Accès transfrontière aux preuves électroniques : l'avenir de l'entraide internationale en matière de cybercriminalité ?

Ludwiczak, Maria

How to cite

LUDWICZAK, Maria. Accès transfrontière aux preuves électroniques : l'avenir de l'entraide internationale en matière de cybercriminalité ? In: Lutter contre la cybercriminalité en Suisse. Perrier Depeursinge, Camille ; Métille, Sylvain ; Vuille, Joëlle (Ed.). Lausanne. Berne : Stämpfli, 2024. p. 117–130. (Collection lausannoise. CEDIDAC)

This publication URL: https://archive-ouverte.unige.ch/unige:181165

Accès transfrontière aux preuves électroniques : l'avenir de l'entraide internationale en matière de cybercriminalité ?

MARIA LUDWICZAK GLASSEY
Dr iur., Professeure
Facultés de droit, Universités de Genève et Neuchâtel

Table des matières

I. Introduction

Si l'on définit la cybercriminalité en fonction non pas du type d'infraction commise (par exemple l'accès indu à un système informatique, art. 143bis CP) ni selon le mode opératoire choisi par l'auteur (par exemple l'utilisation d'un site de rencontres en ligne afin de contacter le potentiel lésé d'une « arnaque aux sentiments » ou *romance scam*[1]), mais en fonction de la nature des preuves qu'il faut/faudra administrer afin d'établir les faits, l'on

[1] À ce propos, voir notamment la page dédiée de l'Office fédéral de la cybersécurité (OFSC), disponible sous : <https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/romance-scam.html> (*consulté le 15.03.2024*).

s'aperçoit que la quasi-totalité de la criminalité actuelle, y compris les infractions du droit pénal classique comme le meurtre ou le vol peut être qualifiée de « cyber ». En effet, qu'il s'agisse de messages, de courriels ou de fichiers, notamment de photographies, d'enregistrements audio ou de vidéos[2], force est de constater qu'il s'agit de moyens de preuve essentiels dans un monde numérique et interconnecté. Ces données numériques sont parfois enregistrées sur des supports locaux, comme un disque dur d'ordinateur. Plus souvent, elles sont (aussi) stockées dans des centres de données, éventuellement sur un *Cloud* (informatique en nuage). Elles se caractérisent alors par une accessibilité en tout temps et à distance, sans l'accord de, ni l'information à, la personne concernée. Par ailleurs, cette accessibilité peut les rendre éphémères : elles peuvent être créées, consultées, modifiées, voire supprimées.

Se pose la question de l'accès à ces preuves électroniques pour les besoins d'une procédure pénale. En l'absence d'élément d'extranéité, cette question relève du droit de la procédure pénale classique. Il n'est toutefois pas rare que le lieu de stockage se trouve dans un État autre que celui qui conduit la procédure pénale. Dans ce cas, l'on doit se demander si la voie de l'entraide judiciaire internationale en matière pénale, traditionnellement suivie s'agissant de preuves « classiques », doit être suivie ou s'il se justifie, au vu de la nature particulière des preuves électroniques, de prévoir une voie plus efficiente parce que, notamment, moins chronophage (*infra* II). Afin de répondre à cette question, l'on s'intéressera dans cette contribution aux modèles mis en place unilatéralement par les États-Unis d'Amérique, d'une part, et entre les États membres de l'Union européenne, d'autre part (*infra* III) avant de s'interroger sur la situation en Suisse et les perspectives qui s'offrent à notre État (*infra* IV).

II. Preuves électroniques et entraide internationale : une inadéquation manifeste

A. Preuves électroniques : de quoi parle-t-on ?

Par les termes « preuves électroniques », nous entendons les données sauvegardées sur un support à distance, donc une donnée présentant un format numérique. Ces données peuvent être de trois sortes : on parlera de données relatives aux abonnés, de données relatives au trafic ou de données de contenu. Les données relatives aux abonnés permettent d'identifier une personne. Il peut s'agir par exemple d'un nom, d'un numéro de téléphone ou d'une adresse de l'abonné au service informatique. En d'autres termes, l'obtention de ces

[2] Sont en revanche exclues de la présente contribution les données bancaires, qui font l'objet de réglementations spécifiques. À ce propos, voir LASSALLE, p. 191 ss.

données permet de répondre à la question « qui » est concerné par les données en cause, qu'il s'agisse de l'auteur de l'infraction ou d'une personne autrement impliquée dans les faits commis. Les données relatives au trafic sont des données caractérisant le contenu : elles permettent de comprendre « comment » les données ont été générées. En particulier, il s'agira de déterminer quelle est la nature de la connexion utilisée, combien de temps celle-ci a duré, avec qui l'abonné a communiqué. On parle à ce titre également de données accessoires ou secondaires, ou de métadonnées. Finalement, les données de contenu sont l'information elle-même (« quoi ») : le texte du message ou de l'*email*, la vidéo, l'enregistrement audio, la photographie.

Les données peuvent être interceptées au moment où elles sont générées ; nous avons toutefois exclu volontairement cette forme d'interception de la présente contribution[3]. Elles peuvent aussi, et c'est plus fréquemment le cas, être obtenues *a posteriori* auprès des fournisseurs informatiques alors qu'elles sont déjà stockées.

B. Procédure d'entraide *vs* preuves électroniques

Encadrée par des règles strictes, l'entraide judiciaire internationale en matière pénale dans sa forme classique implique l'interaction de deux États, requérant et requis : les autorités du second exécutent la demande qui leur est adressée par le premier pour les besoins d'une procédure pénale. Toutefois, présenter une demande d'entraide présuppose de savoir à quel État l'adresser, donc de savoir dans quel État se trouvent les éléments nécessaires. Or le lieu d'enregistrement des données électronique est aléatoire et dépend uniquement d'exigences logistiques liées au stockage. Par ailleurs, il n'est pas rare que les données soient fragmentées. Ainsi, l'*email* peut être stocké dans un *data center* localisé dans un État, pendant que la pièce jointe, par exemple le fichier vidéo, sera stockée dans un autre État. Moyennant d'identifier au préalable de quels États il s'agit, il n'est pas exclu de leur adresser des demandes d'entraide en sollicitant une mesure de contrainte, qu'il s'agisse de la perquisition des locaux où se trouvent les *data center* ou l'obtention des données de la part de la personne habilitée à les gérer, vraisemblablement un fournisseur de services les contrôlant, pour autant que le droit de ces États le permette.

[3] Elle est couverte par U.S. CLOUD Act, H.R. 4943, voir notamment Sec. 104 ; en revanche, le système *e-Evidence* exclut expressément l'interception des données de son champ d'application, par. 19 Règlement (UE) 2023/1543 du 12 juillet 2023 relatif aux injonctions européennes de production et de conservation concernant les preuves électroniques dans le cadre des procédures pénales, JO L 191 du 28 juillet 2023, p. 118-180) (ci-après : Règlement (UE) 2023/1543). En droit suisse, elle se fonde sur les art. 269 ss CPP, voir *infra*.

Cela étant dit, il ne nous semble pas utile, tant cela est évident, de rappeler combien la procédure d'entraide internationale est chronophage. Les mois voire années nécessaires pour obtenir une information s'accordent mal avec le caractère éphémère, déjà mentionné, des données en cause, en particulier le risque que les données de contenu soient modifiées ou supprimées.

L'entraide internationale dans sa forme classique, attachée à la souveraineté des États, ne constituant pas une solution efficace à la problématique posée par les preuves électroniques, se pose la question pour les autorités pénales de la possibilité d'un accès simplifié, à distance, n'impliquant pas les autorités de l'État de localisation des données, voire n'impliquant pas la détermination de ce lieu. Doit alors être envisagée l'opportunité de renoncer au critère de la localisation physique des données au profit d'autres critères plus pertinents.

III. État des lieux à l'étranger

Deux systèmes vont être présentés ci-après, à savoir la solution adoptée unilatéralement par les États-Unis d'Amérique véhiculée par le *U.S. Clarifying Lawful Overseas Use of Data* (abrégé *CLOUD*) *Act* de 2018 (*infra* A) ainsi que le système *e-Evidence* mis en place en juillet 2023 entre les États membres de l'Union européenne (*infra* B). Ces exposés ne se veulent pas exhaustifs, mais visent à donner au lecteur un aperçu des solutions en vigueur à l'étranger, dans le but de poser les bases des réflexions menées en fin de la présente contribution (*infra* IV)[4].

A. Aux États-Unis d'Amérique : *U.S. CLOUD Act*

La communication des données par les fournisseurs informatiques aux autorités pénales des États-Unis d'Amérique se fondait jusqu'à récemment sur le *Stored Communications Act*[5] adopté dans les années 80 du siècle passé. En adéquation avec les besoins au moment de son adoption, cette loi ne traitait pas de la question des données électroniques stockées physiquement à l'étranger. Les autorités pénales américaines obtenaient lesdites données de la part des fournisseurs informatiques américains sans qu'ils ne manifestent de réticences.

Ce n'est qu'en 2016 que *Microsoft* a refusé pour la première fois de fournir des données numériques, en l'occurrence des *emails*, à une autorité de poursuite

4 Pour approfondir, voir (en général) BIASIOTTI *et al.*, p. 13 ss ; GIACOMETTI, p. 459 ss ; LUDWICZAK GLASSEY ; PFEFFER ; (pour des rapports nationaux) SIEBER/VON ZUR MÜHLEN/TROPINA, Vol. I, p. 127 ss et Vol. II.

5 18 U.S.C., § 2701 ss.

américaine qui les sollicitait dans le cadre d'une procédure pénale conduite en matière de stupéfiants. Le motif invoqué pour motiver le refus résidait dans la localisation géographique des données, stockées dans un *data center* en Irlande. *Microsoft* a indiqué ne pas pouvoir fournir lesdites données sans porter atteinte à la souveraineté de cet État et a préconisé à l'autorité requérante de passer par la voie de l'entraide internationale. En 2018, avant que la Cour suprême américaine statue sur la question – le litige ayant occupé diverses instances au préalable, avec des réponses variées[6] – une loi venant compléter le *Stored Communications Act* a été adoptée : le *U.S. CLOUD Act*[7].

Le système mis en place repose sur deux principes essentiels. D'une part, la localisation physique des données électroniques, *i.e.* leur lieu de stockage – qu'il soit aux États-Unis ou à l'étranger, n'est pas pertinent (*U.S. CLOUD Act*, Sec. 103). D'autre part, tout fournisseur présent sur sol américain a l'obligation de fournir les données dont il dispose lorsqu'elles sont requises par une autorité de poursuite pénale américaine (*U.S. CLOUD Act*, Sec. 103). En d'autres termes, le critère de rattachement de la localisation physique des données est remplacé par celui, volontairement vague et large, de la présence du fournisseur de services sur sol américain. Par la notion de présence, l'on entend le siège, une filiale mais aussi toute autre forme de présence aux États-Unis. Sont visés les services fournis sur sol américain, l'activité économique qui y est déployée[8]. Les données concernées ne doivent pas nécessairement être contrôlées par le fournisseur de services lui-même : il peut en particulier s'agir d'une filiale sise à l'étranger. Tel est le cas indépendamment du fait de savoir si la maison-mère a ou non accès aux données[9].

L'obligation de remise des données n'est pas limitée à un certain degré de gravité des faits (en particulier la notion de *serious crime*, mentionnée en préambule du *CLOUD Act* [*U.S. CLOUD Act*, Sec. 101] ne semble pas être pertinente dans ce cas de figure[10]), ni à la nature des données (*i.e.* qu'elles soient relatives aux abonnés ou au trafic ou encore de contenu). Les données doivent être remises sur présentation, par l'autorité de poursuite, d'un *warrant*, délivré par

---

6 District Court for the Southern District of New York, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) ; Second Circuit Court of Appeals, 829 F.3d 197 (2d Cir. 2016).

7 18 U.S.C., § 2701 ss. Contrairement à ce que pourrait impliquer son intitulé, cette loi ne s'applique pas exclusivement aux données stockées sur un *Cloud*.

8 À ce propos, voir U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, Avril 2019, p. 8 et 17. Voir aussi notamment MIGNON, p. 111 et 113.

9 U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, Avril 2019, p. 16-17.

10 Cette notion n'est toutefois pas définie dans le *U.S. CLOUD Act* ; le critère trouve application uniquement en lien avec un *Executive Agreement*. *U.S. CLOUD Act*, Sec. 105. *Contra* FISCHER/PITTET.

une autorité judiciaire américaine, qui se fonde sur la *probable cause*, *i.e.* en substance le fait que les données sont la preuve de la commission d'un crime[11]. Le fournisseur ne peut contester l'ordre de transmettre les données que dans un seul cas de figure, lié à l'existence d'un *Executive Agreement* et pour autant que la personne concernée par les données ne soit pas une *U.S. person*[12] ni ne réside sur le territoire des États-Unis (*U.S. CLOUD Act*, Sec. 103). L'exception a ainsi une portée très limitée. Cette exception ne vise pas à protéger la personne concernée par les données à remettre, mais éviter au fournisseur de service de se voir imposer des exigences contradictoires, *i.e.* l'obligation de remettre les données imposée par le *U.S. CLOUD Act* d'une part et, d'autre part, la potentielle interdiction de le faire, imposée par le droit de l'État où se trouvent les données, notamment en raison de normes applicables à la protection des données personnelles, tel par exemple le Règlement général sur la protection des données (RGPD[13]) au sein de l'Espace économique européen.

En tant que de très nombreux fournisseurs de services informatiques, en particulier les géants du *web*, ont leur siège aux États-Unis et que, pour le surplus, la notion de présence sur sol américain comprise généreusement[14] est susceptible d'englober les cas de figure restants, les autorités pénales américaines sont désormais assurées de pouvoir obtenir les données électroniques sans avoir recours à l'entraide internationale. Afin d'éviter aux fournisseurs de services d'être astreints à des obligations contradictoires, le processus de conclusion d'*Executive Agreements* est en cours. Les premiers, conclus avec le Royaume-Uni[15] et

11 U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, Avril 2019, p. 8 et 15.

12 Une *U.S. person* est « *a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States* », *U.S. CLOUD Act,,* Sec. 2523. Sur cette notion, voir MIGNON, p. 109.

13 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, JO L 119 du 4 mai 2016, p. 1-88. Sur la compatibilité entre les obligations découlant du *U.S. CLOUD Act* et du RGPD, voir notamment Office fédéral de la justice, Rapport sur le US CLOUD Act (loi *Cloud*), 17 septembre 2021, p. 23 ss. Voir aussi EDPB-EDPS, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 10 juillet 2019.

14 U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, Avril 2019, p. 17.

15 *Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime*, 3 octobre 2019.

l'Australie[16], sont déjà en vigueur, pendant que d'autres discussions sont en cours, notamment avec le Canada et l'Union européenne[17].

B. Entre les États de l'Union européenne : système *e-Evidence*

En parallèle au système permettant aux autorités américaines d'accéder aux données stockées dans des États étrangers, les États membres de l'Union européenne ont, eux aussi, mis en place une solution venant remplacer les formes préexistantes d'accès transnational aux données électroniques. Celles-ci, variant fortement entre les États membres, rendaient la problématique d'autant plus complexe et urgente à régler. Cette nécessité concernait non seulement les autorités pénales et le besoin d'une administration efficace des preuves afin de faciliter la lutte contre la criminalité, mais aussi les fournisseurs de services qui, bien qu'actifs au sein d'un espace caractérisé avant tout par un marché unique européen, étaient confrontés à des exigences potentiellement divergentes, voire contradictoires dans les différents États membres.

Ainsi, la question de l'accès transfrontière aux preuves électroniques a été réglée dans un Règlement et une Directive *e-Evidence* du 12 juillet 2023[18], dont l'entrée en vigueur est agendée au 18 août 2026. Ce que nous appellerons le « système *e-Evidence* » dans les lignes qui suivent s'articule en deux volets. Le premier volet consiste en la mise en place d'un critère de rattachement uniformisé. Tout comme aux États-Unis, la localisation physique du stockage des données n'a plus d'importance (art. 1 par. 1 Règlement *e-Evidence*), mais le critère choisi est différent : bien qu'il concerne le fournisseur de service, il porte non pas sur sa « nationalité » mais sur la question de savoir si le fournisseur propose des services dans l'espace européen (art. 2 par. 1 Règlement *e-Evidence*). Si tel est le cas, et il s'agit du deuxième volet de la solution mise en place, le fournisseur de services a l'obligation d'indiquer un établissement désigné ou annoncer un représentant légal dans un des États membres de l'Union européenne (art. 3 Directive *e-Evidence*). Ce représentant est l'unique interlocuteur des autorités pénales : il est chargé de répondre aux demandes des autorités pénales de tous les États membres portant sur l'intégralité des preuves

16 *Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime*, 15 décembre 2021.

17 À ce propos, voir BISMUTH, p. 689 ss ; BRIÈRE, p. 502 ss ; MIGNON, p. 115-116.

18 Règlement (UE) 2023/1543 ; Directive (UE) 2023/1544 du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales, JO L 191 du 28 juillet 2023, p. 181-190).

électroniques qu'il stocke ou qui sont stockées pour son compte (art. 3 par. 8 Règlement *e-Evidence*), indépendamment du lieu de stockage.

La fourniture de services dans l'Union européenne consiste dans le fait de permettre aux personnes physiques ou morales dans un État membre d'utiliser les services et avoir un lien substantiel, fondé sur des critères factuels spécifiques, avec cet État membre (art. 3 par. 4 Règlement *e-Evidence)*. Un lien substantiel est réputé exister lorsque le fournisseur de services dispose d'un établissement dans un État membre ou lorsqu'il existe un nombre significatif d'utilisateurs dans un ou plusieurs États membres ou encore lorsqu'il existe un ciblage des activités sur un ou plusieurs États membres (art. 3 par. 4 Règlement *e-Evidence*). La notion se définit ainsi de manière large et nombreux seront les fournisseurs de services astreints au système *e-Evidence*, voire rares seront ceux qui ne le seront pas.

Les demandes doivent être adressées directement par l'autorité pénale de l'État membre dit d'émission au représentant du fournisseur de services (art. 7 Règlement *e-Evidence*), au moyen d'un formulaire standardisé, appelé certificat d'injonction européenne de production (*European Production Order Certificate*, EPOC, art. 9 et Annexe I Règlement *e-Evidence*)[19].

Le fournisseur a l'obligation de transmettre toutes les données dont il dispose, les motifs de refus pouvant être invoqués par les autorités de l'État chargé de la mise en œuvre étant très limités (art. 10 Règlement *e-Evidence*). L'obligation porte sur les données relatives aux abonnés et au trafic ainsi que les données de contenu. Toutefois, en tant que les deux derniers types de données sont plus intrusifs, une autorité judiciaire de l'État d'émission doit valider la demande (art. 4 Règlement *e-Evidence*). Le EPOC est alors, en principe, transmis en parallèle à une autorité de l'État de mise en œuvre (art. 8 par. 1 Règlement *e-Evidence*)[20]. De plus, dans ce cas, l'application du mécanisme est limitée à un certain degré de gravité des faits (art. 5 par. 4 Règlement *e-Evidence*).

Le système *e-Evidence* supprime ainsi la nécessité de recourir à l'entraide internationale entre les États membres de l'Union européenne pour obtenir des preuves électroniques et pose des règles de procédure pénale communes[21]. Par ailleurs, au vu de la portée large du critère de rattachement choisi, rares seront les fournisseurs qui ne seront pas soumis au système et donc de fournir directement les données électroniques aux autorités pénales des États membres, y compris s'agissant de données hébergées hors du territoire de l'UE. Dans les (vraisemblablement rares) cas dans lesquels les conditions du système

19 Pour une critique de l'opportunité de procéder par le biais d'un formulaire standardisé, voir CASEY *et al*., p. 43 ss.

20 Voir toutefois les exceptions prévues à l'art. 8 par. 2 Règlement *e-Evidence*.

21 Pour une appréciation critique, voir CHRISTODOULOU *et al.*, p. 423 ss.

e-Evidence ne seraient pas réunies, les autorités pénales des États membres devront (continuer à) procéder par la voie classique de l'entraide internationale.

IV. État des lieux en Suisse

A. Les règles de la procédure pénale et la Convention cybercriminalité

L'accès par les autorités de poursuite pénale suisses aux fournisseurs de services électroniques est régi par le droit de procédure pénale[22]. Le système en place ne prévoit pas d'accès direct, mais désigne le Service Surveillance de la correspondance par poste et télécommunication (Service SCPT, art. 3 al. 1 LSCPT) comme intermédiaire compétent. Sur demande, le Service SCPT est chargé de recueillir les données auprès des fournisseurs puis de les transmettre à l'autorité de poursuite (art. 15 al. 1 LSCPT). Chaque fournisseur est tenu de désigner un service responsable de la surveillance et de la fourniture de renseignements auquel le Service SCPT adressera les demandes (art. 5 al. 1 *cum* 4 al. 1 OME-SCPT)[23]. En principe[24], toute surveillance de la correspondance par télécommunication, qu'elle porte sur des données relatives aux abonnés, au trafic ou au contenu, doit être validée par une autorité judiciaire, à savoir le Tribunal des mesures de contrainte (TMC ; art. 272 al. 1 et 273 al. 2 CPP). La procédure se fait en deux temps : l'autorité de poursuite ordonne la mesure et l'adresse au Service SCPT, puis dispose de 24 heures pour transmettre sa demande au TMC (art. 274 al. 1 CPP), qui statue dans les cinq jours (art. 274 al. 2 CPP) et communique sa décision tant à l'autorité de poursuite qu'au Service SCPT (art. 274 al. 3 CPP). Le fournisseur a l'obligation de transmettre les données requises au Service SCPT (art. 21 ss LSCPT) qui, lui-même, les transmet à l'autorité pénale requérante (art. 17 let. d LSCPT).

S'est posée la question de savoir quelle est la portée (extraterritoriale) des règles suisses de procédure pénale *i.e.,* d'une part, quel fournisseur est astreint à l'obligation de fournir et, d'autre part, quelles sont les données sur lesquelles porte ladite obligation, en particulier lorsqu'elles sont stockées à l'étranger. La jurisprudence a répondu à cette question en ce sens que l'obligation vise le seul fournisseur de services « soumis au droit suisse » et qui « contrôle » les données requises[25]. Le fait d'être soumis au droit suisse concerne notamment les

22 Sur cette notion, voir CR CPP-MÉTILLE, Intro. art. 269-281, N 26 ss.

23 Ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication du 15 novembre 2017 (OME-SCPT), RS 780.117.

24 Par exemple, l'identification des auteurs (22 LSCPT) n'y est pas soumise.

25 ATF 143 IV 21, consid. 3.4 ; TF, arrêt 1B_142/2016 du 16 novembre 2016, consid. 3.6. À ce propos, voir BENHAMOU/OETTLI, p. 214 ss.

sociétés dont le siège se trouve en Suisse et les filiales suisses d'un fournisseur de services étranger[26]. Les données doivent être contrôlées par cette entité, et non par exemple la maison mère (étrangère) de la filiale suisse[27], par quoi il y a lieu d'entendre que l'entité doit disposer d'« *un pouvoir de disposition, en fait et en droit, sur ces données* »[28]. À défaut, l'autorité de poursuite pénale suisse doit procéder par le biais de l'entraide judiciaire internationale en matière pénale. Les possibilités qui s'offrent aux autorités de poursuite suisses en vertu du droit de procédure pénale ne s'écartent ainsi pas, sur le principe, de celles dont disposent les autorités américaines et celles des États membres de l'Union européenne. Toutefois, le critère choisi en droit suisse a pour conséquence pratique que rares sont les fournisseurs qui sont astreints à l'obligation de transmettre les données. En effet, il n'existe que peu de fournisseurs suisses, respectivement peu d'entités soumises au droit suisse contrôlent les données stockées à l'étranger.

Au-delà des règles posées par le CPP, la Suisse applique la Convention sur la cybercriminalité (CCC), à laquelle sont également parties les États-Unis d'Amérique et quasiment tous les États membres de l'Union européenne[29]. La Convention pose des règles de base en matière de procédure pénale (art. 18 ss CCC) et d'entraide internationale (art. 23 ss CCC), qui ne vont toutefois pas au-delà de ce que permet le droit suisse interne. L'exception est l'art. 32 let. b CCC qui permet aux États parties, sans l'autorisation de l'autre État partie, d'« *accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique* ». L'art. 32 let. b CCC prévoit ainsi une possibilité d'accès transfrontière supplémentaire par rapport au CPP : les autorités pénales suisses peuvent accéder à des données stockées situées dans un autre État partie à la CCC, données qui ne seraient par hypothèse pas contrôlées par un fournisseur soumis au droit suisse. Toutefois, le mécanisme repose sur une base volontaire : le fournisseur de service peut, librement, refuser de fournir les données aux

26 Voir l'état de fait de l'ATF 143 IV 21.

27 BENHAMOU/OETTLI, p. 215.

28 ATF 143 IV 21, consid. 3.4 ; TF, arrêt 1B_142/2016 du 16 novembre 2016, consid. 3.6. Pour une discussion relative au critère de la localisation des données vs le pouvoir de contrôle sur les données, voir Jan SPOENLE, *Cloud Computing and cybercrime investigations : Territoriality vs. The power of disposal?, Discussion Paper, Council of Europe, Economic Crime Division, Project on Cybercrime*, 21 août 2010.

29 Convention sur la cybercriminalité du 23 novembre 2001 (CCC), RS 0.311.43. Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques du 12 mai 2022 (STCE n°224), n'a, quant à lui, en l'état pas été ratifié par la Suisse.

autorités de l'État partie[30]. Les demandes adressées par les autorités suisses aux fournisseurs américains sont traitées de la sorte depuis plusieurs années déjà, ce afin de désengorger les autorités exécutant les demandes d'entraide internationale[31]. Pour le surplus, nous ne nous rallions pas à l'avis de GRAF, selon lequel la disposition prévoit un mécanisme violant la souveraineté étrangère. En effet, la solution est prévue par une convention internationale librement ratifiée par les États parties et ne s'applique qu'entre lesdits États[32].

S'agissant du système *e-Evidence*, il ne fait pas partie des acquis de Schengen, ne fait pas l'objet d'un accord bilatéral entre l'UE et la Suisse et ne pourra en l'état être appliqué par la Suisse. Ainsi, les autorités suisses ne pourront s'adresser directement à l'établissement désigné ou au représentant légal dans l'Union européenne. Le système *e-Evidence* ne permet pas non plus à un État non-membre, en l'occurrence la Suisse, d'adresser une demande d'entraide à un État membre qui fera usage de l'EPOC pour l'exécuter (par. 23 des considérants et art. 2 par. 4 Règlement *e-Evidence*). En d'autres termes, le système *e-Evidence* ne permet pas de remplacer les règles applicables en matière de coopération internationale en matière pénale avec les États non-membres de l'Union[33].

B. Perspectives

Face au constat selon lequel les États-Unis d'Amérique et les États de l'Union européenne ont connu des évolutions majeures ces dernières années et que les autorités pénales de ces États ont désormais les moyens d'accéder largement aux preuves électroniques situées à l'étranger, l'on peut se demander quelles sont les perspectives pour la Suisse, dont le droit est bien plus restrictif. Se pose en particulier la question de l'opportunité de la conclusion d'un *Executive Agreement* avec les États-Unis, d'une part, et de négociations avec l'Union européenne, d'autre part.

La première solution, bien qu'elle permettrait aux fournisseurs américains, en application du *U.S. CLOUD Act*, de pouvoir s'opposer à la remise de données aux autorités américaines s'ils venaient à être soumis à des obligations incompatibles découlant du droit suisse (*U.S. CLOUD Act*, Sec. 103), ne permettrait

30 À propos du consentement, en particulier la question de savoir qui est habilité à le donner, voir ATF 141 IV 108, consid. 5.9-5.12, JdT 2015 IV 207 (trad.).

31 *U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World : The Purpose and Impact of the CLOUD Act, White Paper*, avril 2019, p. 5.

32 OK CCC-GRAF, art. 32, N 4.

33 Pour une analyse détaillée du droit de la coopération internationale en matière de surveillance des télécommunications, voir TOSZA, p. 270 ss ; WAHL, p. 11 ss.

vraisemblablement pas aux autorités suisses d'avoir un accès plus large aux données que ce qui est pratiqué actuellement[34]. Il faudrait pour cela que l'injonction suisse de produire ait un effet obligatoire pour les fournisseurs américains, ce qui dépendrait des négociations menées par les deux États[35]. De plus, l'*Executive Agreement* ne pourrait probablement concerner que des données relatives à des personnes soumises au droit suisse : là aussi la solution dépendrait des négociations entre les deux États[36]. Par ailleurs, seules des données ne concernant pas une *U.S. person* ou un résident américain pourraient être obtenues par cette voie (*U.S. CLOUD Act*, Sec. 103). Finalement, une telle solution ne serait pas sans poser de problème sous l'angle du droit de la protection des données personnelles.

Quant à l'adhésion de la Suisse au système *e-Evidence*, elle pourrait être très intéressante mais ne nous semble pas réaliste sans un certain nombre d'aménagements. À titre d'exemple, les motifs (résiduels) de refus prévus dans le Règlement *e-Evidence* renvoient à d'autres instruments du droit de l'Union européenne en matière de collecte des preuves notamment, dont le Règlement *e-Evidence* reprend les conditions et les mécanismes. La Suisse ne connait ni n'applique ces instruments, qui ne sont pas compatibles avec notre droit. Plus généralement, le système *e-Evidence* repose sur le principe de la confiance mutuelle, pierre angulaire des rapports entre les États membres de l'Union européenne dans le domaine pénal, principe qui ne s'applique pas dans les relations entre la Suisse et lesdits États[37]. Par ailleurs, l'on peut se demander quel pourrait être l'avantage de l'Union européenne à associer la Suisse à ce système. En tout état de cause, dans la mesure où des discussions sont en cours entre l'Union européenne et les États-Unis, il est, à ce stade, probablement plus judicieux d'attendre leur issue.

Cela étant, une solution pour la Suisse pourrait résider dans l'adaptation du droit de la procédure pénale et plus particulièrement des exigences fixées par la jurisprudence en la matière : si les critères choisis venaient à être adaptés aux réalités et besoins suisses, la voie de l'entraide internationale perdrait du terrain au profit de la procédure pénale et de l'accès unilatéral par les autorités pénales

---

34 En général sur la compatibilité du U.S. *CLOUD Act* avec le droit suisse et l'opportunité pour la Suisse de conclure un *Executive Agreement* avec les États-Unis d'Amérique, voir Office fédéral de la justice, Rapport sur le U.S. CLOUD Act (loi *Cloud*), 17 septembre 2021.

35 Tel n'est par exemple pas le cas dans l'*Executive Agreement* conclu avec le Royaume-Uni. Voir à ce propos Office fédéral de la justice, Rapport sur le U.S. CLOUD Act (loi *Cloud*), 17 septembre 2021, p. 24.

36 À propos de l'asymétrie existant dans l'accord avec le Royaume-Uni, voir Office fédéral de la justice, Rapport sur le U.S. CLOUD Act (loi *Cloud*), 17 septembre 2021, p. 24.

37 En général sur ce principe, voir les très nombreuses contributions doctrinales, dont la récente thèse de RIZCALLAH.

suisses. Il en serait ainsi en cas de suppression de l'exigence du contrôle sur les données ou du remplacement de la condition de la soumission de l'entité au droit suisse par celle de l'activité déployée en Suisse. De tels modèles, calqués sur le *CLOUD Act* et le système *e-Evidence*, seraient plus intrusifs dans la souveraineté étrangère que celui, plus respectueux, en vigueur en Suisse. Ils auraient aussi pour conséquence d'exiger d'une entité des données qu'elle ne contrôle pas. Ils se profileraient néanmoins dans le sens d'une procédure pénale transnationale, constituant possiblement l'avenir – par l'abandon – de l'entraide internationale en matière pénale.

V. Bibliographie

Lorena BACHMAIER, Mutual Admissibility of Evidence and Electronic Evidence in the EU, A New Try for European Minimum Rules in Criminal Proceedings?, Eucrim 2023 ; **Yaniv BENHAMOU/Jean-René OETTLI**, Traitement des données par les autorités pénales : de l'accès aux données à la procédure de tri, RPS 2021, p. 209 ss ; **Maria Angela BIASIOTTI/Jeanne P. MIFSUD BONNICI/Joe CANNATACI/Frabrizio TURCHI** (éds), Handling and Exchanging Electronic Evidence Across Europe, Cham 2018 ; **Régis BISMUTH**, Le Cloud Act face au projet européen *e-evidence* : confrontation ou coopération ?, Revue critique de droit international privé 2019, p. 681 ss ; **Chloé BRIÈRE**, EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments, European Papers 2021, N°1, p. 493 ss ; **Eoghan CASEY *et al.***, The Evolution of Expressing and Exchanging Cyber-Investigation Information in a Standardized Form, *in* Maria Angela BIASIOTTI/Jeanne P. MIFSUD BONNICI/Joe CANNATACI/Frabrizio TURCHI (éds), Handling and Exchanging Electronic Evidence Across Europe, Cham 2018, p. 43 ss ; **Hélène CHRISTODOULOU/Laetitia GAURIER/Alice MORNET**, La proposition e-evidence : révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire ?, European Papers 2021, N°1, p. 423 ss (cité : CHRISTODOULOU *et al.*) ; **Philipp FISCHER/Sébastien PITTET**, US CLOUD Act – un aperçu, 8.11.2021 (<www.swissprivacy.law/101>, *consulté le 29.11.2023*) ; **Mona GIACOMETTI**, La récolte transfrontière de preuves électroniques dans le contexte européen, Bruxelles 2023 ; **Damian K. GRAF** (éd.), Onlinekommentar Übereinkommen über die Cyberkriminalität (Cybercrime Convention), version du 26.10.2023 (<https://onlinekommentar.ch/de/kommentare/ccc32>, *consulté le 29.11.2023*) (cité : OK CCC-AUTEUR/E) ; **Maxime LASSALLE**, L'accès transnational aux données bancaires dans le cadre de l'enquête pénale, Bruxelles 2021 ; **Maria LUDWICZAK GLASSEY**, Preuves électroniques : état de la situation en Suisse face à l'avancée majeure du droit européen, Eucrim 2023, p. 204 ss ; **Yvan JEANNERET/André KUHN/Camille PERRIER DEPEURSINGE** (éds), Commentaire romand CPP, 2e éd., Bâle 2019 (cité : CR CPP-AUTEUR/E) ; **Emmanuelle MIGNON**, The CLOUD Act : Unveiling European Powerlessness, Revue européenne du droit 2020, N°1, p. 108 ss ; **Kristin PFEFFER**, Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln, Aktuelle nationale, europa- und völkerrechtliche Entwicklungen, Eucrim 2023, p. 170 ss ; **Cecilia RIZCALLAH**, The Principle of Mutual Trust in European Union Law, An Essential Principle Facing a Crisis of Values, Bruxelles 2022 ; **Ulrich SIEBER/Nicolas VON ZUR MÜHLEN/Thomas WAHL**, Rechtshilfe zur Telekommunikationsüberwachung, Berlin 2021 ; **Ulrich SIEBER/Nicolas VON ZUR MÜHLEN/Tatiana TROPINA** (éds), Access to Telecommunication Data in

Criminal Justice, A Comparative Legal Analysis, Vol. 1 et 2, 2e éd., Berlin 2021 ; **Stanislaw TOSZA**, Cross-Border Gathering of Electronic Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies, *in* Vanessa FRANSSEN/Daniel FLORE (éds), Société numérique et droit pénal, Belgique, France, Europe, Bruxelles 2019, p. 269 ss ; **Thomas WAHL**, Grundlagen : Internationale Zusammenarbeit in der Telekommunikationsüberwachung, *in* Ulrich SIEBER/Nicolas VON ZUR MÜHLEN/Thomas WAHL (éds), Rechtshilfe zur Telekommunikationsüberwachung, Berlin 2021, p. 11 ss.