



COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

COMMENTAIRE

Art. 33 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: 10.17176/20240309-093618-0

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.....	3
II. Notions.....	4
III. Mise en œuvre en droit suisse.....	6
A. L'art. 18b EIMP	6
1. Historique.....	6
2. Définitions	6
3. Procédure.....	6
4. Quelques délimitations matérielles	9
B. Distinctions.....	10
Bibliographie	11
Matériaux.....	11

I. INTRODUCTION

- 1 Figurant au chapitre III de la Convention sur la Cybercriminalité¹ 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.
- 2 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 Parties².
- 3 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 zéroaccès (*zero-access encryption*), mais aussi par l'absence de conservation des journaux de connexion (*logs*)³, de telle sorte que ni une surveillance rétroactive des données relatives au trafic, ni la 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 nationale⁴, solution que la Suisse n'a pas décidé d'adopter⁵.
- 5 Au niveau du droit procédural national justement, la CCC oblige les Etats parties à adopter des mesures législatives qui se révèlent nécessaires pour habilitier 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,

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. 295.

3. 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.

4. Rapport explicatif du Conseil de l'Europe, n. 296.

5. Cf. *infra* III.A.3.

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 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-même⁶. 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 instantanée⁷. 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 communication⁸.
- 7 La définition même des « données relatives au trafic » n'a pas été expressément reprise par le législateur suisse dans le cadre de la mise en œuvre de la Convention (en particulier à l'art. 18b EIMP⁹ ; 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 »¹⁰. Depuis le 1^{er} septembre 2016¹¹, le droit suisse définit les « **données secondaires de télécommunication** » (art. 273 CPP renvoyant à l'art. 8 let. b LSCPT¹²) 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 général¹³ - et non uniquement au trafic informatique -, elle couvre la notion de données relatives au trafic¹⁴. 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 intervenues¹⁵. Cette temporalité directe implique l'absence de prise sur ces

6. Rapport explicatif du Conseil de l'Europe, n. 28.

7. Rapport explicatif du Conseil de l'Europe, n. 30.

8. BSK-Böhi, art. 18b EIMP, n. 4.

9. RS 351.1.

10. Message CCC, 4316 s., citant S. Bondallaz : La protection des personnes et de leurs données dans les télécommunications, n. 1821 et 1823, p. 518.

11. Date d'entrée en vigueur de la LSCPT révisée.

12. RS 780.1.

13. Cf. *infra* III.A.4.

14. Message LSCPT, 2434.

15. 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).

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*)¹⁶. 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 destinée¹⁷. 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 trafic¹⁸. Cette disposition ne saurait donc justifier une recherche indéterminée de moyens de preuve (« *fishing expedition* »). De l'avis des auteurs, sont également « associés à une communication spécifique » au terme de cette disposition les journaux des connexions à une boîte 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 communication¹⁹, 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 déconnexion²⁰. 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 données²¹. 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**

16. 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).

17. Rapport explicatif du Conseil de l'Europe, n. 219.

18. Rapport explicatif du Conseil de l'Europe, n. 219.

19. 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.

20. Message CCC, 4316 s., citant S. Bondallaz : La protection des personnes et de leurs données dans les télécommunications, n. 1821 et 1823, p. 518.

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. 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 informatique²².

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 Suisse²³. 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 CCC²⁴.

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)²⁵. 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 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 jugée²⁶. 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

- 15 L'art. 18b al. 1 let. b EIMP renvoie aux art. 269 à 281 CPP et donc notamment, s'agissant de surveillance de données secondaires de télécommunication, à l'art. 273 CPP. Ce dernier prévoit en

21. Arrêt du Tribunal fédéral 1B_142/2016 consid. 3 et ATF 143 IV 21.

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

23. Message CCC, 4276.

24. FF 2010 4275, 4311 s.

25. 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).

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 télécommunication²⁷. 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 OSCPT²⁸).
- 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 OEIMP²⁹ 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 conventionnel³⁰.
- 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 l'autorisation est accordée, il faut relever que l'art. 279 CPP prévoyant la

26. 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.

27. 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).

28. RS 780.11.

29. RS 351.11

30. 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 ».

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)³¹. 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**³². 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 procédure³³. 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.

- 20 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 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 posteriori³⁴. 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 identité³⁵, 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

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

32. 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.

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

34. Donatsch/Heimgartner/Meyer/Simonek, p. 55 s.

35. Dans ce sens : arrêt du Tribunal fédéral 1C_626/2015 du 8 décembre 2015 consid. 1.4 s.

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 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.

- 24 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 cauteles de l'art. 18b al. 2 EIMP sont respectées³⁶. Un recours au Tribunal fédéral demeure possible aux conditions restrictives de l'art. 84 LTF³⁷ (cas particulièrement important). Une partie de la doctrine soutient qu'en cas d'admission du recours, les informations transmises doivent être retirées du dossier étranger³⁸. 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 EIMP³⁹.
- 25 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.

4. Quelques délimitations matérielles

- 26 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 boîte de courriel peut être obtenu au moyen d'une surveillance en temps réel⁴⁰ 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).
- 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 conventionnelle⁴¹.
- 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**⁴². 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

36. 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).

37. RS 173.110.

38. Donatsch/Heimgartner/Meyer/Simonek, p. 56.

39. 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*.

40. Art. 58 OSCPT.

41. ATF 143 IV 186, consid. 2.3 ; v. aussi Hansjakob/Pajarola, art. 272 CPP, n. 39-41.

42. 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 rapporte pas aux données sur la téléphonie, celles-ci étant couverte par l'art. 18a EIMP (Message CCC, 4316 s.).

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 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)⁴³.
- 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 internationale⁴⁴. Du point de vue du champ d'application matériel, l'art. 18b EIMP ne connaît aucune limitation, alors que l'art. 80d^{bis} EIMP se limite, sauf danger grave et imminent, à la criminalité organisée et au terrorisme⁴⁵. 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 biais⁴⁶, 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 téléphonique⁴⁷. 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 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)⁴⁸.
- 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,**

43. Pour plus de détails, cf. BSK-Glutz, art. 67a EIMP ou encore Ludwiczak Glassey/Bonzanigo, p. 402-427.

44. Ludwiczak, p. 75.

45. Cf. Ludwiczak Glassey/Bonzanigo, p. 402-427.

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

47. ATF 143 IV 186.

JIT ; **art. 80^{dter} à 80^{duodecies} EIMP**) ; en effet, le champ matériel restreint de l'art. 80^{bis} EIMP, ne s'applique pas, de l'avis des auteurs, aux équipes communes d'enquête, malgré le renvoi malheureux de l'art. 80^{octies} EIMP aux conditions de l'art. 80^{bis} EIMP⁴⁹.

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, 1^{ère} édition, Bâle 2015.

Dangubic Miro/Clerc Yves, Art. 80^{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, 1^{ère} 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, 3^e édition, Zurich 2020.

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, 5^e 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).

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

49. Cf. Ludwiczak Glassey/Bonzanigo qui estime cet avis « soutenable ».