



COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

COMMENTAIRE

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

Un commentaire de Jérémie Müller
Edité par Damian K. Graf

État du traitement : 29.07.2026
PDF créé le : 06.10.2026
DOI: 10.17176/20260729-162745-0

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	4
II. Système informatique (Let. A).....	4
A. Un dispositif	5
B. Un programme	6
C. Un traitement des données automatique.....	6
D. Perspectives	7
1. La dématérialisation des systèmes informatiques	7
2. L'Internet des objets (IoT)	7
3. L'intelligence artificielle	8
III. Données informatiques (let. b)	9
A. La forme des données	9
B. Les types de données	9
C. Les programmes	10
D. Perspectives	10
E. Excursus : la distinction entre données relatives à l'abonné, données relatives au trafic et données de contenu en droit pénal suisse	11
1. Les données relatives à l'abonné	11
2. Les données relatives au trafic (ou données secondaires)	11
3. Les données de contenu	12
IV. Fournisseur de Services (let. c)	13
A. Les fournisseurs d'accès.....	13
B. Les fournisseurs de stockage ou de contenu.....	14
C. Perspectives	15
V. Données relatives au trafic (let. d)	15
Bibliographie	17
Travaux législatifs.....	17

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 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.
- 4 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
- 5 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*.

1. Rapport explicatif de la Convention sur la cybercriminalité, n. 22.

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

3. T-CY Note d'orientation 1, ch. 3

A. Un dispositif

- 6 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.
- 7 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 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 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.

4. Egalement appelé CPU (*Central Processing Unit*).

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*).

- 12 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.

B. Un programme

- 13 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.
- 14 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.
- 15 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.
- 16 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.
- 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

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

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.

D. Perspectives

1. La dématérialisation des systèmes informatiques

- 21 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.
- 22 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.
- 23 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 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

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

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

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.

3. L'intelligence artificielle

- 27 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.
- 28 **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.
- 29 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 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 2⁸, 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 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, « 1110011011111011000000 ». Cette donnée de 24 bits permet au programme de dessin d'afficher un pixel couleur abricot sur la page blanche.
- 33 Les exemples qui précèdent illustrent que, en informatique, la donnée 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

- 34 La définition de l'art. 1 let. b CCC n'opère **pas de distinction** entre les différents types de données. Toutes les données informatiques sont concernées, qu'elles soient personnelles ou non, privées ou

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

11. Rapport explicatif sur la Convention sur la cybercriminalité, n. 25.

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.

- 35 Aux données créées par l'humain il faut à notre avis ajouter celles qui sont 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

- 39 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,

12. Binary digit.

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.

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

- 40 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 1^{er} janvier 2002. Elle a été entièrement révisée en 2016, puis a subi plusieurs révisions partielles, dont notamment une importante en 2024.
- 41 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*).
- 42 La Convention sur la cybercriminalité opère cette même distinction à son article 18.

1. Les données relatives à l'abonné

- 43 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 la profession de l'utilisateur (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 principe¹⁵, 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

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

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.

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-publié¹⁶.

- 48 La Convention sur la cybercriminalité les définit à l'art. 1 let. d CCC. Elles seront examinées en détail au chapitre V ci-dessous¹⁷.
- 49 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).
- 50 L'obtention de ces données n'est en outre possible qu'avec l'**autorisation** du Tribunal des mesures de contrainte (art. 274 CPP).

3. Les données de contenu

- 51 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.
- 52 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.
- 53 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.
- 54 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. 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).

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.

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.
- 59 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
- 60 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.
- 61 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.

- 62 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 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 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.
- 68 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.
- 69 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

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

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

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

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*).

- 70 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.

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 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

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

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

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

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.

- 74 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.
- 75 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.
- 76 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.
- 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

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

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).