



COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

COMMENTAIRE

Art. 34 CCC (Convention sur la cybercriminalité [Cybercrime Convention])

Un commentaire de Nicolas Bottinelli / Julien Wenger
Edité par Damian K. Graf

État du traitement : 09.03.2024
PDF créé le : 06.10.2026
DOI: 10.17176/20240309-093848-0

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.....	3
II. Notions.....	3
III. Mise en œuvre en droit suisse.....	5
A. L'interception des données relatives au contenu en droit suisse	5
B. Distinctions et cas particuliers.....	7
1. Transmission anticipée des données relatives au contenu ?	7
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	8
3. Utilisation d'une fausse identité	9
Bibliographie.....	9
Matériaux.....	9

I. INTRODUCTION

- 1 Figurant au chapitre III de la Convention sur la Cybercriminalité¹ 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**.
- 2 La CCC reconnaît 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 télécommunications².
- 3 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 télécommunications³. Le Deuxième Protocole additionnel à la CCC, du 12 mai 2022⁴, ne traite pas de cette mesure, pas plus que les travaux préparatoires au 3^e Protocole additionnel à la CEEJ.

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 débuts⁵.
- 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)⁶. 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

1. RS 0.311.43 ; citée dans la suite de la contribution sous « CCC » ou « la Convention ».

2. Rapport explicatif du Conseil de l'Europe, n. 228.

3. Recommandation no R (85) 10.

4. 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).

5. Rapport explicatif du Conseil de l'Europe, n. 297 et Message CCC, 4314

6. Rapport explicatif du Conseil de l'Europe, n. 209.

la rubrique « objet »⁷⁾, 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 EIMP⁸, ce qui est exclu en matière de données relatives au contenu (cf. *infra* III.B.1.)⁹.

- 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 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*)¹⁰ ; 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.
- 7 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 incertaine¹¹, 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).
- 8 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 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 illicites¹². A l'évidence, ce terme ne signifie pas qu'il soit

7. 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).

8. RS 351.1.

9. ATF 143 IV 186 consid. 2.3.

10. 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).

11. 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 ».

12. 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.

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 téléphonie 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 informatique¹³.

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 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.
- 11 **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 requérante¹⁴, 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)¹⁵. 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)¹⁶.
- 12 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 OSCPT¹⁷). Il sera ainsi possible d'ordonner la surveillance en temps réel du contenu et des données secondaires de

13. Rapport explicatif du Conseil de l'Europe, n. 206.

14. BSK-Aeppli, 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.

15. RS 780.1.

16. BSK-Aeppli, art. 18a EIMP, n. 10.

17. RS 780.11.

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).

- 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 CEEJ¹⁸, 28 EIMP et 10 OEIMP¹⁹ 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 conventionnel²⁰.
- 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)²¹. 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**²². 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 procédure²³. 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

18. RS 0.351.1.

19. RS 351.11.

20. 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 ».

21. Arrêt du Tribunal fédéral 1C_558/2017 du 21 novembre 2017 consid. 1.2.

22. 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.

23. Dans ce sens : arrêts du Tribunal fédéral 1B_563/2011, 1B_631/2011 et 1B_633/2011 du 16 janvier 2012 consid. 2.3.

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 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 LTF²⁴ (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 disposition²⁵. 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 internationale²⁶. **L'art. 80d^{bis} EIMP (entraide dynamique)** 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. Cette disposition vise à

24. RS 173.110.

25. ATF 140 IV 181 consid. 2 ; v. aussi Message CCC, 4314.

26. Ludwiczak, p. 71–75.

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 importance²⁷. 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 classique²⁸, l'art. 80d^{bis} EIMP prévoit que **tout type de moyen de preuve ou information** peut être transmis de manière anticipée par ce biais²⁹. 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)³⁰. 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.

- 19 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 remplies³¹.

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 fondamental³². 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 boîte aux lettres électronique³³. 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 boîte de courriels, et ce indépendamment de savoir s'il a effectivement ouvert et pris connaissance

27. Message terrorisme, 6527 s.

28. ATF 140 181, consid. 2.

29. V. Dangubic/Clerc, p. 291.

30. Pour une présentation plus complète de l'art. 80d^{bis} EIMP, voir Dangubic/Clerc, p. 287.

31. Cf. Ludwiczak Glassey/Bonzanigo, p. 407, qui estime cet avis « soutenable ».

32. Message LSCPT, 2481.

33. ATF 140 IV 181 consid. 2.

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 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 reconnaître 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 zéroaccès [*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 ressource³⁴.

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

Aeppli Michael, commentaire de l'art. 18a EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1^{ère} 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.

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, 5^e édition, Berne 2019.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, *Internationale Rechtshilfe*, 2^e 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).

34. Dans ce sens : voir arrêt du Tribunal fédéral 1C_626/2015 du 8 décembre 2015 consid. 1.5 transposable à ce cas particulier.

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).