorsque la personne touchée par la mesure de surveillance est inconnue, n'est pas domiciliée en Suisse, ni y a pas élu domicile, voire utilise une fausse identité[223], l'autorité d'exécution peut rapidement valider l'utilisation des données à titre de moyen de preuve par décision de clôture. Celle-ci étant uniquement notifiée à l'OFJ (art. 80h let. a EIMP), le secret sur l'existence des mesures est préservé.

23 Lorsque la personne touchée par la mesure de surveillance est domiciliée en Suisse ou qu'elle y a élu domicile, son droit d'être entendue devra lui être garanti (art. 80m al. 1 EIMP en lien avec l'art. 80b EIMP), ce qui implique qu'elle devra être informée de la mesure et avoir eu l'occasion de s'exprimer par écrit avant le rendu de la décision de clôture. L'art. 18b EIMP permet précisément de **repousser l'information à la personne touchée et l'octroi de son droit d'être entendu** aussi longtemps que nécessaire pour la procédure à l'étranger. En pratique, l'autorité d'exécution devra régulièrement

222. Donatsch/Heimgartner/Meyer/Simonek, p. 55 s.
223. Dans ce sens : arrêt du Tribunal fédéral 1C_626/2015 du 8 décembre 2015 consid. 1.4 s.

s'enquérir auprès de l'autorité requérante de la nécessité, pour la procédure à l'étranger, de maintenir secrète la mesure de surveillance ordonnée en Suisse.

La décision de clôture est susceptible de **recours** au Tribunal pénal fédéral (art. 80e EIMP). La décision incidente de transmission anticipée des données relatives au trafic au sens de l'art. 18b EIMP pourra être contestée conjointement à la décision de clôture (art. 80e al. 1 EIMP). Un recours immédiat contre la décision incidente semble possible, si l'autorité d'exécution n'a pas pris les précautions nécessaires à s'assurer que les cautèles de l'art. 18b al. 2 EIMP sont respectées[224]. Un recours au Tribunal fédéral demeure possible aux conditions restrictives de l'art. 84 LTF[225] (cas particulièrement important). Une partie de la doctrine soutient qu'en cas d'admission du recours, les informations transmises doivent être retirées du dossier étranger[226]. Tel est certainement le cas si l'autorité étrangère s'est engagée à le faire, bien que cette obligation ne figure pas à l'art. 18b EIMP[227]. 24

La rédaction très large de l'art. 18b al. 1 let. b EIMP semble permettre également la transmission anticipée de données relatives au trafic informatique lorsque celles-ci ont été interceptées au moyen d'*IMSI catcher* (art. 269bis CPP), de *govware* (art. 269ter CPP) voire d'autres dispositifs techniques de surveillance (art. 280 CPP), quand bien même l'art. 33 CCC ne ferait pas une telle obligation. 25

4. Quelques délimitations matérielles

Contrairement au texte de l'art. 33 CCC, l'art. 18b EIMP n'est pas limité à des « **communications spécifiées** ». Ainsi, le **journal de connexion (logs)** à une boite de courriel peut être obtenu au moyen d'une surveillance en temps réel[228] et transmis de manière anticipée à l'autorité requérante, même en l'absence de communication (p.ex. pas de courriel envoyé au cours de cette session de connexion ou de courriel reçu). 26

224. Une telle décision étant susceptible d'avoir les mêmes effets qu'une décision de clôture (cf. dans ce sens : arrêt du Tribunal fédéral 1C_1/2017 du 27 mars 2017 et les références citées.
225. RS 173.110.
226. Donatsch/Heimgartner/Meyer/Simonek, p. 56.
227. A contrario de l'art. 80d^{bis} al. 4 EIMP ; sur la compatibilité de ces restrictions avec les engagements internationaux de la Suisse découlant de l'art. 33 CCC, voir note 26 *supra*.
228. Art. 58 OSCPT.

27 Le Tribunal fédéral a eu l'occasion d'affirmer que l'art. 18b EIMP constitue une base légale permettant le transfert anticipé des données **relatives au trafic** issues d'une surveillance en temps réel, **à l'exclusion des données relatives au contenu**, faute de base légale ou conventionnelle[229].

28 Dans le même arrêt, le Tribunal fédéral a ouvert la transmission anticipée des données au sens de l'art. 18b EIMP aux données relatives au **trafic téléphonique**[230]. Ainsi, les données secondaires issues d'une surveillance active d'un raccordement téléphonique (p.ex. numéros appelé ou appelant, durée de la conversation téléphonique ou encore antenne activée) sont des données qui devraient pouvoir être transmises de manière anticipée à une autorité étrangère sur la base de l'art. 18b EIMP. A notre sens, cette interprétation du Tribunal fédéral est somme toute logique au regard de la numérisation généralisée des systèmes de télécommunication et, partant, du caractère de plus en plus caduc et artificiel de la distinction entre système de télécommunication
classique d'une part, et système informatique d'autre part.

29 L'art. 18b EIMP présente un autre avantage : si la collecte de données relatives au trafic transmises de manière anticipée permet de constater qu'une **nouvelle mesure de surveillance** sur un autre compte, une autre ligne, etc., en Suisse ou à l'étranger, se justifie, l'autorité requérante peut immédiatement requérir l'exécution d'une telle mesure.

B. Distinctions

30 La transmission anticipée des informations liées au trafic informatique prévue par l'art. 18b EIMP doit être distinguée de la **transmission spontanée de moyens de preuve et d'informations (art. 67a EIMP)** qui fait également exception au principe selon lequel une décision de clôture entrée en force est nécessaire avant toute transmission à l'étranger. A la différence du système de l'art. 67a EIMP, l'art. 18b EIMP intervient nécessairement dans le cadre de l'exécution d'une demande d'entraide étrangère tendant à obtenir ces moyens

229. ATF 143 IV 186, consid. 2.3 ; v. aussi Hansjakob/Pajarola, art. 272 CPP, n. 39-41.

230. ATF 143 IV 186, consid. 2.3 : « *Une application analogique de l'art. 18b EIMP pourrait certes être envisagée s'agissant des données relatives au trafic téléphonique [...]* » ; cette position s'oppose à l'avis du Conseil fédéral qui, dans son message, a expressément considéré que l'art. 18b EIMP ne se rapport pas aux données sur la téléphonie, celles-ci étant couverte par l'art. 18a EIMP (Message CCC, 4316 s.).

de preuve. L'art. 18b EIMP ne prévoit en effet aucunement une transmission anticipée « spontanée » des données relatives au trafic. De surcroît, l'art. 67a EIMP prohibe la transmission de moyens de preuve dès qu'ils touchent au domaine secret (art. 67 al. 4 EIMP). Dans ce cas, seules des informations peuvent être fournies à une autorité étrangère (art. 67a al. 5 EIMP)[231].

31 La transmission anticipée des informations liées au trafic informatique prévue par l'art. 18b EIMP doit également être distinguée de **l'entraide dynamique (art. 80d^{bis} EIMP)** qui permet, à titre exceptionnel, une transmission anticipée d'informations ou de moyens de preuve (a) lorsque les enquêtes étrangères portant sur des affaires de criminalité organisée ou de terrorisme seraient excessivement difficiles sans cette mesure d'entraide judiciaire, notamment en raison du risque de collusion, ou parce que la confidentialité de la procédure doit être préservée, ou (b) afin de prévenir un danger grave et imminent, notamment la commission d'un acte terroriste. L'introduction en 2021 de cette nouvelle disposition – accompagnée de nouvelles règles sur l'équipe commune d'enquête - a été considérée comme un premier pas important vers des règles assouplies et une entraide plus rapide et réactive, fondée sur la confiance internationale[232]. Du point de vue du champ d'application matériel, l'art. 18b EIMP ne connait aucune limitation, alors que l'art. 80d^{bis} EIMP se limite, sauf danger grave et imminent, à la criminalité organisée et au terrorisme[233]. A l'inverse, l'art. 80d^{bis} EIMP prévoit que tout type de moyen de preuve ou information peut être transmis de manière anticipée par ce biais[234], alors que le champ d'application de l'art. 18b EIMP est limité aux seules données relatives au trafic informatique, étant néanmoins rappelé que le Tribunal fédéral a ouvert la voie à une application analogique de l'art. 18b EIMP en matière de surveillance téléphonique[235]. Enfin, l'art. 18b EIMP ne prévoit – explicitement du moins – aucun engagement préalable de l'autorité requérante, l'autorité d'exécution devant informer celle-ci du fait que les données transmises de manière anticipée ne peuvent pas être utilisées comme moyens de preuve avant que la décision sur l'octroi et l'étendue de

231. Pour plus de détails, cf. BSK-Glutz, art. 67a EIMP ou encore Ludwiczak Glassey/Bonzanigo, p. 402-427.
232. Ludwiczak, p. 75.
233. Cf. Ludwiczak Glassey/Bonzanigo, p. 402-427.
234. V. Dangubic/Clerc, p. 291.
235. ATF 143 IV 186.

l'entraide n'ait acquis force de chose jugée (art. 18b al. 2 EIMP). Sur ce point, l'art. 80d^{bis} EIMP est plus formaliste (cf. art. 80d^{bis} al. 4 EIMP)[236].

32 Enfin, une transmission anticipée au sens de l'art 18b EIMP ne semble pas présenter d'intérêt particulier dans le cadre d'une **équipe commune d'enquête (ECE ; ou** *Joint Investigation Team, JIT* **; art. 80d^{ter} à 80d^{duodecies} EIMP)** ; en effet, le champ matériel restreint de l'art. 80d^{bis} EIMP, ne s'applique pas, de l'avis des auteurs, aux équipes communes d'enquête, malgré le renvoi malheureux de l'art. 80d^{octies} EIMP aux conditions de l'art. 80d^{bis} EIMP[237].

Les auteurs ont rédigé la présente contribution à titre personnel. Les appréciations et opinions présentées sont les leurs et n'engagent pas le Ministère public de la Confédération.

BIBLIOGRAPHIE

Böhi Simon, commentaire de l'art. 18b EIMP, in : Niggli Marcel Alexander/ Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1ère édition, Bâle 2015.

Dangubic Miro/Clerc Yves, Art. 80d^{bis} IRSG – ein Überblick, forumpoenale 4 (2022) p. 287.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, Internationale Rechtshilfe, 2e édition., Zurich et al. 2015.

Glutz Alexander M., commentaire de l'art. 67a EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1ère édition, Bâle 2015.

Hansjakob Thomas/Pajarola Umberto, commentaire de l'art. 272 CPP, in : Donatsch Andreas/Lieber Viktor/ Summers Sarah/Wohlers Wolfgang (édit.), Kommentar zur Schweizerischen Strafprozessordnung StPO, 3e édition, Zurich 2020.

236. Pour une présentation plus complète de l'art. 80d^{bis} EIMP, voir Dangubic/Clerc, p. 287.
237. Cf. Ludwiczak Glassey/Bonzanigo qui estime cet avis « soutenable ».

Isenring Bernhard/Maybud Roy D./Quiblier Laura, Phänomen Cybercrime – Herausforderungen und Grenzen des Straf- und Strafprozessrechts im Überblick, SJZ 115 (2019) p. 439.

Ludwiczak Glassey Maria/Bonzanigo Francesca, L'artificielle distinction entre « informations » et « moyens de preuve » en entraide pénale internationale, Revue Pénale Suisse 140/2022 p. 402-427.

Ludwiczak Maria, L'entraide pénale internationale 'dynamique' en bref. Le projet, les débats, le compromis, Pratique juridique actuelle, 1 (2021) p. 71–75.

Zimmermann Robert, La coopération judiciaire internationale en matière pénale, 5e édition, Berne 2019.

MATÉRIAUX

Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 27 février 2013, FF 2013 2379, consultable sous https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2013/512/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2013-512-fr-pdf-a.pdf, consulté en janvier 2024 (cité : Message LSCPT).

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité du 18 juin 2010, FF 2010 4275, consultable sous https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2010/813/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2010-813-fr-pdf-a.pdf, consulté en janvier 2024 (cité : Message CCC).

Rapport explicatif de la Convention sur la cybercriminalité du 23 novembre 2001, Conseil de l'Europe, Série des traités européens – no 185, consultable sous https://rm.coe.int/16800ccea4, consulté en janvier 2024 (cité : Rapport explicatif du Conseil de l'Europe).

COMMENTAIRE

Art. 34 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Nicolas Bottinelli / Julien Wenger

PROPOSITION DE CITATION

Nicolas Bottinelli/Julien Wenger, Commentaire de l'art. 34 CCC, in: Damian K. Graf (édit.), Commentaire en ligne de la Convention sur la cybercriminalité (Cybercrime Convention)

Citation abrégée: OK-Bottinelli/Wenger, art. 34 CCC N. XXX.

Art. 34 Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

TABLE DES MATIÈRES

I. Introduction 323
II. Notions 324
III. Mise en œuvre en droit suisse 326
A. L'interception des données relatives au contenu en droit suisse 326
B. Distinctions et cas particuliers 330
1. Transmission anticipée des données relatives au contenu ? 330
2. Distinction entre un ordre de dépôt (art. 265 CPP) et une mesure de surveillance (art. 269 ss CPP), en particulier s'agissant des boîtes de courriel 332
3. Utilisation d'une fausse identité 333
Bibliographie 333
Matériaux 334

I. INTRODUCTION

Figurant au chapitre III de la Convention sur la Cybercriminalité[238] intitulé « Coopération internationale », **l'art. 34 CCC** se penche sur la coopération internationale en lien avec les données relatives au contenu, par opposition aux données relatives au trafic, traitées quant à elles à **l'art. 33 CCC**. 1

La CCC reconnait l'importance de pouvoir procéder à l'interception de données relatives au contenu pour les besoins de procédures pénales nationales (art. 21 CCC) : la collecte de données relative au contenu des télécommunications a toujours été un instrument d'enquête utile pour déterminer si la communication a un caractère illégal et pour apporter la preuve d'infractions passées ou futures. Les communications informatiques peuvent constituer ou prouver le même type d'infraction, tout en offrant de plus vastes possibilités grâce à la transmission de grandes quantités de données (texte, images et son). Il n'est pas possible de déterminer en temps réel la nature préjudiciable et illégale de ces communications sans intercepter le contenu du message. Si elles ne pouvaient pas établir et prévenir la commission d'infractions au moment où elles ont eu lieu, les autorités chargées de l'application de la loi en seraient réduites à enquêter sur des infractions révolues, dans le cas desquelles le préjudice a déjà été causé. Il en découle que l'interception en temps réel des données relatives au contenu des communications informatiques est au moins, sinon plus importante que l'interception en temps réel des télécommunications[239]. 2

Toutefois, l'art. 34 CCC ne fait aucune obligation aux Etats parties d'être en mesure de coopérer dans la collecte transfrontalière de ces données ; tout au plus le Rapport explicatif du Conseil de l'Europe renvoie-t-il aux bonnes pratiques figurant dans la Recommandation de 1985 relative à l'application de la CEEJ à la surveillance des télécommunications[240]. Le Deuxième Protocole additionnel à la CCC, du 12 mai 2022[241], ne traite pas de cette mesure, pas plus que les travaux préparatoires au 3e Protocole additionnel à la CEEJ. 3

238. RS 0.311.43 ; citée dans la suite de la contribution sous « CCC » ou « la Convention ».
239. Rapport explicatif du Conseil de l'Europe, n. 228.
240. Recommandation no R (85) 10.
241. Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE no 224) (2022).

II. NOTIONS

4 L'art. 34 CCC prévoit que les Parties s'accordent l'entraide dans ce cadre « **dans la mesure permise par leurs traités et lois internes applicables** ». Contrairement à ce qui prévaut à l'art. 33 CCC en matière de données relatives au trafic informatique, l'art. 34 CCC n'impose strictement aucune obligation de la part des Etats parties s'agissant de l'entraide en matière d'interception de données relatives au contenu des communications informatiques. La décision de s'en remettre aux régimes et législations internes est justifiée par le caractère très intrusif de l'interception et à une pratique de l'entraide en la matière alors encore à ses débuts[242].

5 La notion de « **données relatives au contenu** » n'est pas définie dans la Convention. Elle désigne le contenu informatif de la communication, c'est-à-dire le sens de la communication ou le message ou l'information transmis par la communication (autre que les données relatives au trafic)[243]. Concrètement, par « données relatives au contenu », il faut entendre la communication proprement dite, son objet même, à savoir notamment le texte d'un courriel (y compris dans la conception suisse la rubrique « objet »[244]), d'un message instantané, les éventuelles pièces jointes ou encore le fichier ou le flux audio et/ou vidéo transmis. Cette notion s'oppose à celle de « données relatives au trafic » qui regroupe en substance les éléments de la chaîne de communication (origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ; art. 1 let. d CCC). Cette distinction est fondamentale en matière de mesures de surveillance et a des conséquences directes sur l'octroi de l'entraide internationale. Ainsi, la Suisse permet à certaines conditions la transmission rapide et anticipée de données relatives au trafic informatique sur la base de l'art. 18b EIMP[245], ce qui est exclu en matière de données relatives au contenu (cf. *infra* III.B.1.)[246].

6 L'art. 34 CCC couvre « **l'interception en temps réel** », notion qui s'oppose à la perquisition de données enregistrées, respectivement stockées sur un

242. Rapport explicatif du Conseil de l'Europe, n. 297 et Message CCC, 4314
243. Rapport explicatif du Conseil de l'Europe, n. 209.
244. Le Rapport explicatif OSCPT considère expressément que « la ligne d'en-tête où figure l'objet » a déjà trait au contenu (cf. commentaire de l'art. 58, p. 62).
245. RS 351.1.
246. ATF 143 IV 186 consid. 2.3.

support informatique (serveur, *cloud*, ou autre). Cette temporalité directe implique l'absence de prise sur ces données par la personne surveillée. En d'autres termes, celle-ci ne dispose pas de la possibilité de les supprimer avant leur interception. L'« **interception** » de ces données intervient en principe **auprès d'un fournisseur tiers** (fournisseurs internet et/ou de téléphonie, fournisseurs de services de communication dérivés [ci-après : FSCD], tels que les sociétés gérant des applications de communication). A notre sens, l'art. 34 CCC ne couvre en particulier pas l'interception de données relatives au contenu directement auprès du suspect de l'enquête au moyen d'un logiciel de type Cheval de Troie (*Govware*)[247] ; rien n'exclut toutefois que l'art. 34 CCC puisse servir de base pour l'interception de communications par le biais d'un IMSI Catcher.

La disposition prévoit que l'entraide est accordée pour la « **collecte ou l'enregistrement** » en temps réel des données. A notre sens, bien que la distinction entre ces deux termes semble incertaine[248], la collecte couvre l'acte initial de recueillir les données tandis que l'enregistrement concerne leur conservation en vue de leur transmission à l'autorité requérante, respectivement de leur utilisation dans le cadre de l'enquête pénale. Ces deux notions constituent ainsi deux étapes successives nécessaires à l'exécution de la surveillance, mais leur distinction n'a guère de portée pratique. Par ailleurs, si à première lecture, les notions de « collecte » et d'« enregistrement » comprennent celle de « transmission » – puisque cette collecte intervient à la demande et pour les besoins d'une autorité étrangère – nous verrons que le législateur suisse a distingué ces notions. En effet, les données collectées en exécution d'une demande d'entraide judiciaire étrangère n'échappent pas à la procédure d'entraide usuelle avant toute transmission du moyen de preuve à l'étranger (cf. en particulier *infra* III.A. ad art. 18a EIMP). 7

Les données interceptées doivent être liées à des « **communications spécifiques** ». Il faut comprendre par ce terme que la Convention ne requiert ni n'autorise la surveillance et la collecte générales ou systématiques de 8

247. Dans sa partie matérielle, la Convention distingue d'ailleurs l'interception illégale (art. 3) de l'atteinte à l'intégrité des données (art. 4) qui inclut l'introduction de codes malveillants tels que des virus ou des chevaux de Troie (cf. Rapport explicatif du Conseil de l'Europe, n. 61).

248. Le Rapport explicatif du Conseil de l'Europe, n. 208, semble associer l'enregistrement à l'acte de copier la donnée collectée sans procéder pour autant à une distinction claire entre « collecte » et « enregistrement ».

quantité importantes de données relatives au contenu (surveillance de masse). Elle n'autorise pas non plus les « missions exploratoires » (« *fishing expedition* ») à la faveur desquelles on espère découvrir des activités criminelles, situation très différente des enquêtes ouvertes sur des cas précis d'agissements illicites[249]. A l'évidence, ce terme ne signifie pas qu'il soit nécessaire de déterminer quelle communication spécifique future entre plusieurs systèmes informatiques devra être surveillée, puisqu'il n'est que rarement possible d'anticiper des communications à venir. Ce qu'il faut néanmoins retenir est que l'objet de la surveillance (adresse de courriel, identifiant d'un utilisateur d'une application de messagerie, etc.) doit être précisément déterminé.

9 Enfin, la Convention ne s'applique pas en tant que telle aux télécommunications classiques (téléphonie analogique) puisque les données doivent **être transmises au moyen d'un système informatique**. L'avènement de la téléphonique numérique et plus généralement la convergence des technologies des télécommunications brouille néanmoins les distinctions entre télécommunications et téléinformatique et les spécificités de leurs infrastructures. Ainsi la Convention – notamment les art. 21 et 34 CCC - s'applique à des communications spécifiées transmises au moyen d'un système informatique, la communication pouvant être transmise par le biais d'un réseau de télécommunications avant d'être reçue par un autre système informatique[250].

III. MISE EN ŒUVRE EN DROIT SUISSE

A. L'interception des données relatives au contenu en droit suisse

10 Si l'art. 33 CCC a été à l'origine de l'introduction de l'art. 18b EIMP permettant une transmission anticipée (c'est-à-dire avant l'entrée en force d'une décision de clôture) des données relatives au trafic informatique à l'autorité requérante, l'art. 34 CCC n'a engendré – directement du moins - aucune modification de la législation suisse en matière d'interception de

249. Rapport explicatif du Conseil de l'Europe, n. 219 relatif à l'art. 20 CCC, mais applicable *mutatis mutandis* à l'art. 21 CCC et donc à l'art. 34 CCC.

250. Rapport explicatif du Conseil de l'Europe, n. 206.

données relatives au contenu. Ce sont ainsi, et sous quelques réserves, les règles usuelles de la procédure pénale suisse qui s'appliquent (art. 269 ss CPP) par renvoi de l'art. 18a EIMP.

L'art. 18a EIMP est la disposition topique relative à la surveillance de la correspondance par poste et télécommunication en matière d'entraide judiciaire. Il en ressort en substance que sur demande expresse d'une autorité requérante[251], le Ministère public - voire dans certains cas l'Office fédéral de la justice - peut ordonner une telle surveillance (al. 2) et que l'ordre doit être soumis à l'approbation du Tribunal des mesures de contrainte compétent (al. 3). Pour le surplus, l'art. 18a EIMP renvoie aux art. 269 à 279 CPP ainsi qu'à la loi fédérale du 6 octobre 2000 concernant la surveillance de la correspondance par poste et télécommunication (LSCPT)[252]. Ce renvoi aux art. 269 et suivants CPP – en particulier au catalogue d'infractions de l'art. 269 CPP – correspond à « l'éventail d'infractions graves » que les Parties doivent définir en droit interne aux fins de permettre l'interception des données relatives au contenu (art. 21 et 34 CCC). Le renvoi général aux dispositions de la LSCPT permet également de considérer que l'art. 18a EIMP s'applique tant aux communications ordinaires (téléphonie analogique classique) qu'aux communications liées à un système informatique (cf. not. art. 2 let. c LSCPT)[253]. 11

Dans les faits, après être entrée en matière (art. 80a EIMP), l'autorité d'exécution ordonnera la mesure de surveillance par l'intermédiaire du Service Surveillance de la correspondance par poste et télécommunication (ci-après : Service SCPT ; art. 269 CPP en lien avec les art. 55 ss OSCPT[254]). Il sera ainsi possible d'ordonner la surveillance en temps réel du contenu et des données secondaires de services d'accès au réseau (art. 55 OSCPT), la surveillance en temps réel du contenu et des données secondaires de services de téléphonie et multimédia (art. 57 OSCPT) ou encore la surveillance en temps réel du contenu et des données secondaires de services de courrier électronique (art. 59 OSCPT). 12

251. BSK-Aepli, art. 18a EIMP, n. 22 et Donatsch/Heimgartner/ Meyer/Simonek, p. 190 s. auxquels nous nous rallions ; d'un autre avis : Zimmermann, n. 439, qui estime qu'une requête expresse de l'Etat requérant n'est pas indispensable.
252. RS 780.1.
253. BSK-Aepli, art. 18a EIMP, n. 10.
254. RS 780.11.

13 L'autorité d'exécution devra ensuite faire autoriser la mesure par le Tribunal des mesures de contrainte dans les 24 heures à compter de l'ordre (art. 274 al. 1 CPP). A noter que, s'agissant de la condition, posée à l'art. 269 al. 1 let. a CPP, de l'existence d'un « **grave soupçon** », le Tribunal fédéral a rappelé à juste titre que selon les règles sur l'entraide judiciaire et la jurisprudence constante, les art. 14 CEEJ[255], 28 EIMP et 10 OEIMP[256] imposent à l'autorité requérante d'expliquer en quoi consistent ses soupçons, mais pas de les prouver ni même de les rendre vraisemblables. Sous réserve de l'interdiction des requêtes exploratoires, les soupçons de l'autorité requérante n'ont donc pas à être particulièrement graves ou précis. En effet, si le droit interne doit s'appliquer lorsqu'il est plus favorable à la coopération que le droit conventionnel, il ne saurait en revanche poser des conditions matérielles à l'entraide qui ne sont pas prévues par le droit conventionnel[257].

14 Le Tribunal des mesures de contrainte statue dans les cinq jours (art. 274 al. 2 CPP). En cas de refus de la surveillance, les documents et enregistrements collectés doivent être immédiatement détruits (art. 277 al. 1 CPP). Si l'autorisation est accordée, il faut relever que l'art. 279 CPP prévoyant la communication au prévenu ou au tiers objet de la surveillance et aménageant un droit de recours à ces derniers ainsi qu'au service de télécommunication surveillé (art. 279 al. 3 CPP) ne trouve pas application, malgré le renvoi de l'art. 18a al. 4 EIMP aux art. 269 à 279 CPP. En effet, les conventions et lois applicables dans le domaine de l'entraide judiciaire internationale en matière pénale dérogent au système usuel du CPP qui ne trouve application que s'il est plus favorable à la coopération que ces conventions et lois applicables (principe de faveur)[258]. Cela a notamment pour effet que **la qualité de partie, le droit à la notification ainsi que les voies de droit sont régis par les dispositions spécifiques en matière d'entraide**[259]. Or selon l'art. 80m al. 1

255. RS 0.351.1.

256. RS 351.11.

257. Arrêt du Tribunal fédéral 1C_558/2017 du 21 novembre 2017 consid. 1.2 relatif à des écoutes téléphoniques mais parfaitement transposable en matière informatique. C'est le lieu de rappeler que la CEEJ reste applicable même aux demandes d'entraide présentées dans l'une des matières traitées par la CCC. En effet, la CCC, a pour but, selon son préambule, de compléter les conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, « en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale ».

258. Arrêt du Tribunal fédéral 1C_558/2017 du 21 novembre 2017 consid. 1.2.

EIMP, les obligations de notifier les décisions en matière d'entraide sont limitées aux personnes résidant ou ayant élu domicile en Suisse. D'éventuelles indications contraires de la part du TMC, que ce soit par rappel de la loi ou par apposition de conditions au sens de l'art. 274 al. 2 CPP seraient donc invalides, faute de compétence du TMC pour connaître de cet aspect de la procédure[260]. Il reviendra à l'autorité d'exécution, dans le cadre de la procédure d'entraide judiciaire de veiller au respect de ces conventions et lois applicables et de procéder aux seules notifications prévues par l'art. 80m EIMP.

15 A réception des données issues de la surveillance, l'autorité d'exécution devra garantir le droit d'être entendu de la personne touchée par la mesure de surveillance (art. 80b EIMP). On verra en effet que, s'agissant de données relatives au contenu, toute **transmission anticipée**, c'est-à-dire avant l'entrée en force d'une décision de clôture, **est en principe exclue** (cf. *infra* III.B.1.). Dès lors que la mesure de contrainte en question est par essence secrète, sa divulgation à la personne touchée peut se révéler lourde de conséquence pour la procédure à l'étranger. Il y a lieu de distinguer deux cas de figure :

1. Si la personne visée par la mesure n'est pas domiciliée en Suisse ou n'y a pas élu domicile, la décision de l'autorité n'a pas à lui être notifiée (art. 80m al. 1 EIMP). La décision de clôture ne sera ainsi notifiée qu'à l'OFJ (art. 80h let. a EIMP) ce qui permet une transmission à l'autorité requérant du résultat de la surveillance sans que la personne concernée n'en ait été effectivement informée. Bien entendu, si la personne concernée se manifeste auprès de l'autorité d'exécution en ayant élu domicile en Suisse avant l'entrée en force de la décision de clôture, son droit de participer à la procédure et d'accéder au dossier devra lui être garanti (art. 80b al. 1 en lien avec l'art. 80m al. 2 EIMP).

2. Si la personne visée par la mesure est domiciliée en Suisse ou y a élu domicile, l'autorité d'exécution devra lui garantir le droit de participer à la procédure et de consulter le dossier (art. 80b al. 1 EIMP ; sous réserve du cas particulier de l'utilisation d'une fausse identité, cf. *infra* III.B.3) avant toute

259. Dans ce sens : arrêt du Tribunal pénal fédéral RR.2015.142-143/RR.2015.144-145 du 30 octobre 2015 consid. 5.2.2 ; arrêt du Tribunal fédéral 1C_36/2015 du 19 janvier 2015.

260. Dans ce sens : arrêts du Tribunal fédéral 1B_563/2011, 1B_631/2011 et 1B_633/2011 du 16 janvier 2012 consid. 2.3.

transmission du moyen de preuve à l'étranger. Rien n'oblige néanmoins l'autorité requérante à octroyer ce droit à la personne concernée dès la fin de la mesure de surveillance. La mesure peut demeurer secrète aussi longtemps que nécessaire pour la procédure à l'étranger. Il s'agira pour l'autorité d'exécution de s'assurer auprès de l'autorité requérante du moment où l'existence de la mesure de surveillance peut être dévoilée pour permettre la poursuite de la procédure d'entraide.

16 A l'issue de la procédure, l'autorité d'exécution rendra **une décision de clôture** susceptible de **recours** au Tribunal pénal fédéral (art. 80e EIMP). Un recours subséquent au Tribunal fédéral demeure possible aux conditions restrictives de l'art. 84 LTF[261] (cas particulièrement important).

B. Distinctions et cas particuliers

1. Transmission anticipée des données relatives au contenu ?

17 A certaines conditions, l'art. 18b EIMP permet la transmission anticipée – c'est-à-dire avant le prononcé d'une décision de clôture - de données relatives au trafic informatique recueillies en vertu d'un ordre de surveillance en temps réel qui a été autorisé. L'art. 18b EIMP constitue la mise en œuvre des obligations découlant de l'art. 33 CCC. S'agissant de données relatives au contenu néanmoins, le Tribunal fédéral a eu l'occasion de confirmer que l'art. 18b EIMP ne trouvait pas application et que par conséquent toute **transmission anticipée**, c'est-à-dire avant l'entrée en force d'une décision de clôture, **est exclue** sur la base de cette disposition[262]. La Suisse se voit ainsi privée d'un outil important dans la lutte contre la criminalité internationale, en particulier la criminalité organisée et le terrorisme. On peut également se demander si, avec cette interprétation du Tribunal fédéral, l'art. 18a EIMP dispose encore d'une réelle portée et utilité pratiques.

18 En 2021, le législateur a néanmoins introduit de nouvelles dispositions qui pallient en partie cet écueil et qui constituent un pas important vers des règles assouplies et une entraide plus rapide et réactive fondée sur la confiance internationale[263]. **L'art. 80d^{bis} EIMP (entraide dynamique)** permet, à titre exceptionnel, une transmission anticipée d'informations ou de moyens de

261. RS 173.110.
262. ATF 140 IV 181 consid. 2 ; v. aussi Message CCC, 4314.
263. Ludwiczak, p. 71–75.

preuve (a) lorsque les enquêtes étrangères portant sur des affaires de criminalité organisée ou de terrorisme seraient excessivement difficiles sans cette mesure d'entraide judiciaire, notamment en raison du risque de collusion, ou parce que la confidentialité de la procédure doit être préservée, ou (b) afin de prévenir un danger grave et imminent, notamment la commission d'un acte terroriste. Cette disposition vise à permettre une prévention efficace dans des cas urgents et fondés (par ex. prise d'otages ou attentat terroriste), en évitant une réaction trop tardive aux projets d'actes criminels, la confidentialité revêtant dans ce cadre une grande importance[264]. Sous l'angle matériel, à l'inverse de l'art. 18b EIMP qui limite la transmission anticipée aux seules données relatives au trafic informatique, voire aux données secondaires de télécommunication classique[265], l'art. 80d^{bis} EIMP prévoit que **tout type de moyen de preuve ou information** peut être transmis de manière anticipée par ce biais[266]. Sous l'angle formel, l'art. 80d^{bis} al. 4 EIMP exige que l'autorité d'exécution obtienne de l'autorité requérante certains engagements supplémentaires préalablement à toute transmission anticipée, notamment à n'utiliser les informations ou moyens de preuve qu'à des fins d'investigations et en aucun cas pour requérir, motiver ou prononcer une décision finale (let. a) et à retirer du dossier de la procédure étrangère, si l'entraide est refusée, les informations ou moyens de preuve remis de manière anticipée (let. c)[267]. Si toutes ces conditions sont remplies, rien ne s'oppose alors à une transmission anticipée de données relatives au contenu par le biais et aux conditions de l'art. 80d^{bis} EIMP.

Par ailleurs, une transmission anticipée de données relatives au contenu peut tout à fait intervenir dans le cadre et selon les règles d'une **équipe commune d'enquête (ECE ; ou *Joint Investigation Team, JIT* ; art. 80d^{ter} à 80d^{duodecies} EIMP)**. Dans ce cas, elle peut intervenir même si les conditions prévues à l'art. 80d^{bis} al. 1 let. a et b ou al. 2 EIMP ne sont pas remplies[268]. 19

264. Message terrorisme, 6527 s.
265. ATF 140 181, consid. 2.
266. V. Dangubic/Clerc, p. 291.
267. Pour une présentation plus complète de l'art. 80d^{bis} EIMP, voir Dangubic/Clerc, p. 287.
268. Cf. Ludwiczak Glassey/Bonzanigo, p. 407, qui estime cet avis « soutenable ».

2. Distinction entre un ordre de dépôt (art. 265 CPP) et une mesure de surveillance (art. 269 ss CPP), en particulier s'agissant des boîtes de courriel

20 Le secret des télécommunications est une garantie constitutionnelle consacrée à l'art. 13 al. 1 Cst. Ce droit constitue un aspect essentiel du droit au respect de la vie privée. La surveillance de la correspondance ainsi que des relations établies par la poste et les télécommunications constituent une atteinte grave à ce droit fondamental[269]. Il est dès lors essentiel de distinguer ce qui est couvert par cette garantie de ce qui ne l'est pas. A ce titre, on applique traditionnellement deux critères pour distinguer les cas où l'information peut être obtenue directement par un ordre de production à ceux où une demande LSCPT est nécessaire :

- le premier critère déterminant est le rapport avec la correspondance par télécommunication ;
- le second critère est celui de savoir si les données requises relèvent du droit fondamental au secret des télécommunications protégé par l'art. 13 al. 1 Cst.

21 La réunion des deux critères implique l'application de la LSCPT.

22 En pratique, la majorité des cas concernera **l'accès au contenu des boîtes de courrier électronique (courriel, email)**. Pour distinguer les données couvertes par le secret des télécommunications des données pouvant être obtenues directement par l'autorité pénale (ordre de dépôt au sens de l'art. 265 CPP), le Tribunal fédéral a posé le critère du moment du **dernier accès** (connexion, log) du destinataire du courriel à sa boite aux lettres électronique[270]. Le Tribunal fédéral retient que la procédure de communication doit être considérée comme se terminant au moment où le destinataire devient l'unique maître des données, c'est-à-dire au moment où ce dernier accède à sa boite de courriels, et ce indépendamment de savoir s'il a effectivement ouvert et pris connaissance des courriels reçus. En pratique, cela implique que le procureur pourra obtenir directement auprès du fournisseur de services le contenu des courriels antérieurs à la dernière connexion (art. 265 CPP), alors qu'il devra passer par le Service SCPT et le

269. Message LSCPT, 2481.
270. ATF 140 IV 181 consid. 2.

Tribunal des mesures de contrainte pour obtenir le contenu des emails postérieurs au dernier log (art. 269 ss CPP). En d'autres termes, c'est l'art. 31 CCC (entraide concernant l'accès aux données stockées) et non l'art. 34 CCC qui s'applique à la récolte et à la transmission des courriels antérieurs au dernier log.

3. Utilisation d'une fausse identité

23 A notre sens, ne devrait pas se voir reconnaitre la qualité de partie à la procédure d'entraide celui qui, pour commettre une infraction, utilise un compte auprès d'une plateforme (application de messagerie, boîte de courriels, etc.) garantissant un degré élevé de confidentialité (type chiffrement des données de bout en bout [*end-to-end encryption*], parfois couplé d'un chiffrement de type zéro-accès [*zero-access encryption*], pas ou peu de données requises à l'enregistrement, etc.), rendant ainsi son identification pour les autorités pénales plus difficile. En effet, en l'absence de toute identification initiale, il n'existe que peu de moyens de vérifier que la personne qui prétend à cette qualité soit réellement l'utilisatrice de cette ressource[271].

Les auteurs ont rédigé la présente contribution à titre personnel. Les appréciations et opinions présentées sont les leurs et n'engagent pas le Ministère public de la Confédération.

BIBLIOGRAPHIE

Aepli Michael, commentaire de l'art. 18a EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1ère édition, Bâle 2015.

Dangubic Miro/Clerc Yves, Art. 80d^{bis} IRSG – ein Überblick, forumpoenale 4 (2022) p. 287-292.

Ludwiczak Glassey Maria/Bonzanigo Francesca, L'artificielle distinction entre « informations » et « moyens de preuve » en entraide pénale internationale, Revue Pénale Suisse 140 (2022) p. 402-427.

271. Dans ce sens : voir arrêt du Tribunal fédéral 1C_626/2015 du 8 décembre 2015 consid. 1.5 transposable à ce cas particulier.

Ludwiczak Maria, L'entraide pénale internationale 'dynamique' en bref. Le projet, les débats, le compromis, Pratique juridique actuelle, 1 (2021) p. 71–75.

Zimmermann Robert, La coopération judiciaire internationale en matière pénale, 5e édition, Berne 2019.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, Internationale Rechtshilfe, 2e édition., Zurich et al. 2015.

MATÉRIAUX

Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 27 février 2013, FF 2013 2379, consultable sous https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2013/512/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2013-512-fr-pdf-a.pdf, consulté en janvier 2024 (cité : Message LSCPT).

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité du 18 juin 2010, FF 2010 4275, consultable sous https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2010/813/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2010-813-fr-pdf-a.pdf, consulté en janvier 2024 (cité : Message CCC).

Message relatif à l'arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe pour la prévention du terrorisme et de son Protocole additionnel et concernant le renforcement des normes pénales contre le terrorisme et le crime organisé, FF 2018 6469 ss, consultable sous https://www.fedlex.admin.ch/eli/fga/2018/2301/fr, consulté en janvier 2024 (cité : Message terrorisme).

Rapport explicatif de la Convention sur la cybercriminalité du 23 novembre 2001, Conseil de l'Europe, Série des traités européens – no 185, consultable sous https://rm.coe.int/16800ccea4, consulté en janvier 2024 (cité : Rapport explicatif du Conseil de l'Europe).

Rapport explicatif relatif à la révision totale de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT; RS 780.11) du Service Surveillance de la correspondance par poste et télécommunication, consultable sous https://www.li.admin.ch/sites/default/files/2018-02/Rapport_explicatif_OSCPT.pdf, consulté en janvier 2024 (cité : Rapport explicatif OSCPT).

Recommandation n° R (85) 10 du Comité des Ministres aux États membres concernant l'application pratique de la convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications du 28 juin 1985, consultable sous : https://rm.coe.int/09000016804e3071, consulté en janvier 2024 (cité : Recommandation no R (85) 10).