Preuves électroniques : état de la situation en Suisse face à l'avancée majeure du droit européen

Maria Ludwiczak Glassey

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

This contribution is a comparison of the solution adopted in the European Union (EU) concerning cross-border access to electronic evidence and the Swiss law applicable in this area, based on a number of key features of the European system. It gives rise to a reflection on the prospects for relations between the European Union and Switzerland, in particular the opportunity for Switzerland to coordinate its rules with those of European law.

AUTHOR

Maria Ludwiczak Glassey

Professeure associée
Université de Genève

CITE THIS ARTICLE

Ludwiczak Glassey, M. (2023). Preuves électroniques : état de la situation en Suisse face à l'avancée majeure du droit européen. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-017

Published in eucrim 2023, Vol. 18(2) pp 204 – 209

https://eucrim.eu

ISSN:

CC BY ND

I. Introduction

L'aboutissement, en juillet 2023, du projet *e-Evidence* représente un pas fondamental dans la modernisation de l'accès transfrontalier aux preuves électroniques au sein de l'Union européenne. En effet, l'adoption du 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[1] (ci-après : Règlement *e-Evidence*) et de la 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[2] (ci-après : Directive *e-Evidence*) permet une adaptation de l'accès transfrontalier aux preuves, compte tenu de la nature dématérialisée des données. Cela crée une cohérence entre la nature des données et le processus à disposition des autorités de poursuite pénale des États membres de l'UE pour les obtenir.[3]

La présente contribution se propose de comparer, sur la base de quelques traits majeurs du système *e-Evidence*, la solution novatrice retenue dans l'Union véhiculée par le système *e-Evidence* et le droit suisse applicable en l'état à la matière :[4] la surveillance de la correspondance par télécommunications relevant du droit de la procédure pénale suisse, c'est-à-dire les art. 269 ss CPP[5] et la LSCPT[6].

Afin de limiter le champ de la contribution, ne sera abordée que la question de la production des preuves électroniques par le biais de l'injonction européenne de production (*European Production Order*, EPO), celle portant sur la conservation étant mise de côté. Par ailleurs, ne sera pas traitée la question de la surveillance en temps réel, celle-ci ne faisant pas partie du champ du système *e-Evidence* (art. 3 par. 8 Règlement *e-Evidence* : « données […] stockées par un fournisseur […] au moment de la réception d'un certificat »). Finalement, nous nous concentrerons sur les données électroniques requises au titre de moyens de preuve dans le cadre d'une procédure pénale en cours et pas pour l'exécution d'une sanction déjà prononcée, bien que ces cas de figure soient également couverts par le système *e-Evidence* (voir déjà l'intitulé du Règlement *e-Evidence*).

II. Quelques points de comparaison

Seront développés dans les lignes qui suivent quelques aspects essentiels du système *e-Evidence* permettant d'opérer une comparaison, non exhaustive, avec le droit suisse actuellement en vigueur régissant la transmission des preuves en format numérique pour les besoins d'une procédure pénale. Ainsi, seront traités tour à tour le type de données concernées et leur lieu de stockage physique (1.), la détermination du fournisseur de services astreint à l'obligation de fournir les données et la portée extraterritoriale de cette obligation (2.), le seuil de gravité des faits à partir duquel le système est applicable (3.), les modalités de contact avec le fournisseur de services (4.) et l'étendue de l'obligation de fournir les données (5.).

1. Données concernées et lieu de stockage

Le système *e-Evidence* concerne les « preuves électroniques », par quoi il faut entendre les données relatives aux abonnés, au trafic et au contenu stockées sous une forme numérique par un fournisseur de services ou pour le compte d'un tel fournisseur (art. 3 par. 8 Règlement *e-Evidence*). Les données relatives aux abonnés sont celles concernant l'identité d'un abonné ou d'un client (nom, date de naissance, adresse), les données de facturation et de paiement, le numéro de téléphone et l'adresse électronique fournis, mais aussi notamment les données relatives au type de service et à sa durée (art. 3 par. 9 Règlement *e-Evidence*). Certaines données, tels les adresses *IP* et les ports de provenance et l'horodatage pertinents, peuvent être

demandées à la seule fin d'identifier l'utilisateur (art. 3 par. 10 Règlement *e-Evidence*) et seront alors assimilées aux données relatives aux abonnés. Les données relatives au trafic sont celles qui concernent la fourniture d'un service proposé par le fournisseur, tels par exemple la source et la destination d'un message, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé, le type de compression, etc. (art. 3 par. 11 Règlement *e-Evidence*). Finalement, les données relatives au contenu sont toutes les données dans un format numérique (texte, voix, vidéos, images et son) qui ne sont relatives ni aux abonnés ni au trafic (art. 3 par. 12 Règlement *e-Evidence*). Selon le type de données, des régimes différenciés sont prévus, notamment en fonction du seuil de gravité des faits et s'agissant de la question de savoir si l'intervention d'une autorité judiciaire est nécessaire (*infra* II.3. et II.4.b).

Le droit suisse établit également une distinction entre les types de données concernées, mais ne connait que deux catégories, à savoir les données relatives au contenu, d'une part, et les données dites secondaires (ou métadonnées) visant l'identification, la localisation et les caractéristiques techniques de la correspondance[7], d'autre part. Les données secondaires au sens du droit suisse regroupent ainsi les données relatives aux abonnés, les données demandées à la seule fin d'identifier l'utilisateur et les données relatives au trafic désignées par le système *e-Evidence*. Les différences entre les régimes applicables sont moindres qu'en droit européen (*infra* II.3. et II.4.b).

Le système *e-Evidence* se caractérise par l'abandon du critère de la localisation des données. En d'autres termes, le lieu de stockage physique, c'est-à-dire l'endroit où se trouve le *data center* où les données sont enregistrées, n'est pas pertinent. Ainsi, que les données soient physiquement stockées dans un (ou plusieurs) État(s) de l'UE ou dans un État tiers n'a aucune pertinence. De même, le droit de la procédure pénale suisse, tel qu'interprété par le Tribunal fédéral suisse, permet l'accès des autorités suisses à des données stockées à l'étranger.[8] La possibilité de perquisitionner le *data center*, lorsqu'il se trouve sur le sol suisse est réservée (art. 244 ss CPP), tout comme celle, pour les autorités de poursuite des États de l'UE, de faire usage de leurs règles de procédure pénale interne pour accéder aux données physiquement localisées sur leurs territoires respectifs. Selon notre compréhension, le système *e-Evidence* permet à l'autorité de poursuite pénale d'un État de l'UE de choisir entre une perquisition et une EPO si le *data center* se trouve sur son territoire, mais que le fournisseur est rattaché à un autre État de l'UE.

2. Fournisseur de services concerné

a) Notion de fournisseur de services

Tel qu'exposé ci-dessus, le critère permettant l'application du système *e-Evidence* ne réside pas dans la localisation des données dans un État membre de l'UE, respectivement en Suisse pour la surveillance de la correspondance par télécommunications. Il est lié au fait qu'un fournisseur propose des services électroniques dans l'Union, respectivement est soumis au droit suisse.

Au sens du Règlement *e-Evidence* (art. 3 par. 3 Règlement *e-Evidence*), est considéré comme un fournisseur de services toute personne physique ou morale qui fournit des services de communications électroniques[9]. Il s'agit des **services d'attribution de noms de domaine** sur l'internet et de numérotation *IP* et d'autres services de la société de l'information[10] qui permettent à leurs utilisateurs de **communiquer** entre eux, de **stocker** ou de **traiter** d'une autre manière des données pour le compte des utilisateurs auxquels le service est fourni, à condition que le stockage des données soit une composante déterminante du service fourni à l'utilisateur. Sont expressément exclus les services financiers tels que ceux ayant trait à la banque, au crédit, à l'assurance et à la réassurance, aux retraites professionnelles ou individuelles, aux titres, aux fonds d'investissements, aux paiements et aux conseils en investissement (art. 3 par. 3 Règlement *e-Evidence* renvoyant à

l'art. 2 par. 2 let. b Directive 2006/123/CE du 12 décembre 2006 relative aux services dans le marché intérieur).

Il n'est pas pertinent de savoir si le fournisseur est **établi ou non dans l'UE**, étant précisé que par établissement on entend une entité qui exerce de manière effective une activité économique pendant une durée indéterminée au moyen d'une infrastructure stable à partir de laquelle l'activité de fourniture de services est réalisée ou gérée (art. 2 par. 4 et art. 3 par. 5 Directive *e-Evidence*). Concrètement, si un fournisseur est établi dans un État de l'UE qui participe au système *e-Evidence*, cet État devra veiller à ce que ce fournisseur désigne le (ou les) établissement(s) qui sera (seront) le point de contact pour les autorités pénales (art. 3 par. 1 let. a Directive *e-Evidence*) ; si tel n'est pas le cas, c'est aux États membres sur les territoires desquels le fournisseur propose ses services qu'il incombe d'y veiller (art. 3 par.1 let. b Directive *e-Evidence*).

Selon le droit suisse, sont concernés les fournisseurs de services de télécommunication, notion qui a une portée large.[11] Est déterminante la transmission d'informations pour le compte de tiers au moyen de techniques de télécommunication.[12] Sont visés en particulier les fournisseurs d'accès à Internet, soit tout fournisseur de services de télécommunication qui offre une prestation publique de transmission d'informations sur la base de la technologie *IP* et d'adresses *IP*, mais aussi les fournisseurs de services de télécommunication et les services de communication dérivés. Selon le Conseil fédéral suisse, cela comprend notamment les fournisseurs de services Internet qui permettent une communication unilatérale rendant possible le chargement de documents, ceux qui permettent une communication multilatérale rendant possible la communication entre usagers, les fournisseurs d'espaces de stockage d'e-mails, les fournisseurs d'hébergement d'applications ou services email, les fournisseurs d'hébergement y compris de type « *cloud* », les plates-formes de *chat*, les plates-formes d'échange de données et les fournisseurs de services de téléphonie par Internet.[13]

b) Caractéristiques des fournisseurs de service visés

Tout fournisseur de services électroniques n'est toutefois pas concerné. Le critère choisi dans le système *e-Evidence* est le fait de proposer des services dans l'Union, pendant qu'il s'agit, selon le système suisse, du fait d'être soumis au droit suisse, d'une part, et du contrôle des données, d'autre part. Les critères choisis dans les deux systèmes sont ainsi différents. Des précisions s'imposent sur ces notions.

Proposer des services dans l'UE se définit comme 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 ledit État membre. Un tel 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 lorsqu'il existe un ciblage des activités sur un ou plusieurs États membres (art. 3 par. 4 Règlement *e-Evidence*).

Le fait d'être **soumis au droit suisse** est une notion juridique impliquant que l'entité dispose de droits et est astreinte à des devoirs imposés par le droit suisse. Ainsi, une société dont le siège se trouve en Suisse remplit cette condition. Il en est de même de la filiale suisse d'un fournisseur de services étranger. La jurisprudence suisse exige un critère supplémentaire à savoir le fait que l'entité soumise au droit suisse (et non par exemple la maison mère en cas de filiale en Suisse) doit avoir un **contrôle sur les données à produire**, ce par quoi il faut entendre « un pouvoir de disposition, en fait et en droit, sur ces données »[14].

Il sied encore de préciser que sont exclus du système *e-Evidence* les cas dans lesquels une procédure pénale est conduite dans un État membre de l'UE et que le fournisseur déploie ses activités dans ce même État membre. En effet, le système a une vocation extraterritoriale et est ainsi sans préjudice des pouvoirs des autorités nationales de s'adresser aux fournisseurs de services établis ou représentés sur leur territoire afin

qu'ils se conforment à des mesures nationales similaires (art. 1 par. 1 al. 2 Règlement *e-Evidence*). Le droit suisse, applicable au seul État suisse, ne connait par la force des choses pas cette distinction.

3. Seuil de gravité des faits

Un seuil de gravité des faits est prévu dans les deux systèmes. En droit de l'UE, l'EPO est soumise aux principes de nécessité et de proportionnalité (art. 5 par. 2 Règlement *e-Evidence*). Une distinction est faite selon si les données sont relatives aux abonnés ou demandées aux seules fins d'identifier une personne, d'une part, ou si elles sont relatives au trafic ou au contenu, d'autre part. Ainsi, une EPO est possible dans le premier cas pour **toutes les infractions pénales** (art. 5 par. 3 Règlement *e-Evidence*). Dans le second cas, une EPO est possible uniquement pour des infractions punissables dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'**au moins trois ans** (art. 5 par. 4 let. a Règlement *e-Evidence*), pour certaines infractions totalement ou partiellement commises au moyen d'un système d'information (art. 5 par. 4 let. b Règlement *e-Evidence*) et pour certaines infractions terroristes (art. 5 par. 4 let. c Règlement *e-Evidence* renvoyant à la Directive (UE) 2017/541 du 15 mars 2017 relative à la lutte contre le terrorisme).

En droit suisse également, la surveillance de la correspondance par télécommunications est conditionnée par les principes de nécessité (art. 269 al. 1 let. c CPP) et de proportionnalité (art. 269 al. 1 let. a et b CPP) et une distinction est opérée en fonction de la nature des données. S'agissant des données secondaires (c'est-à-dire relatives aux abonnés et au trafic), l'obtention des preuves électroniques est possible pour **tous les crimes et les délits** (art. 263 al. 1 CPP), donc les infractions passibles d'une peine privative de liberté de plus de trois ans (crimes au sens de l'art. 10 al. 2 CP[15]), respectivement d'une peine privative de liberté n'excédant pas trois ans ou d'une peine pécuniaire (délits au sens de l'art. 10 al. 3 *cum* 34 et 40 CP). Le droit suisse se montre ainsi plus limitatif que le droit de l'UE s'agissant des données secondaires, qui ne pourront être obtenues pour des contraventions (passibles uniquement d'une amende, art. 103 *cum* 106 al. 1 CP).

L'obtention des données relatives au contenu est, quant à elle, limitée à un (long) catalogue d'infractions énumérées exhaustivement dans la loi (art. 269 al. 2 CPP), parmi lesquelles ne se trouvent que les **infractions les plus graves**, crimes et délit confondus. À titre d'exemples, parmi les infractions dirigées contre la vie, ne font pas partie du catalogue les délits que sont le meurtre sur la demande de la victime (art. 114 CP), l'infanticide au sens de l'article 116 CP, l'homicide par négligence (art. 117 CP) et l'interruption de grossesse punissable avec le consentement de la mère (art. 118 ch. 1 CP), alors que d'autres formes d'homicide sont listées (meurtre, art. 111 CP ; assassinat, art. 112 CP ; meurtre passionnel, art. 113 CP ; incitation et assistance au suicide, art. 115 CP ; interruption de grossesse punissable sans le consentement de la mère (art. 118 ch. 2 CP). Le droit suisse peut être considéré comme plus restrictif, en ce sens que les données relatives au contenu ne peuvent pas être obtenues pour certaines infractions passibles, selon le droit suisse, d'une peine privative de liberté de plus de trois ans (p. ex. l'interruption de grossesse punissable avec le consentement de la femme enceinte, passible d'une peine privative de liberté de cinq ans au plus, art. 119 al. 1 CP).

4. Modalités de contact avec le fournisseur de services par l'autorité de poursuite pénale

a) Accès (in)direct au fournisseur de services

Le système e-*Evidence* repose sur un **accès direct** au fournisseur de services par l'autorité de poursuite pénale (art. 7 par. 1 Règlement *e-Evidence*).[16]. À cette fin, pour tenir compte de la multiplicité des États concernés, chaque fournisseur de services est tenu d'indiquer un établissement désigné ou annoncer un représentant légal qui sera son point de contact (art. 3 Directive *e-Evidence*). Lorsque plusieurs établisse-

ments ou représentants légaux sont désignés, leurs compétences respectives en particulier la portée territoriale de leurs attributions, doivent être clairement énoncées (art. 4 par. 3 Directive *e-Evidence*). Les autorités pénales des États membres s'adressent ainsi directement au représentant légal ou à l'établissement désigné se trouvant dans un autre État membre au moyen du certificat d'injonction européenne de production (*European Production Order Certificate*, EPOC, art. 9 et Annexe I Règlement *e-Evidence*).[17] Lorsque les données requises sont relatives au trafic ou au contenu, l'EPOC est, en principe, adressé parallèlement à l'autorité chargée de la mise en œuvre (art. 8 par. 1 Règlement *e-Evidence*).[18]

Le droit suisse quant à lui ne permet pas d'accès direct par les autorités pénales suisses aux fournisseurs de services électroniques. Les autorités pénales sont tenues de s'adresser, au moyen d'un formulaire, au Service Surveillance de la correspondance par poste et télécommunication (Service SCPT, art. 3 al. 1 LSCPT) qui 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 renseignement auquel le Service SCPT adressera les demandes (art. 5 al. 1 *cum* 4 al. 1 OME-SCPT[19]).

b) Intervention d'une autorité judiciaire

S'agissant de la question de savoir si l'injonction de production peut être émise par un procureur sans l'intervention d'une autorité judiciaire, le système e-*Evidence* fait une distinction selon si les données sont relatives aux abonnés ou visent à identifier une personne, d'une part, ou si elles sont relatives au trafic ou au contenu, d'autre part. Une validation par une autorité judiciaire de l'État d'émission n'est nécessaire que dans le second cas (art. 4 par. 1 let. a et art. 4 par. 2 let. a Règlement *e-Evidence*, respectivement). Les règles de procédure pénale de l'État d'émission sont alors applicables.

Le droit de la procédure suisse exige quant à lui que toute surveillance de la correspondance par télécommunication, qu'elle porte sur des données relatives aux abonnés, au trafic ou au contenu, soit 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). En ce qui concerne les données secondaires, le droit suisse est ainsi plus strict sous cet angle que le droit européen.

5. Obligation de fournir les données et possibilité de refus

Le système *e-Evidence* prévoit que l'établissement désigné ou le représentant légal du fournisseur concerné (voir *supra* II.2.b) est le point de contact compétent pour la réception, le respect et l'exécution des EPO (art. 3 par. 1 Directive *e-Evidence* ; art. 7 par. 1 Règlement *e-Evidence*). Il est soumis à l'obligation de fournir les données directement à l'autorité de poursuite pénale d'un autre État membre, sous la menace de procédures de mise en œuvre et de sanctions (art. 7 ss Règlement *e-Evidence*). Des motifs de refus d'EPO sont prévus à l'art. 12 Règlement *e-Evidence*, mais ils ne sont applicables que si l'EPO est adressé, parallèlement au point de contact du fournisseur, à l'autorité chargée de la mise en œuvre. C'est cette autorité qui pourra alors se prévaloir du motif de refus. En d'autres termes, une EPO ne peut être refusée que s'agissant des données relatives au trafic et au contenu (art. 8 Règlement *e-Evidence*) et pour des raisons très limitées prévues exhaustivement à l'art. 12 du Règlement, que sont les cas d'immunités et privilèges, la protection de la liberté de la presse, la violation manifeste d'un droit fondamental, le principe *ne bis in idem* et l'absence de double

incrimination. Une procédure de prise de contact entre les autorités nationales est alors prévue (art. 12 par. 2 Règlement *e-Evidence*).

En droit suisse, 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). À la différence du système *e-Evidence*, aucun motif de refus n'est prévu.

II. L'accès aux preuves électroniques au-delà des frontières de l'UE et perspectives pour la Suisse

Le système *e-Evidence* et l'accès direct au fournisseur de services électroniques qu'il met en place remplace les mécanismes antérieurs prévalant entre les États membres de l'UE participants. Il s'agit d'un système interne à l'UE : il ne permet pas aux autorités pénales d'un État tiers à l'UE, comme la Suisse, de s'adresser directement à l'établissement désigné ou au représentant légal. Il ne permet pas non plus à un État non-membre d'adresser une demande d'entraide à un État membre qui fera usage de l'EPO pour l'exécuter (par. 23 des considérants et art. 2 par. 4 Règlement *e-Evidence*). Ainsi, le système e-Evidence ne remplace pas les règles applicables à la coopération internationale en matière pénale avec les États non-membres de l'Union[20].

Se pose ainsi la question des règles applicables lorsque les autorités d'un État membre de l'UE veulent obtenir des données auxquelles la Suisse a accès, ou *vice versa*. Hormis les instruments classiques de coopération, telle la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 (CEEJ) complétée par ses Protocoles additionnels (dont seul le second est applicable pour la Suisse), la Convention sur la cybercriminalité conclue à Budapest le 23 novembre 2001 (CCC)[21] contient des règles sur l'accès transfrontalier aux preuves électroniques. Le Deuxième Protocole, relatif au renforcement de la coopération et de la divulgation de preuves électroniques, conclu à Strasbourg le 12 mai 2022 (STE 224), permettant un accès direct au fournisseur de services, n'a pas été ratifié par la Suisse. La CCC ne va pas au-delà de ce qui était déjà possible en application du droit suisse pertinent, à savoir la Loi fédérale régissant l'entraide internationale en matière pénale (EIMP)[22], à tout le moins s'agissant de la surveillance rétroactive. Ainsi, lorsque la Suisse reçoit une demande d'entraide portant sur une forme de surveillance de la correspondance par télécommunication, elle appliquera les règles exposées dans la présente contribution (notamment et pour partie par renvoi de l'art. 18*a* EIMP).[23] Par application du principe de la réciprocité, les autorités suisses ne peuvent adresser à un État étranger de demande portant sur des mesures qu'elles ne pourraient pas entreprendre si les rôles étaient inversés (art. 30 al. 1 EIMP). La coopération est soumise aux motifs de refus ordinaires applicables en matière de coopération internationale (notamment principes *ne bis in idem*, double incrimination et proportionnalité), mais elle est surtout chronophage et tributaire de formalités qui ne s'accommodent que très peu des caractéristiques des preuves électroniques.[24]

Afin de pallier ces inconvénients qui peuvent s'avérer rédhibitoires pour la procédure pénale, une possibilité résiderait dans l'association de la Suisse au système européen *e-Evidence*. Ainsi, les autorités de poursuite des États membres de l'UE pourraient avoir accès aux données contrôlées par des fournisseurs suisses (qui ne proposent pas de services dans l'UE) et *vice versa*. Si une volonté politique naît en ce sens, resteront à déterminer les modalités d'une telle avancée, en particulier comment concilier les différences exposées dans la présente contribution, notamment s'agissant de l'accès direct aux représentants des fournisseurs de services possible dans le système *e-Evidence* mais exclue en droit suisse ou les divergences s'agissant des seuils de gravité prévalant dans les deux systèmes.

III. Conclusion

Le système *e-Evidence* renverse la logique classique de la coopération internationale en matière pénale entre les États membres. Il fait fi de la localisation physique des données, permet aux autorités de poursuite un accès direct au fournisseur de services sans impliquer ni l'État où les données sont stockées, ni celui où le fournisseur de services est établi, ni la personne concernée par la transmission des preuves en question. En ce sens, il exclut en partie le contrôle sur la transmission et déroge ainsi fondamentalement à la logique souverainiste du droit de la coopération. Il crée un espace européen de procédure pénale en matière d'accès transnational aux preuves électroniques.

La Suisse, bien que disposant des bases légales lui permettant d'accéder aux preuves électroniques situées à l'étranger, a opté pour des critères de rattachement qui restreignent cet accès, en tant qu'ils ne correspondent pas aux réalités concrètes. Les autorités pénales suisses sont ainsi systématiquement amenées à procéder par le biais de la coopération judiciaire internationale classique pour obtenir des données électroniques, voie qui n'est pas adaptée à ce type de données et, plus généralement à la cybercriminalité. Une réflexion doit, à notre avis, être initiée à ce propos.

Cela étant, tant au sein de l'UE qu'en Suisse demeure la question de l'exploitabilité et donc l'admissibilité dans le cadre d'une procédure pénale des moyens de preuve obtenus sur le plan transnational.[25] Éphémères et manipulables par nature, ces données impliquent des précautions particulières pour assurer leur fiabilité. C'est sans doute là un des terrains sur lesquels les juristes, suisses et européens, devront, ensemble on l'espère, réfléchir dans un avenir proche.

---

1. [2023] *JO* L 191/118.↩
2. [2023] *JO* L 191/181.↩
3. L'Irlande a exercé son droit de *opt-in* (considérant 100 du Règlement *e-Evidence*) et le Danemark celui d'opt out (considérant 101du Règlement *e-Evidence*).↩
4. Pour une comparaison de droits d'autres États, voir U. Sieber /N. von zur Mühlen /T, Tropina (édit.), *Access to Telecommunication Data in Criminal Justice. A Comparative Legal Analysis*, 2e ed., Berlin 2022.↩
5. Code de procédure pénale suisse du 5 octobre 2007 ; Recueil systématique du droit fédéral suisse 312.0.↩
6. Loi fédérale sur la surveillance par poste et télécommunications du 18 mars 2016 ; Recueil systématique du droit fédéral suisse 780.1.↩
7. Voir l'intitulé de l'art. 273 CPP.↩
8. ATF 143 IV 21, considérant 3.3 ; voir aussi TF, 1B_142/2016, 16 novembre 2016, considérant 3.3.↩
9. Renvoi est fait ici à l'art. 2 par. 4 de la Directive (UE) 2018/1972 du 11 décembre 2018 établissant le code des communications électroniques européen.↩
10. Renvoi est fait ici à l'art. 1 par. 1 let. b, de la Directive (UE) 2015/1535 du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des règlementations techniques et des règles relatives aux services de la société de l'information (texte codifié).↩
11. S. Métille , « Introduction aux art. 269-281 CPP N 26 » in Y. Jeanneret /A. Kuhn /C. Perrier Depeursinge (ed.), *Commentaire romand CPP*, 2e ed.., pp. 1733 ff., p. 1738, Bâle 2019.↩
12. Renvoi est fait à l'art. 3 de la Loi fédérale sur les télécommunications du 30 avril 1997 (LTC ; Recueil systématique du droit fédéral 784.10).↩
13. Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), Feuille fédérale 2013 2379, p. 2404. Critique à propos de cette définition très large, S. Métille, *op. cit.* (n. 11), pp. 1739.↩
14. ATF 143 IV 21, considérant 3.4 ; TF, 1B_142/2016, 16 novembre 2016, considérant 3.6. Pour une discussion relative au critère de la localisation des données vs le pouvoir de contrôle sur les données, voir J. 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.↩
15. Code pénal suisse ; Recueil systématique du droit fédéral suisse 311.0.↩
16. Sur les liens avec la Décision d'enquête européenne, voir considérant 8 Règlement *e-Evidence*. À propos de l'(in)adéquation de la Décision d'enquête européenne concernant les preuves électroniques, voir S. Arasi, « The EIO Proposal and the Rules on Interception of Telecommunications » in S. Ruggeri (ed.), *Transnational Evidence and Multicultural Inquiries in Europe. Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Cham 2014, pp. 127 ff. ; C. Brière , « EU Criminal Procedural Law onto the Global Stage : The e-Evidence Proposals and Their Interaction with International Developments », *European Papers* 2021, pp. 493 ff., p. 499.↩
17. À propos de l'opportunité de procéder par le biais d'un formulaire standardisé, voir E. Casey et al., « The Evolution of Expressing and Exchanging Cyber-Investigation Information in a Standardized Form » in M. A. Biasiotto et al. (ed.), *Handling and Exchanging Electronic Evidence Across Europe*, Cham 2018, pp. 43 ss.↩
18. Voir toutefois les exceptions prévues à l'art. 8 par. 2 Règlement *e-Evidence*.↩

19. Ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication du 15 novembre 2017, Recueil systématique du droit fédéral suisse 780.117.↩
20. Pour une analyse détaillée du droit de la coopération internationale en matière de surveillance des télécommunications, voir U. Sieber/N. von zur Mühlen/T. Wahl, *Rechtshilfe zur Telekommunikationsüberwachung*, Berlin 2021 ; S. Tosza, « Cross-Border Gathering of Electronic Evidence : Mutual Legal Assistance, its Shortcomings and Remedies » in V. Franssen/D. Flore (ed.), *Société numérique et droit pénal. Belgique, France, Europe*, Bruxelles 2019, pp. 270 ff.↩
21. STE 185. Pour un manuel des bonnes pratiques en la matière, voir P. Verdelho, *The effectiveness of international co-operation against cybercrime : examples of good practices,* Report, Council of Europe, Economic Crime Division, Project on Cybercrime, 12 mars 2008. Voir aussi Comité de la Convention Cybercriminalité, du Conseil de l'Europe, Rapport d'évaluation : Les dispositions de la Convention de Budapest sur la criminalité concernant l'entraide, 2-3 décembre 2014, T-CY(2013)17rev.↩
22. Recueil systématique du droit fédéral suisse 351.1.↩
23. Voir L. Moreillon/S. Blank, « La surveillance policière et judiciaire des communications par Internet », *Medialex* 2004, pp. 81 ff. pp. 87. En revanche, l'entrée en vigueur pour la Suisse de la CCC a permis la transmission en temps réel de données informatiques relatives au trafic (art. 33 CCC ; la règle a été transposée en droit suisse à l'art. 18*b* EIMP). Les conditions sont toutefois restrictives et l'utilisation permise limitée.↩
24. À propos en particulier de l'inadéquation s'agissant des données stockées sur des *cloud*, voir L. Siry, « Cloudy days ahead : Cross-border evidence collection and its impact on the rights of EU citizens », *New Journal of European Criminal Law* 2019, pp. 227 ff., pp. 229 ff.↩
25. Pour une analyse détaillée des défis véhiculés par la portée internationale des moyens de preuve, voir J. D. Jackson/S. J. Summers, *The Internationalisation of Criminal Evidence. Beyond the Common Law and Civil Law Traditions*, Cambridge 2012. Pour une proposition d'acte relatif à l'admissibilité des preuves, voir European Law Institute, Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings. Draft Legislative Proposal of the European Law Institute, 8 mai 2023 (à propos de cette proposition, voir L. Bachmaier, « Mutual Admissibility of Evidence and Electronic Evidence in the EU - A New Try for European Minimum Rules in Criminal Proceedings? », dans ce numéro).↩

COPYRIGHT/DISCLAIMER
© 2023 The Author(s). Published by the Max Planck Institute for the Study of Crime, Security and Law. This is an open access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see https://creativecommons.org/licenses/by-nd/4.0/.
Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union