La collecte transfrontière de preuves numériques en matière pénale. Enjeux et perspectives européennes *

By Vanessa Franssen / Alyson Berrendorf* / Marine CORHAY**

La collecte de preuves numériques constitue, de nos jours, un enjeu majeur dans un nombre croissant de dossiers répressifs. Toutefois, force est de constater que les autorités policières et judiciaires sont confrontées à de multiples obstacles et incertitudes, surtout lorsque cette collecte est de nature transfrontière. Ces difficultés s'expliquent, d'un côté, par l'existence d'un cadre juridique en pleine évolution (la plupart du temps sous l'impulsion de l'Europe) mais souventencore fragmentaire et mal adapté, et de l'autre, par le fait que la problématique des preuves numériques reste encore trop peu connue par la grande majorité des autorités compétentes.

L'objectif de cette contribution est dès lors d'exposer les enjeux et défis que présentent les preuves numériques dans le cadre des enquêtes pénales aujourd'hui (Section 1), de circonscrire la problématique de la collecte transfrontière de telles preuves (Section 2), de décrire le cadre juridique européen existant et ses défauts (Section 3) et enfin, de donner un bref aperçu des enjeux futurs (Section 4). Ainsi, nous espérons contribuer à une meilleure compréhension de la problématique et à une plus grande prise de conscience par les autorités policières et judiciaires, d'un côté, et par le législateur européen, de l'autre.

Section 1 : Introduction – enjeux et défis relatifs aux preuves numériques

1. Enjeux

Les enjeux des preuves numériques sont importants, au niveau tant opérationnel que législatif. Il n'existe actuellement presque plus d'enquêtes pénales dans lesquelles il n'est pas fait recours, d'une manière ou d'une autre, à des preuves numériques. En effet, ce serait erroné de penser que ce type de preuves est limité à la seule cybercriminalité[1]. Telle est la conséquence de la dématérialisation des moyens de preuve. Celle-ci s'explique par la **numérisation de la société** qui ne cesse de s'amplifier. Au fil des deux dernières décennies, la société a en effet connu une modification profonde de son fonctionnement, tant au niveau de l'organisation globale de celle-ci que dans les rapports qu'elle a refaçonnés entre les individus. Dans le même temps, on observe l'emploi répandu des nouvelles *technologies de l'information et de la communication* (ci-après : T.I.C.)[2], à des fins légitimes, mais aussi à des fins criminelles.

Des exemples de preuves numériques dans le contexte pénal sont nombreux et très divers. Il peut s'agir, d'un côté, d'autorités policières et judiciaires qui recourent, elles-mêmes, à de nouvelles technologies, comme l'usage de radars (pour verbaliser), de caméras lecture de plaque d'immatriculation (pour identifier et/ou suivre l'itinéraire d'un suspect) ou d'un système de géolocalisation (qui permet de suivre un suspect en temps réel), la mise en place d'une observation à l'aide de moyens techniques qui peut être précédée par un contrôle visuel discret, notamment pour placer le dispositif technique ou pour activer le système de vidéosurveillance existant dans un lieu privé, ou encore l'exécution d'une infiltration sur internet (par exemple, l'infiltration

---

* Cette contribution a été écrite dans le prolongement d'une communication orale donnée par Vanessa FRANSSEN le 19 septembre 2018 lors d'une journée de formation à la Cour de cassation française, organisée par l'Association française de droit pénal, l'Association internationale de droit pénal (ci-après : AIDP), l'École nationale de la magistrature et la Cour de cassation. La rédaction de ce texte a été clôturée le 23 mai 2019. Elle a fait l'objet d'une publication antérieure dans la Revue *Justice actualités*, éd. Intranet École nationale de la magistrature (ENM), n° 21 (consacré au traitement de la preuve numérique par les magistrats dans les procédures judiciaires civiles et pénales), juin 2019, pp. 32-47. Cette version a été mise à jour à la lumière de développements récents au niveau européen.

* Chargée de cours à l'Unité de Recherche Cité de l'Université de Liège, Chercheuse Affiliée à la KU Leuven et Avocate au Barreau de Bruxelles.

* Doctorante à l'Unité de Recherche Cité de l'Université de Liège.

* Assistante à l'Unité de Recherche Cité de l'Université de Liège.

[1] Tel fut déjà mis en évidence en 2001, lors de l'adoption de la convention sur la cybercriminalité par le Conseil de l'Europe (STE n° 185, Budapest, 23 novembre 2001 ; ci-après : convention sur la cybercriminalité). L'article 14, paragraphe 2 prévoit en effet que les mesures d'enquête réglées par la convention ne s'appliquent pas uniquement aux cyber-infractions définies par la convention, mais aussi « *b) à toutes les autres infractions pénales commises au moyen d'un système informatique; et c) à la collecte des preuves électroniques de toute infraction pénale.* » (Nous soulignons.)

[2] X., « Technologies de l'information et de la communication (T.I.C.) », in *Universalis Junior*, *Encyclopaedia Universalis*, disponible sur https://junior.universalis.fr/encyclopedie/technologies-de-l-information-et-de-la-communication-t-i-c/ (consulté le 1er mars 2019).

par un policier sous couvert d'une identité fictive dans des forums ou *chatrooms* privés afin de collecter des éléments de preuve).

De l'autre côté, ce sont les citoyens qui utilisent de plus en plus les nouvelles T.I.C., laissant ainsi d'innombrables traces numériques, chaque jour, derrière eux. Si celles-ci sont parfois volontaires – comme c'est le cas pour l'envoi d'emails, la publication de tweets, ou le post de commentaires sur les réseaux sociaux – souvent, ces traces s'esquissent à notre insu, de manière involontaire et invisible. Ces traces constituent incontestablement une mine d'informations pour les autorités policières et judiciaires ; ces données peuvent en effet s'avérer utiles, voire dans certains cas indispensables, tant à charge qu'à décharge du suspect dans le cadre d'une enquête pénale. Se pose alors la question de savoir qui possède l'accès à ces données, qui en a le contrôle, et qui peut les transmettre, voire les stocker, le cas échéant. Dans la mesure où elles sont traitées ou stockées par des entreprises privées (que ce soient de traditionnels opérateurs de télécommunications, des fournisseurs de services internet ou d'autres), cela soulève des questions délicates sur leur collaboration avec les autorités policières et judiciaires, ainsi que sur la possibilité de trouver un juste équilibre entre l'efficacité de la procédure pénale, d'une part, et le respect des droits fondamentaux des personnes concernées par la collecte et l'utilisation de données, d'autre part.

Dans ce même contexte, il convient de s'interroger sur la manière dont on peut **adapter** notre **procédure pénale** pour faire face à cette numérisation et aux nouveaux modes de communication. À cet égard, deux approches majeures semblent se profiler[3]. D'un côté, il y a des systèmes juridiques qui s'en tiennent à des *règles générales* s'appliquant tant à la preuve physique (c'est-à-dire tangible) qu'à la preuve numérique. Cette approche est basée soit sur un manque d'intervention soit sur l'idée que, dans la mesure du possible, la conduite en ligne devrait être réglementée de la même manière que toute autre conduite et que les lois existantes devraient également s'y référer[4]. Cette approche risque cependant de négliger les défis propres aux preuves numériques comme, par exemple, leur volatilité et l'intégrité des données informatiques qui sont collectées. De l'autre côté, certains législateurs préfèrent adopter des *règles spécifiques* pour la preuve numérique. Si cette démarche permet une approche plus adaptée à la réalité numérique, le grand enjeu est toutefois de créer des règles ayant un caractère technologiquement neutre qui résistent à l'épreuve du temps et aux futurs développements technologiques, sans créer de l'incertitude juridique.

2. Défis

- Un premier défi en matière de preuve numérique découle de la **nature volatile des données informatiques**[5]. Cette volatilité pose surtout problème pour les données qui ne sont, en principe, pas stockées ou conservées, telles les données de trafic et de localisation. Plus particulièrement, les données à caractère personnel transmises dans le cadre de communications électroniques ne sont stockées qu'à des fins commerciales (telle la facturation) ou techniques ou à condition que l'utilisateur y donne son consentement[6]. Dès que ces données relatives au trafic ne sont plus nécessaires à la transmission d'une communication ou à une fin commerciale, elles doivent être effacées ou rendues anonymes[7]. Une exception à ce principe est l'obligation générale de

[3] Notons, toutefois, que ces deux approches peuvent aussi être combinées au sein d'un même système juridique. Telle semble notamment l'approche choisie par le législateur français qui, d'une part, a adapté certaines mesures d'enquête existantes conçues pour la collecte de preuves physiques et, d'autre part, a créé de nouvelles mesures d'enquête spécifiques. Pour une excellente analyse, voy. Jean-Marie BRIGANT, « Mesures d'investigation face au défi numérique en droit français », *in* Vanessa FRANSSEN et Daniel FLORE (dir.), *Société numérique et droit pénal. Belgique, France, Europe*, Bruxelles, Larcier/Bruylant, 2019, pp. 217-244.

[4] Jonathan CLOUGH, *Principles of Cybercrime*, 2ème éd., Cambridge, Cambridge University Press, 2015, pp. 17-18.

[5] Sur ce point voy., entre autres, Résolution 18 de la Section III, adoptée au XIXème Congrès international de droit pénal de l'AIDP à Rio de Janeiro (2014) : « *En raison de la nature volatile des preuves électroniques les règles juridiques devraient faciliter la préservation expéditive et le stockage des données informatiques. Les outils d'analyse pour prévenir des modifications sur les données stockées devraient être disponibles et régulièrement appliqués.* »

[6] Article 5, paragraphes 1er et 2 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.U.E.*, L 201, 31 juillet 2002, p. 37. Cette directive sera, à terme, remplacée par le Règlement « *e-Privacy* » qui est actuellement négocié par les institutions européennes : Commission européenne, Proposition de Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM(2017) 10 final, 10 janvier 2017.

[7] Article 6, paragraphe 1er de la directive 2002/58/CE.

conservation de données de communications, qui était prévue par la directive 2006/24/CE[8]. Cette directive a toutefois été annulée par la Cour de justice de l'Union européenne (ci-après : CJUE) en 2014[9] et la légalité des législations nationales basées sur cette directive est fortement remise en cause par la même Cour[10]. Cette jurisprudence a mis à mal les autorités policières et judiciaires, qui soulignent l'importance de telles données dans le cadre des enquêtes pénales. Se pose donc la question de savoir sous quelles conditions de telles données peuvent encore être conservées et rendues disponibles aux fins de poursuites pénales[11].

- Un second défi réside dans la **possibilité d'anonymiser la communication et le chiffrement de plus en plus courant des données** qui les rend inaccessibles et/ou incompréhensibles à toute personne qui ne dispose pas de la clé de chiffrement. D'un côté, l'usage d'un VPN ou d'autres techniques d'anonymisation permet de rendre l'identification des utilisateurs de nouvelles T.I.C. et de services en ligne par les autorités plus difficile, voire impossible[12]. De l'autre, nous remarquons que la plupart des outils de communication contemporains – comme c'est le cas pour *Whatsapp*[13], *Telegram*[14] ou *Skype*[15] – sont aujourd'hui, par défaut, chiffrés. Ce chiffrement garantit la confidentialité et l'intégrité des données[16]. Toutefois, – revers de la médaille – cette protection peut s'avérer un atout pour les criminels ou délinquants souhaitant communiquer à l'abri de toute interférence des autorités policières et judiciaires et créer un obstacle insurmontable pour ces autorités.
- En troisième lieu, la collecte de preuves numériques se heurte à la **difficulté de la localisation des données**. Sur ce point, plusieurs questions entrent en ligne de compte : où les données sont-elles stockées ? Qui peut y avoir accès ? Quel droit s'y applique ? Ce problème porte en lui le germe d'un enjeu de plus en plus stratégique, tant pour les autorités policières et judiciaires que pour les criminels, mais aussi au niveau politique et diplomatique[17].
- Dans un quatrième temps, il convient d'assurer et **ne pas compromettre l'intégrité de la preuve numérique**, que ce soit tant avant qu'après sa collecte. Tout d'abord, de manière *ex ante*, il faut s'assurer que lorsque les autorités procéderont à la saisie des données, ces dernières n'auront pas été préalablement manipulées. Par après, il convient également de garantir à la défense l'authenticité des données récoltées. Il est essentiel pour

---

[8] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, L 105, 13 avril 2006, p. 54.

[9] CJUE (Grande Chambre), *Digital Rights Ireland Ltd*, 8 avril 2014, affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238.

[10] CJUE (Grande Chambre), *Tele2 Sverige c. Post- och telestyrelsen et Secretary of State for the Home Departement c. T. Watson e.a.*, 21 décembre 2016, C-203/15 et C-698/15, ECLI:EU:C:2016:970.

[11] Pour une analyse critique de la jurisprudence européenne, voy. Frank VERBRUGGEN, Sofie ROYER et Helena SEVERIJNS, « Reconsidering the Blanket-Data-Retention-Taboo, for Human Rights' Sake ? », *European Law Blog*, 1er octobre 2018, disponible sur http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/. Pour une analyse des répercussions de cette jurisprudence sur la législation belge, voy. Frank VERBRUGGEN et Fanny COUDERT, « Conservation des données de communications électroniques en Belgique : un juste équilibre ? », *in* Vanessa FRANSSEN et Daniel FLORE (dir.), *Société numérique et droit pénal. Belgique, France, Europe,* Bruxelles, Larcier/Bruylant, 2019, pp. 245-266.

[12] Ces outils d'anonymisation sont facilement accessibles, peu compliqués à mettre en œuvre et souvent gratuits. Voy., par exemple, une explication pour utiliser Skype de façon anonyme : Kenrick CALLWOOD, « How to Use Skype Anonymously », *Techwalla*, disponible sur https://www.techwalla.com/articles/how-to-use-skype-anonymously (consulté le 16 mai 2019). Pour un service de *proxy server* gratuit, voy. www.proxy4free.com.

[13] Voy. le fonctionnement du chiffrement de bout en bout de *Whatsapp*, disponible sur https://faq.whatsapp.com/en/android/28030015/?lang=fr.

[14] Pour un aperçu des caractéristiques de *Telegram* et de ses avantages pour les utilisateurs, voy. la présentation commerciale du service, disponible sur https://telegram.org/.

[15] Concernant le chiffrement des communications par *Skype*, voy. https://support.skype.com/en/faq/FA31/does-skype-use-encryption.

[16] À noter que les fournisseurs d'un service de communications électroniques sont tenus de garantir la sécurité de leurs services et que, de manière plus générale, toute personne responsable du traitement de données à caractère personnel est obligée de garantir une sécurité appropriée de ces données, y compris par le biais du chiffrement. Voy. article 4, paragraphe 1er de la directive 2002/58/CE et article 5, paragraphe 1er, (f) and article 32 du Règlement 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 (règlement général sur la protection des données), *J.O.U.E.*, L 199, 4 mai 2016, p. 1.

[17] Renvoyons, par exemple, aux efforts récents de la Russie de territorialiser l'internet : Tom BALMFORTH, « Russian lawmakers approve second reading of 'sovereign' Internet bill », *Reuters*, 11 avril 2019, disponible sur https://www.reuters.com/article/us-russia-internet-bill/russian-lawmakers-approve-second-reading-of-sovereign-internet-bill-idUSKCN1RN0UX (consulté le 22 mai 2019).

la défense de pouvoir vérifier la manipulation intègre des données qui se trouvent dans le dossier répressif ; à cet effet, l'intervention d'un expert informatique peut s'avérer nécessaire.
- Cinquièmement, afin de pouvoir faire face à tous ces défis, une **formation constante** des autorités policières et judiciaires qui devront appréhender ce nouveau terrain d'investigation paraît indispensable. Ces acteurs sont habitués à faire face à des situations où il est question de preuves physiques – comme c'est le cas, pour la collecte de stupéfiants ou d'armes – mais sont frileux lorsqu'il s'agit d'appréhender ce nouveau type de preuves, relevant du numérique.
- Sixièmement, afin de répondre aux différents défis ainsi posés, une **collaboration entre les autorités policières et judiciaires et le secteur privé** est un incontournable. Dans cette perspective, trois questions se doivent d'être prises en considération : (i) quelles personnes ont accès à ces données informatiques, (ii) quelles sont les conditions d'accès à celles-ci, et (iii) comment mettre en balance la protection de la vie privée – dont l'interférence grave nécessite un contrôle par un organe juridictionnel (ou indépendant) – et l'efficacité de l'enquête pénale.
- Cela nous amène au septième défi qui concerne, de manière plus générale, la question de la **sauvegarde des droits fondamentaux**. À cet effet, il conviendra de déterminer quelle sera l'autorité garante de cette tâche et quelles seront les personnes concernées. Est-ce que le secteur privé a également un rôle à jouer dans ce contexte ? Cette question fait actuellement l'objet d'un grand débat au sein de l'Union européenne (ci-après : UE), notamment dans le cadre des négociations portant sur la proposition *e-evidence* de la Commission européenne (*infra*)[18]. Enfin, il conviendra de déterminer comment articuler effectivement la mise en œuvre de ces différents droits et leurs protections.
- Enfin, un dernier défi majeur concerne l'existence de **différentes approches régionale, supranationale et internationale en matière de collecte** de preuves numériques. Tandis que l'internet est sans frontières et accessible pour tous de n'importe où, le paysage législatif et réglementaire est fort fragmenté, ce qui engendre des conflits de lois et de l'insécurité juridique pour tous les acteurs (autorités, citoyens, entreprises privées). À notre sens, une approche supranationale globale est indispensable afin d'apporter plus d'homogénéité dans la collecte de ce nouveau moyen de preuves. L'analyse de l'actuel cadre juridique à l'échelle européenne ci-dessous montrera cependant que l'on est encore loin du compte.

Section 2 : La collecte transfrontière - tentative de définition

Avant d'ouvrir la boîte à outils européenne, il convient de procéder, d'abord, à une définition de la notion de « collecte transfrontière » : qu'est-ce qu'on entend par là ? Cette tentative de circonscription est fondamentale parce que selon l'étendue que l'on donne au territoire dans le cyberespace, la problématique de la collecte transfrontière est plus ou moins aiguë.

1. Le principe de territorialité et le concept de territoire

L'État exerce sur son territoire la plénitude de ses compétences, que celles-ci soient législatives, exécutives, ou juridictionnelles. Ces prérogatives forment la compétence territoriale – à savoir l'une des manifestations majeures de la souveraineté nationale des États. En principe, la compétence territoriale en matière pénale est une compétence de fond et implique « *que les lois pénales s'appliquent sur l'ensemble du territoire à toute personne s'y trouvant et que le juge peut les appliquer pour toute infraction commise sur le territoire* »[19].
Ainsi, la compétence territoriale des autorités policières et judiciaires signifie que toute infraction commise sur le territoire d'un État peut faire l'objet d'une poursuite pénale par les autorités judiciaires dudit État. Leur sphère d'action est, en principe, limitée au territoire national, qu'il s'agisse des poursuites pénales ou de l'exercice de mesures d'enquête. Au-delà des frontières nationales, elles sont censées recourir à l'aide des autorités policières et judiciaires de l'État étranger en question.
Vu l'importance du principe de la territorialité, la définition du concept de territoire est un préalable indispensable. En effet, celle-ci aura une influence déterminante sur la compétence territoriale des autorités répressives nationales dans le cyberespace. Si la définition traditionnelle du territoire pose relativement peu

[18] Cette proposition consiste, en réalité, en deux textes intrinsèquement liés : d'un côté, une proposition de règlement et, de l'autre, une proposition de directive. Commission européenne, Proposition de règlement du parlement européen et du conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, 2018/0108(COD), Strasbourg, 17 avril 2018 (ci-après : la proposition de règlement *e-evidence*) ; Commission européenne, Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de collecte de preuves en matière pénale, 2018/0107 (COD), Strasbourg, 17 avril 2018 (ci-après : la proposition de directive *e-evidence*).
[19] Éric DAVID, *Éléments de droit pénal international et européen*, 2ème éd., Bruxelles, Bruylant, 2018, p. 35.

de problèmes – le territoire d'un État est la portion du globe sur laquelle celui-ci exerce sa souveraineté, il comprend nécessairement un élément terrestre et un élément aérien et, en fonction de la situation géographique de l'État concerné, également un élément maritime[20] –, les critères qui permettent de rattacher une affaire au territoire d'un État font moins l'objet d'unanimité à l'échelle supranationale et internationale, comme un bref tour d'horizon des instruments juridiques existants le révèlera (*infra*). En effet, différents critères de rattachement entre le territoire national et le cybermonde peuvent être envisagés, tel l'endroit de stockage des données ou celui où se trouvent des éléments d'infrastructure – comme des câbles, des antennes, des serveurs ou des centres de données. Un autre critère bien connu est l'endroit où réside/se trouve le suspect ou la cible. Le siège social du fournisseur de services pourrait également être sollicité, surtout s'il se fait ressentir un besoin de collaboration dans l'enquête pénale. Enfin, plus récemment, on constate que l'endroit où le service est offert commence à jouer un rôle de plus en plus important.

2. Les critères de rattachement prévus dans des conventions et d'autres instruments législatifs : quelques illustrations

Les critères potentiels susdits se trouvent tous dans les conventions et autres textes législatifs déjà adoptés en matière de preuves numériques au niveau européen[21]. Toutefois, alors qu'une approche uniforme serait souhaitable, force est de constater, dans un premier temps, que **les critères de rattachement varient** selon les instruments juridiques et les mesures d'enquête envisagés.

À titre d'illustration, l'article 18 de la convention sur la cybercriminalité relatif à l'injonction de production de données informatiques, utilise comme critère de rattachement territorial *l'endroit où les services sont offerts*, du moins pour ce qui concerne la production de données relatives aux abonnés (art. 18, paragraphe 1er, b)). Ainsi, cet État est compétent pour demander à un fournisseur de services offrant des services sur son territoire – même si le siège social du fournisseur de services se trouve à l'étranger – de lui transmettre les données d'identification de l'abonné qu'il a en sa possession ou sous son contrôle. Par contre, lorsqu'il s'agit d'autres données informatiques stockées (qu'il s'agisse du contenu de la communication ou de données relatives au trafic concernant des communications passées dans la mesure où ces données sont conservées), la personne appelée à collaborer avec les autorités compétentes doit être *juridiquement ou physiquement présente* sur le territoire de l'État de ces autorités (art. 18, paragraphe 1er, a))[22]. Sinon, celles-ci doivent recourir à l'entraide judiciaire et donc solliciter l'intervention de leurs collègues étrangers sur le territoire duquel se trouve le siège social ou, le cas échéant, une succursale de cette personne.

Le critère de l'endroit où les services sont offerts est également utilisé par la Commission européenne dans sa proposition de règlement *e-evidence*. Cette proposition prévoit notamment la création d'une injonction européenne de production et de conservation de preuves numériques émise par l'État membre où les services sont offerts, à l'égard d'un fournisseur de services ayant désigné un représentant légal dans un autre État membre. Cette injonction pourrait concerner toutes les données informatiques stockées (voy. aussi *infra*)[23].

À titre de comparaison, observons qu'en ce qui concerne l'interception de télécommunications en temps réel, diverses dispositions légales utilisent le *lieu où se trouve le suspect ou la cible* comme facteur de rattachement territorial, afin de déterminer quelles sont les autorités compétentes. Telle est notamment l'approche privilégiée par les articles 18, paragraphe 2, b) et 19, paragraphe 2 de la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'UE (ci-après : convention de l'UE relative à l'entraide judiciaire)[24] et par l'article 31 de la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale (ci-après : directive DEE)[25].

Par ailleurs, on remarque que *l'endroit de l'infrastructure et/ou de la localisation des données*, si celles-ci sont stockées, reste également un critère très fréquent, voire déterminant dans beaucoup de cas. En effet, il s'agit du critère utilisé notamment pour (1) l'interception de télécommunications par l'État où se trouve la station

---

[20] Plus généralement, il s'agit de l'espace géographique sur lequel un État exerce l'intégralité de ses compétences, à l'exclusion de tout autre État. Voy. Jean SALMON (dir.), *Dictionnaire de droit international public*, Bruylant/AUF, 2001, p. 1076.

[21] On retrouve une diversité comparable au niveau national, les États ne privilégiant pas forcément le(s) même(s) critère(s) de rattachement pour une même mesure d'enquête.

[22] Comité de la Convention sur la Cybercriminalité (T-CY), *T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention)*, Strasbourg, 1er mars 2017, p. 6, disponible sur https://rm.coe.int/16806f943e.

[23] Proposition de règlement *e-evidence*, exposé des motifs, pp. 4-5.

[24] Convention établie par le Conseil conformément à l'article 34 du traité sur l'Union européenne, relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne du 29 mai 2000, *J.O.U.E.*, C 197, 12 juillet 2000.

[25] Directive 2014/41/UE du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, *J.O.U.E.*, L 130, 1er mai 2014, p. 1.

terrestre via laquelle les systèmes de services de télécommunications opèrent[26] ; (2) la conservation rapide de données informatiques stockées au moyen d'un système informatique se trouvant sur le territoire d'un autre État[27] ; et (3) la recherche (ou « perquisition ») dans un système informatique (comme, par exemple, un *smartphone* ou un ordinateur) et la saisie des données qui y sont stockées[28]. Toutefois, il est intéressant d'observer que la proposition *e-evidence* de la Commission européenne écarte justement la localisation des données comme critère de rattachement territorial « *étant donné que le stockage n'implique aucun contrôle de la part de l'État au sein duquel les données sont stockées* »[29]. En effet, « *[l]es conditions de stockage des données sont généralement déterminées par le fournisseur sur la base de considérations commerciales* »[30].

Le deuxième constat est qu'en plus d'une diversité des critères de rattachement, **les instruments juridiques existants prévoient parfois même une combinaison de plusieurs critères** qui sont utilisés simultanément, comme c'est le cas, par exemple, pour l'interception de télécommunications[31].

Troisièmement, on remarque **quelquefois également que le critère de rattachement choisi manque en clarté**. À titre d'illustration, il suffit de nous pencher sur l'entraide dans la collecte en temps réel de données relatives au trafic. Cette collecte est régie par l'article 33 de la convention sur la cybercriminalité, qui mentionne explicitement les « *données relatives au trafic, associées à des communications spécifiées sur leur territoire* ». Or, la problématique se situe sur la localisation de telles communications. S'agit-il de l'endroit où se situent les interlocuteurs ou l'un d'eux ? Alors que telle interprétation paraît plausible, le rapport explicatif prend le parti d'une autre approche : il s'agit plutôt des « *communications transmises par un système informatique se trouvant sur le territoire* »[32]. Compte tenu de cette précision, se pose la question de savoir comment on applique ce critère à des systèmes de communications tels que *Skype* fonctionnant sur la base du principe de *peer-to-peer*, c'est-à-dire où les échanges se font directement entre deux ordinateurs connectés au système, sans transiter par un serveur central. Le système informatique en question pourrait, à notre sens, être l'ordinateur de chacun des interlocuteurs ou le réseau du fournisseur d'accès à internet (comme *Proximus* ou *Orange*) ; par contre, la localisation de *Skype* ne jouerait aucun rôle.

3. Vers quelle définition du territoire et de la souveraineté dans un cybermonde ?

Face à ces différents constats, la question fondamentale reste de savoir quelle souveraineté est à privilégier dans un cybermonde. Clairement, il y a plusieurs critères de rattachement en concurrence qui s'appliquent à géométrie variable aux différentes mesures d'enquête relative à la collecte des preuves numériques. Ces différences sont encore renforcées par les divergences au niveau national : alors que certains États tiennent très fort à la localisation des données et imposent parfois même des obligations de localisation des données aux fournisseurs étrangers actifs sur leur territoire (par exemple la Chine ou la Russie), d'autres s'en distancient explicitement (par exemple les États-Unis[33]). Tandis que certains États se centrent plutôt sur la présence (physique ou virtuelle) des fournisseurs de services sur leur territoire (par exemple la Belgique[34]), d'autres simplement admettent l'application extraterritoriale de certains pouvoirs (par exemple le Royaume-

---

[26] Articles 18, paragraphe 2 et 19, paragraphe 1er de la convention de l'UE relative à l'entraide judiciaire (« *besoin de l'aide technique* », « *systèmes de services de télécommunications qui opèrent sur leur territoire via une station terrestre* »).

[27] Article 29, paragraphe 1er de la convention sur la cybercriminalité.

[28] Articles 19 et 31, paragraphe 1er de la convention sur la cybercriminalité.

[29] Proposition de règlement *e-evidence*, exposé des motifs, p. 14.

[30] Proposition de règlement *e-evidence*, exposé des motifs, p. 14.

[31] Article 18, paragraphe 2, b) (la présence de la cible *et* la possibilité technique d'intercepter) et article 19, paragraphe 2 (la présence de la cible *et* la présence du fournisseur de services) de la convention de l'UE relative à l'entraide judiciaire.

[32] Paragraphe 295 du rapport explicatif de la convention sur la cybercriminalité, nous soulignons. *Cf.* article 20, paragraphe 1er de la convention sur la cybercriminalité, qui prévoit la même mesure d'enquête au niveau national : « *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes: a) à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire (…) en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique*. »

[33] 18 U.S. Code § 2713 : « *A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States*. » (Nous soulignons.)

[34] Voy. notamment les articles 46*bis*, § 1er, 88*bis*, § 1er et 90*quater*, § 2 du Code d'instruction criminelle, disponible sur http://www.ejustice.just.fgov.be/eli/loi/1808/11/17/1808111701/justel.

Uni[35]). Le manque de consensus international et d'approche uniforme pour toutes les mesures d'enquête crée inévitablement des conflits de lois et de l'insécurité juridique.
Cependant, une chose est certaine : selon l'approche choisie, le besoin d'entraide judiciaire se fera ressentir plus ou moins fortement. Plus un État adhère à une définition large et englobante des concepts de territoire et de compétence territoriale, plus la problématique de la collecte « transfrontière » est limitée.
Si l'on opte, par exemple, pour le critère de l'endroit où les données sont localisées, les autorités compétentes de l'État qui mène l'enquête pénale devront se tourner vers l'État sur le territoire duquel se trouvent les données. Seulement, dans la réalité des choses, la localisation des données dépend de plusieurs facteurs, comme les choix économiques du fournisseur de services et la structure décentralisée de l'internet. De plus, les données se trouvent (ou restent) rarement à un seul endroit[36]. Dès lors, les autorités judiciaires auront du mal à déterminer à quel État étranger adresser leur requête d'entraide judiciaire.
Si on choisit, au contraire, l'endroit où les services sont offerts comme critère de rattachement au territoire, les pouvoirs territoriaux des autorités compétentes s'accroissent considérablement – tel a été le choix du législateur belge en adoptant la loi du 25 décembre 2016[37]. Théoriquement, les autorités belges peuvent obliger à faire collaborer tous les fournisseurs de services qui ciblent le territoire belge, peu importe où se situe leur siège social et/ou infrastructure technique[38]. Par contre, la Cour de cassation française a considéré qu'un fournisseur de services étranger (en l'espèce *Google*) n'est pas contraint à produire des données d'identification et autres aux autorités policières françaises si ces dernières lui demandent directement (c'est-à-dire sans passer par une requête d'entraide judiciaire) de fournir ces données ; il s'agit simplement d'une demande de renseignements à laquelle la société étrangère est libre de répondre ou non[39]. Clairement, la France n'a pas étendu le champ d'application territorial des obligations de collaboration de la même manière que la Belgique. Toutefois, malgré le choix du législateur belge, il reste difficile, dans la réalité des choses, d'exercer une contrainte sur un fournisseur de services étranger sans l'intervention de l'État où se trouve son siège social[40]. C'est la raison pour laquelle la Commission européenne vise à créer, dans le cadre de sa proposition *e-evidence*, l'obligation pour les fournisseurs de services actifs sur le marché de l'UE de désigner un représentant légal dans (au moins) un État membre[41] ; ce dernier assurerait alors la bonne collaboration avec l'État membre émettant l'injonction de production ou de préservation des données[42].
De manière plus générale, que se passerait-il si tous les États décidaient de procéder de la même façon que la Belgique ? Un clash de pouvoirs souverains deviendrait alors inévitable, entraînant des conséquences pernicieuses pour les citoyens et entreprises concernés. Le besoin d'une solution internationale, ou à tout le moins européenne, semble donc, une fois de plus, criant. Il est dès lors temps d'ouvrir maintenant la boîte à outils européenne afin de mieux comprendre dans quelle mesure le cadre juridique actuel répond aux enjeux et défis exposés ci-dessus.

---

[35] Section 85 de la *Investigatory Powers Act* 2016, disponible sur http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf.
[36] Voy. à ce sujet Dillon REISMAN, « Where Is Your Data Really ?: The Technical Case Against Data Localization », *Lawfare blog*, 22 mai 2017, disponible sur https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization.
[37] Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, *M.B.*, 17 janvier 2017. Pour une analyse approfondie de cette loi belge, voy. Vanessa FRANSSEN, « The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level ? », *EDPL*, 2017/4, pp. 534-542; Vanessa FRANSSEN et Olivier LEROUX, « Recherche policière et judiciaire sur internet : analyse critique du nouveau cadre législatif belge », *in* Vanessa FRANSSEN et Daniel FLORE (dir.), *Société numérique et droit pénal. Belgique, France, Europe,* Bruxelles, Larcier/Bruylant, 2019, pp. 132-216.
[38] Tel a encore été confirmé par un arrêt récent de la Cour de cassation belge dans l'affaire *Skype* : Cass. 19 février 2019, R.G. P.17.1229.N.
[39] Cass. crim., 6 novembre 2013, n°12-87.130, ECLI:FR:CCASS:2013:CR05362 : « *les officiers de police judiciaire n'ont, en principe, compétence que dans les limites territoriales où ils exercent leurs fonctions habituelles, il ne leur est pas interdit de recueillir, notamment par un moyen de communication électronique, des renseignements en dehors de leur circonscription, fût-ce en adressant directement une demande à une personne domiciliée à l'étranger, celle-ci restant, dans ce cas, libre de ne pas y répondre* ». (Nous soulignons.)
[40] Pour une excellente analyse de cette problématique, voy. Kristel DE SCHEPPER et Frank VERBRUGGEN, « Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners », *T. Strafr.* 2013, pp. 156-166.
[41] Article 3 de la proposition de directive *e-evidence*.
[42] Article 14 de la proposition de règlement *e-evidence*.

Section 3 : La boîte à outils européenne

Les instruments européens de coopération judiciaire en matière pénale sont élaborés à un double niveau, celui du Conseil de l'Europe et celui de l'UE. De nombreuses interactions existent entre ces organisations et les instruments qu'elles adoptent, comme nous l'exposerons dans les prochains paragraphes. Notre propos aura pour objet de retracer l'évolution législative relative à la collecte transfrontière de preuves numériques et de mettre en avant les perspectives futures en la matière.

1. Les anciens instruments : la coopération judiciaire classique

Dès 1959, le **Conseil de l'Europe** crée un premier instrument, fondé sur la coopération entre deux États, en adoptant la **convention européenne d'entraide judiciaire en matière pénale** (ci-après : « la convention européenne de 1959 »)[43]. Le premier paragraphe de l'article 1er contient un engagement de principe qui confère à la convention un champ d'application potentiellement large dès lors que les États parties à la convention s'engagent à s'accorder mutuellement l'aide judiciaire la plus large possible dans toute procédure visant des infractions dont la répression est de la compétence des autorités judiciaires de la partie requérante. La coopération mise en place par la convention s'exécute par le biais de commissions rogatoires[44]. Elles consistent pour l'autorité judiciaire d'un pays (autorité requérante) à donner mandat à une autorité judiciaire étrangère (autorité requise) afin que cette dernière procède, en lieu et place de l'autorité requérante, à un ou plus actes d'enquête spécifiés par le mandat[45]. Les actes sont exécutés dans les formes prévues par la législation nationale de l'autorité requise[46] et la transmission des commissions rogatoires s'effectue, en règle générale, par l'intermédiaire des ministères de la Justice des deux États parties concernés[47]. Cette convention ne prévoit rien de spécifique en matière de preuves numériques, qui n'existaient pas encore au moment de l'adoption de la convention, mais peut néanmoins s'y appliquer compte tenu de son champ d'application général.

Quatre décennies plus tard, l'**UE** adopte la **convention de l'UE relative à l'entraide judiciaire**, qui est destinée à compléter la convention européenne de 1959 et ses règles sont établies sur la base des principes contenus dans cette même convention[48]. Nonobstant cette relation de filiation à la convention européenne de 1959, la convention de l'UE relative à l'entraide judiciaire modifie substantiellement la coopération judiciaire entre États Membres de l'UE sur deux points. D'une part, elle facilite le fonctionnement de l'entraide par l'instauration de principes nouveaux, dont celui de l'application du droit de l'État requérant pour l'exécution des demandes[49]. D'autre part, elle règle de nouvelles formes de coopération qui ne l'étaient pas jusqu'alors (ou pas de manière explicite), telles que les équipes communes d'enquête et l'interception des télécommunications[50], et qui s'avèrent utiles pour la collecte transfrontière de preuves numériques.

2. Les instruments contemporains : innovations et reconnaissance mutuelle

En 2001, le **Conseil de l'Europe** adopte la **convention sur la cybercriminalité**. Le caractère précurseur de cet instrument se traduit par un mélange unique en termes de contenu. En effet, la convention contient tant des dispositions de droit matériel[51] que de droit procédural[52] ainsi que de coopération internationale[53]. Contrairement à ce que son titre suggère, son champ d'application procédural dépasse nettement le phénomène de la cybercriminalité ; les mesures d'enquête visées ont en effet vocation à s'appliquer « *à toutes les autres infractions pénales commises au moyen d'un système informatique* » et « *à la collecte des preuves électroniques*

---

[43] Convention européenne d'entraide judiciaire en matière pénale, adoptée à Strasbourg le 20 avril 1959. Cette convention fut par la suite complétée par deux protocoles additionnels : protocole additionnel à la convention européenne d'entraide judiciaire en matière pénale, adopté à Strasbourg le 13 mars 1978 et deuxième protocole additionnel à la convention européenne d'entraide judiciaire en matière pénale, adopté à Strasbourg le 8 novembre 2001.

[44] Article 3 de la convention européenne de 1959.

[45] Rapport explicatif de la convention européenne de 1959, p. 5.

[46] Article 3, paragraphe 1er de la convention européenne de 1959.

[47] Article 15, paragraphe 1er de la convention européenne de 1959.

[48] Considérants 5 et 8, respectivement, de la convention de l'UE relative à l'entraide judiciaire.

[49] Article 4, paragraphe 1er de la convention de l'UE relative à l'entraide judiciaire.

[50] Articles 13 et 17 à 22, respectivement, de la convention de l'UE relative à l'entraide judiciaire ; Daniel FLORE, *Droit pénal européen : les enjeux d'une justice pénale européenne*, 2ème éd., Bruxelles, Larcier, 2014, p. 499, n° 895.

[51] Les articles 2 à 10 de la convention sur la cybercriminalité créent, entre autres, des infractions relatives aux atteintes à la confidentialité, à l'intégrité et la disponibilité des données.

[52] Articles 14 à 21 de la convention sur la cybercriminalité.

[53] Articles 23 à 35 de la convention sur la cybercriminalité. À l'instar d'autres conventions du Conseil de l'Europe, la convention sur la cybercriminalité prévoit une base juridique pour l'extradition.

de toute infraction pénale »[54]. La convention impose, entre autres, aux États parties de pouvoir mettre en œuvre des injonctions de produire des données informatiques spécifiées relatives aux abonnés auprès des fournisseurs de services actifs sur leur territoire[55]. À l'heure actuelle, elle a été ratifiée par soixante-trois États dont certains ne sont pas membres du Conseil de l'Europe, ce qui démontre toute l'importance et l'utilité de cette convention qui n'est égalée par aucun autre instrument international[56]. Par ailleurs, et comme nous le verrons par la suite, le mécanisme de l'injonction de production de données a inspiré l'UE qui en fera sa propre application.

Au sein de l'UE, la directive DEE adoptée le 3 avril 2014[57] établit un système global d'obtention de preuves dans les affaires revêtant une dimension transfrontière sur le fondement du principe de reconnaissance mutuelle[58]. La **décision d'enquête européenne** se définit comme une décision judiciaire émise ou validée par une autorité judiciaire dans un État membre afin de faire exécuter une ou plusieurs mesures d'enquête spécifiques dans un autre État membre en vue d'obtenir des preuves[59]. Bien que la directive n'ait pas été élaborée spécifiquement pour permettre la collecte de preuves numériques, son champ d'application matériel lui confère un potentiel considérable en la matière. En vertu de l'article 3 de la directive, la décision d'enquête européenne couvre toute mesure d'enquête, à l'exception de la création d'une équipe commune d'enquête[60], pourvu que la mesure existe dans le pays d'exécution[61]. Afin d'assurer l'admissibilité des preuves, la directive, de manière similaire à la convention de l'UE relative à l'entraide judiciaire, prévoit que la décision est exécutée de la manière et suivant les modalités indiquées par l'État d'émission[62].

L'introduction de délais par la directive DEE représente une évolution considérable en comparaison aux commissions rogatoires et mesures d'entraide contenues dans la convention de l'UE relative à l'entraide judiciaire pour lesquelles aucune limite de temps n'est imposée à l'État d'exécution[63]. La directive DEE pose pour principe que la mesure d'enquête doit être réalisée avec la même célérité et priorité que dans le cadre d'une procédure nationale similaire. Elle impose également un délai de maximum trente jours à l'autorité d'exécution pour décider si elle reconnaît la décision et y donnera suite[64]. L'hypothèse de l'urgence, des contraintes procédurales existant de l'État d'émission et celle de la gravité de l'infraction justifiant des délais plus brefs sont également envisagées par la directive DEE[65]. En ce qui concerne les acteurs impliqués dans la coopération, il y a là une volonté claire de la part du législateur européen de la confier à des autorités qui sont directement responsables pour prendre ou exécuter les décisions concernées. Cela se traduit par une judiciarisation de la coopération[66].

Soulignons, cependant, que, malgré son potentiel, la directive DEE présente plusieurs inconvénients pour la collecte de preuves numériques. Un premier inconvénient majeur réside dans l'hypothèse où il n'existe pas de mesure d'enquête similaire à celle demandée par l'État d'émission dans l'État d'exécution. Il ressort de l'article 10, paragraphe 5 de la directive DEE que, dans pareil scénario, la décision d'enquête européenne ne pourra tout simplement pas être exécutée. Tel serait par exemple le cas où l'État d'exécution ne connaît la

---

[54] Article 14, paragraphe 2, b) et c) de la convention sur la cybercriminalité. Voy. aussi *supra*.

[55] Article 18, paragraphe 1, b) de la convention sur la cybercriminalité.

[56] La convention a été ratifiée par 44 des 47 États membres du Conseil de l'Europe (il ne manque que l'Irlande, la Russie et la Suède) et 19 États sont parties à la convention sans être membre du Conseil de l'Europe, comme c'est le cas pour les États-Unis et le Canada. Pour un aperçu complet des ratifications, voy. https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=lD2Dt351.

[57] Cette directive remplace la décision-cadre 2008/278/JAI du Conseil du 18 décembre 2008 qui concernait la reconnaissance mutuelle des mandats européens d'obtention des preuves.

[58] Considérant 6 de la directive DEE. Pour une analyse plus détaillée de cet instrument, voy. Mona GIACOMETTI, « La décision d'enquête européenne : la révolution de la coopération judiciaire entre États membres de l'Union est en marche ! » *J.T.*, 2017, pp. 649 à 660.

[59] Article 1er, paragraphe 1er de la directive DEE.

[60] Ces équipes font l'objet d'une réglementation spécifique à l'article 13 de la convention de l'UE relative à l'entraide judiciaire ainsi que dans la décision-cadre 2002/465/JAI du Conseil du 13 juin 2002 relative aux équipes communes d'enquête (*J.O.U.E.*, L 162, 20 juin 2002, p. 1). Sur ce point, voy. également Daniel FLORE, *op. cit.*, p. 558, n° 976.

[61] Sur ce dernier point, la directive prévoit le recours à un type différent de mesure d'enquête pour les hypothèses où la mesure demandée par l'État d'émission n'existerait pas dans le droit de l'État d'exécution ou si elle n'était pas disponible dans le cadre d'une procédure nationale similaire. Article 10, paragraphe 1er, a) et b) respectivement.

[62] Article 9 de la directive DEE.

[63] Article 12 de la directive DEE.

[64] Article 12, paragraphes 1er et 3 de la directive DEE.

[65] Article 12, paragraphe 2 de la directive DEE.

[66] Daniel FLORE, *op. cit.*, p. 659, n° 1160 ; article 7 de la directive DEE.

mesure de préservation (ou conservation) rapide de données informatiques, malgré que cette mesure soit imposée par la convention sur la cybercriminalité[67]. L'État d'émission peut, toutefois, proposer une autre mesure permettant d'atteindre le même résultat[68].

Un deuxième désavantage se situe au niveau des délais prévus par la directive DEE. Alors que leur introduction constitue une amélioration substantielle par rapport à la convention de l'UE relative à l'entraide judiciaire, certains auteurs notent, à juste titre, que les délais contenus dans la directive DEE sont trop longs pour la collecte de preuves numériques qui sont caractérisées par leur nature volatile (*supra*)[69].

Enfin, troisième bémol, la directive DEE n'est pas applicable à l'Irlande alors que cet État héberge le siège social de nombreux fournisseurs de services dont celui de *Facebook Ireland Ltd*. À l'égard de cet État membre, les instruments plus anciens continuent donc à s'appliquer.

Pour le surplus, la décision d'enquête européenne n'est sans doute pas encore suffisamment connue des autorités judiciaires nationales étant donné son caractère récent – le délai de transposition s'est écoulé le 22 mai 2017[70]. Il faudra encore qu'elle s'inscrive dans la pratique quotidienne pour que l'on puisse en mesurer l'impact réel.

3. Les futurs instruments : vers un nouveau paradigme

Au niveau du **Conseil de l'Europe**, les travaux du Comité de la convention sur la cybercriminalité pour l'adoption d'un **second protocole additionnel à la convention sur la cybercriminalité** ont débuté en septembre 2017 et il était initialement prévu de les conclure en décembre de cette année[71]. Toutefois, compte tenu de la complexité des questions en cause et des grands enjeux, il a été décidé en juillet 2019 de prolonger le mandat de négociation d'un an, jusqu'en décembre 2020[72]. Les négociations poursuivent la réalisation de plusieurs objectifs dont une entraide judiciaire plus efficace et l'instauration d'une coopération directe entre autorités nationales et fournisseurs de services[73]. Par ailleurs, la collecte de preuves numériques se situant à l'intersection de plusieurs branches du droit, le droit pénal doit composer, notamment, avec les règles en matière de protection des données – élément qui n'échappe pas aux négociations actuellement menées[74]. Après une consultation publique des acteurs intéressés (secteur privé, société civile et experts en protection des données) en février 2019 à propos d'une future procédure d'urgence en matière d'entraide judiciaire et d'une plus grande flexibilité relative à la langue dans laquelle une requête d'entraide judiciaire peut être rédigée[75], de nouveaux textes sur d'autres sujets plus importants et bien plus sensibles (comme la coopération directe avec les fournisseurs de services, la compétence dans le cyberespace et l'extension d'une recherche

---

[67] Articles 16 et 17 de la convention sur la cybercriminalité.

[68] Article 10, paragraphe 5 de la directive DEE.

[69] Stanislaw TOSZA, « Cross-border gathering electronic evidence : mutual legal assistance, its shortcomings and remedies», *in* Vanessa FRANSSEN et Daniel FLORE (dir.), *Société numérique et droit pénal. Belgique, France, Europe,* Bruxelles, Larcier/Bruylant, 2019, pp. 277 ; Mona GIACOMETTI, « La collecte transfrontalière de preuves numériques selon le point de vue belge : la décision d'enquête européenne, un moyen approprié ? », in Vanessa FRANSSEN et Daniel FLORE (dir.), *Société numérique et droit pénal. Belgique, France, Europe,* Bruxelles, Larcier/Bruylant, 2019, pp. 306-307.

[70] Échéance qui a tout juste été respectée par la Belgique en adoptant la loi du 22 mai 2017 relative à la décision d'enquête européenne en matière pénale, *M.B.*, 23 mai 2017. Pour une analyse de la transposition en droit belge, voy. Mona GIACOMETTI, « La collecte transfrontalière de preuves numériques selon le point de vue belge : la décision d'enquête européenne, un moyen approprié ? », *in* Vanessa FRANSSEN et Daniel FLORE (dir.), *op. cit.*, pp. 287-315.

[71] Comité de la Convention sur la cybercriminalité (T-CY), Mandat pour la préparation d'un projet de 2e protocole à La Convention de Budapest sur la Cybercriminalité, adopté par la 17e Réunion Plénière du T-CY le 8 juin 2017, T-CY (2017)3, disponible sur https://rm.coe.int/mandat-pour-la-preparation-d-un-projet-de-2e-protocole-a-la-convention/168072380f. Pour un aperçu de l'état d'avancement de ces négociations, voy. https://www.coe.int/fr/web/cybercrime/t-cy-drafting-group. Observons toutefois que le site en français n'est pas entièrement à jour ; les derniers textes n'y figurent pas. Il est donc important de consulter aussi le site en anglais : https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.

[72] T-CY, Etat d'avancement des négociations relatives au 2ème Protocole additionnel à la Convention de Budapest, Note de la part du Président à l'attention de la 21ème Réunion Plénière du T-CY (8 juillet 2019), 23 juin 2019, T-CY (2019)19, disponible sur https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff (uniquement disponible en anglais).

[73] T-CY, Mandat pour la préparation d'un projet de 2e protocole à La Convention de Budapest sur la Cybercriminalité, adopté par la 17e Réunion Plénière du T-CY le 8 juin 2017, T-CY (2017)3, p. 3.

[74] *Ibidem*, p. 4.

[75] Ces textes provisoires sont disponibles en version anglaise sur le site du T-CY : https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-budapest-convention-further-consultatio-1 (consulté le 9 septembre 2019).

dans un système informatique situé à l'étranger) seront présentés et analysés de plus près lors de la prochaine conférence *Octopus*[76].

De son côté, l'**UE** devrait disposer dans le futur d'un instrument calibré spécifiquement pour la collecte transfrontière de preuves numériques[77]. La **proposition *e-evidence* de la Commission européenne**, déjà évoquée à plusieurs reprises, comprend, d'une part, un corps de règles contenues dans un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques[78] et, d'autre part, un cadre établi par une directive établissant des règles harmonisées concernant la désignation de représentant légaux aux fins de collecte de preuves en matière pénale[79]. Ces instruments introduisent un nouveau paradigme pour la collecte des preuves numériques qui consiste en une coopération directe entre autorités judiciaires d'un État membre de l'Union et un fournisseur de services qui se situe dans un autre État Membre. Grâce à la proposition de règlement, une autorité judiciaire d'un État membre pourra enjoindre à un acteur privé, en l'espèce un fournisseur de services[80], de produire ou de conserver des données, quelle que soit la localisation de ces données (*supra*)[81]. L'application du règlement futur requiert une situation transfrontière, laquelle existe lorsque le fournisseur de services est établi ou représenté dans un autre État membre que celui où l'enquête pénale est menée. Le futur règlement trouvera également à s'appliquer si le fournisseur de services n'est pas établi au sein de l'Union (comme les GAFAM[82]) mais y propose ses services[83]. *A contrario*, la proposition de règlement ne vise pas les fournisseurs de services actifs dans un seul État membre ; ceux-ci resteront soumis à la législation nationale. Toutes les données informatiques peuvent faire l'objet d'une injonction de produire pour autant qu'elles soient stockées. Ces données devront servir de preuves dans le cadre d'enquêtes judiciaires ou de procédures pénales concrètes[84]. Les injonctions ne pourront être émises dans un but de prévention ; dès lors, l'infraction pénale devra avoir été déjà commise, mais peu importe que le(s) auteur(s) soi(en)t connu(s) ou inconnu(s)[85]. De ce fait, l'ouverture d'une enquête pour une infraction particulière se pose comme condition préalable à l'application du règlement[86]. Enfin, le règlement innove par rapport à tous les autres instruments que nous venons d'analyser en ce qu'il introduit de très courts délais pour l'exécution de l'injonction de production[87] et prévoit des sanctions applicables aux fournisseurs de services qui ne respecteraient pas leurs obligations[88].

La proposition de directive *e-evidence* permet la mise en œuvre du règlement en ce qu'elle impose aux fournisseurs de services concernés de désigner un représentant légal dans un État membre (*supra*)[89]. Ce

---

[76] Cette conférence aura lieu du 20 au 22 novembre 2019. Pour plus d'informations, voy. https://www.coe.int/en/web/cybercrime/octopus-conference (uniquement disponible en anglais).

[77] Proposition de règlement *e-evidence*. Le 7 décembre 2018, le Conseil de l'UE a adopté son orientation générale concernant la proposition de règlement, modifiant le texte initialement proposé par la Commission européenne sur plusieurs points. La version consolidée est disponible sur https://data.consilium.europa.eu/doc/document/ST-15292-2018-INIT/en/pdf (uniquement disponible en anglais). Le 17 mai 2019, un supplément comprenant les annexes au règlement a été publié, disponible sur https://data.consilium.europa.eu/doc/document/ST-9365-2019-INIT/en/pdf (uniquement disponible en anglais). Le Parlement européen, de son côté, n'a pas encore pris de position sur la proposition. Il a toutefois produit plusieurs documents de travail, le dernier datant du 1er avril 2019 ; ces documents sont disponibles sur https://www.europarl.europa.eu/committees/en/libe/working-documents.html#sidesForm.

[78] Proposition de règlement *e-evidence*.

[79] Proposition de directive *e-evidence*. Notons que le Conseil de l'UE a adopté début mars 2019 son orientation générale concernant cette proposition de directive. La version consolidée, qui se distingue sur bon nombre de points du texte initial de la Commission européenne, est disponible sur https://data.consilium.europa.eu/doc/document/ST-7348-2019-INIT/en/pdf (uniquement disponible en anglais).

[80] Article 2, (3) de la proposition de règlement *e-evidence*. La proposition de règlement s'applique aux fournisseurs de services qu'il définit en créant trois sous-catégories.

[81] Article 1er de la proposition de règlement *e-evidence*.

[82] Acronyme renvoyant aux géants du web Google, Apple, Facebook, Amazon et Microsoft.

[83] Article 3, paragraphe 1er de la proposition de règlement *e-evidence*. Le règlement définit également ce que comprend l'expression « *proposer des services dans l'Union* » (article 2 (4)).

[84] La procédure pénale s'entend de « *la phase d'instruction préalable au procès jusqu'à la clôture de la procédure par voie de jugement ou d'une autre décision* ». Proposition de règlement *e-evidence*, exposé des motifs, p. 5.

[85] Proposition de règlement *e-evidence*, exposé des motifs, p. 5.

[86] Proposition de règlement *e-evidence*, exposé des motifs, p. 17.

[87] Article 9, paragraphes 1er et 2 de la proposition de règlement *e-evidence*. Pour les injonctions de conservation, la proposition de règlement prévoit que les données sont conservées « *sans retard injustifié* » (article 10, paragraphe 1er).

[88] Article 13 de la proposition de règlement *e-evidence*.

[89] Article 3 de la proposition de directive *e-evidence*.

représentant légal se verra notifier les injonctions de production et de conservation émises par les autorités judiciaires des autres États membres.

Un point sur lequel la proposition *e-evidence* pose toutefois question est qu'elle confère aux fournisseurs de services un rôle clé qui incombe traditionnellement aux États membres. Il découle du fait que ces acteurs privés sont les destinataires directs de l'injonction qu'ils seront seuls habilités à vérifier si celle-ci n'enfreint pas manifestement la Charte des droits fondamentaux de l'UE ou n'est pas manifestement abusive[90]. Ce rôle des fournisseurs de services a déjà provoqué un débat intense au sein du Conseil de l'UE[91] et constitue une préoccupation majeure pour le Parlement européen[92], la société civile[93] et les fournisseurs de services PME[94].

Au moment d'écrire ces lignes, la proposition *e-evidence* n'a pas encore été adoptée mais force est de constater qu'elle présente plusieurs lacunes[95]. Nous n'en mentionnerons que deux en guise d'exemples. D'une part, la proposition *e-evidence* ne s'applique pas aux données non stockées. En conséquence, elle n'offre pas de solution pour les incertitudes créées par la jurisprudence de la CJUE précitée en matière de conservation de données de trafic et de localisation. De l'autre, la proposition ne résout pas les problèmes liés au droit national de certains fournisseurs de services qui ne sont pas installés dans l'UE. À cet égard, il est important de mentionner les **États-Unis** puisqu'ils hébergent le siège social de plusieurs grands groupes tels que *Facebook* et *Google*. Cette dimension transatlantique de la collecte des preuves ne fera pas l'objet de notre propos mais nous tenons à préciser que les États-Unis ont adopté le 23 mars 2018 le ***CLOUD Act***[96]. Cette législation devrait permettre de lever l'obstacle contenu dans l'*United States Electronic Communications Privacy Act*[97] – qui, présentement, interdit aux fournisseurs de services américains de transmettre des données relatives au contenu à des autorités étrangères – puisqu'elle autorise le gouvernement des États-Unis à conclure des accords avec les gouvernements d'autres États concernant l'accès aux données conservées par des fournisseurs de services américains[98]. En février 2019, la Commission européenne avait demandé au Conseil de l'UE l'autorisation de négocier un accord avec les États-Unis pour l'accès transfrontière aux preuves numériques[99], autorisation qui a été accordée en juin dernier[100]. Toutefois, comme l'ont déjà souligné plusieurs

---

[90] Article 9, paragraphe 5, al. 2 de la proposition de règlement *e-evidence.*

[91] Pour un aperçu des négociations et des points faisant l'objet d'intenses discussions, voy. Vanessa FRANSSEN, « The European Commission's E-evidence Proposal : Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement », *European Law Blog*, 12 octobre 2018, disponible sur http://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/ ; Théodore CHRISTAKIS, « 'Big Divergences of Opinions' on E-evidence in the EU Council : A Proposal in Order to Disentangle the Notification Knot », *Cross-border Data Forum*, 22 octobre 2018, disponible sur https://www.crossborderdataforum.org/big-divergence-of-opinions-on-e-evidence-in-the-eu-council-a-proposal-in-order-to-disentangle-the-notification-knot/.

[92] Birgit SIPPEL et Daniel DALTON, au nom de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, 3e Document de travail (A) sur la proposition de règlement relative aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale (2018/0108 (COD)) – Exécution des EPOC(-PR) et role des fournisseurs de services, DT\1177089FR, 13 février 2019, p. 5, disponible sur : http://www.europarl.europa.eu/doceo/document/LIBE-DT-634849_FR.pdf?redirect.

[93] Voy., par exemple, EUROPEAN DIGITAL RIGHTS, « EU "e-evidence" proposal turns service providers into judicial authorities », disponible sur https://edri.org/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities/, 17 avril 2018.

[94] Voy., par exemple, EuroISPA, « Proposal for a regulation on European production and preservation orders for electronic evidence in criminal matters», disponible sur http://www.euroispa.org/e-evidence-euroispa-adopts-position-paper/, 3 juillet 2018.

[95] Sur ce point voy. Vanessa FRANSSEN, « The European Commission's E-evidence Proposal : Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement », *op. cit.*

[96] Consolidated Appropriation Act of 2018, Division V – Clarifying Lawful Overseas Use of Data Act, Pub. L. n°. 115-141, 132 Stat. 348 (2018). Pour une analyse succincte, voy. Jennifer DASKAL, « Unpacking the *CLOUD Act* », *eucrim*, 2018/4, pp. 220-225.

[97] Electronic Communications Privacy Act of 1986 : an Act to amend title 18 of the United States Code with respect to the interception of certain communications, other forms of surveillance, and for other purposes. Texte intégral disponible sur https://www.law.cornell.edu/topn/electronic_communications_privacy_act_of_1986.

[98] Voy. Stanislaw TOSZA, *op. cit.*, pp. 284-285.

[99] Commission européenne, Recommendation for a Council Decision authorizing the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM (2019) 70 Final, Bruxelles, 5 février 2019, uniquement disponible en anglais sur https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf.

[100] Le texte final du mandat accordé ne semble pas encore disponible, mais les textes préparés en amont le sont : Décision du Conseil autorisant l'ouverture de négociations en vue de conclure un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale, 9114/19, 21 mai 2019, disponible sur : https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/fr/pdf ; Addendum à la recommandation de décision du Conseil autorisant l'ouverture de négociations en vue de la conclusion d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire

auteurs outre-Atlantique, la conclusion d'un accord entre l'UE et les États-Unis basé sur le *CLOUD Act* soulève plusieurs questions[101]. Il convient de s'interroger, entre autres, sur l'étendue de la compétence de l'UE pour négocier un tel accord (l'adoption du mandat de négociation semble résoudre cette question, du moins pour l'instant) et, de façon plus fondamentale, de déterminer si l'Union peut être considérée comme gouvernement d'un état étranger (*foreign government*), terme que ne définit pas le *CLOUD Act*. A notre connaissance, les négociations entre l'UE et les États-Unis n'ont pas encore formellement commencé, mais dans une déclaration conjointe les deux pouvoirs ont reconnu l'importance d'élaborer une solution qui assure un accès transfrontière rapide à des preuves numériques et les États-Unis ont déclaré prendre des mesures en vue de l'ouverture des négociations avec l'UE[102]. À suivre.

Section 4 : <u>Quelques enjeux et besoins futurs</u>

Comme l'analyse de la boîte à outils européenne l'a révélé, l'**actuel cadre juridique** relatif à la collecte de preuves numériques est **fort éclaté et reste inachevé**. Certains instruments sont d'ordre très général, conçus pour l'entraide judiciaire classique, sans prendre en compte la spécificité de la problématique de la preuve numérique, telle la nature volatile des données ou la difficulté de les localiser. D'autres instruments sont plus spécifiques, comme la convention sur la cybercriminalité, ou plus rapides, telle la directive DEE, mais présentent tout de même des lacunes importantes. Ainsi, la convention sur la cybercriminalité repose encore très fortement sur l'entraide judiciaire classique, alors que la pratique des enquêtes pénales démontre que l'entraide judiciaire est trop lente et souvent inefficace, raison pour laquelle les autorités compétentes recourent de plus en plus souvent à la collaboration directe avec des fournisseurs de services étrangers[103]. Toutefois, la nature de cette collaboration pose question : est-elle purement volontaire ou obligatoire et quelles sont les garanties encadrant cette collaboration ? Les législations (et pratiques) nationales divergent énormément sur ce point, comme nous l'avons illustré de manière ponctuelle dans ce qui précède. Ces divergences sont également dévoilées dans le cadre d'un projet de recherche de droit comparé que nous menons à l'heure actuelle[104]. La directive DEE, pour sa part, permet une collaboration judiciaire transfrontière plus rapide, mais toujours trop lente pour être vraiment utile en matière de preuves numériques, une procédure d'urgence n'étant pas prévue. De plus, les instruments analysés ne s'appliquent pas tous aux mêmes États : certains s'appliquent uniquement à l'UE (mais pas forcément à tous les États membres) ou au Conseil de l'Europe (mais la ratification de certains États du Conseil de l'Europe fait défaut), d'autres s'appliquent même à des États non-européens. Par conséquent, le praticien du droit est confronté à un cadre juridique qui s'applique à géométrie variable. Dans chaque dossier et pour chaque mesure d'enquête, il faut se demander quel instrument est applicable et lequel est le plus spécifique ou adéquat.

Le **besoin d'un cadre juridique plus homogène** au niveau européen, voire à l'échelle mondiale, est criant, mais sa réalisation ne sera pas pour demain. Il reste à voir quel sera le résultat des négociations portant sur le second protocole additionnel à la convention sur la cybercriminalité. Ce texte pourrait avoir une portée internationale et dès lors déterminer les règles du jeu dans le monde de demain. Néanmoins, les premiers

---

en matière pénale – adoption, 9666/19, 27 mai, disponible sur : https://data.consilium.europa.eu/doc/document/ST-9666-2019-INIT/fr/pdf. Par ailleurs, notons qu'en plus d'un mandat de négociation pour un accord avec les États-Unis, le Conseil a également accordé à la Commission européenne un mandat pour négocier, au nom des États membres de l'UE, le second protocole additionnel à la convention sur la cybercriminalité. Conseil de l'UE, « Le Conseil donne mandat à la Commission pour négocier des accords internationaux concernant les preuves électroniques en matière pénale », communiqué de presse, 6 juin 2019, disponible sur : https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/ .

[101] Voy. Jennifer DASKAL, « A Possible EU-US Agreement on Law Enforcement Access to Data ? », *Lawfare Blog*, 21 mai 2018, disponible sur https://www.lawfareblog.com/possible-eu-us-agreement-law-enforcement-access-data ; Peter SWIRE, « EU and US Negotiations on Cross-Border Data, Within and Outside of the CLOUD Act Framework », *Cross-border Data Forum*, 13 avril 2019, disponible sur https://www.crossborderdataforum.org/eu-and-u-s-negotiations-on-cross-border-data-within-and-outside-of-the-cloud-act-framework/.

[102] Déclaration conjointe UE-États-Unis à l'issue de la réunion ministérielle UE-États-Unis consacrée à la justice et aux affaires intérieures, 19 juin 2019, disponible sur : https://www.consilium.europa.eu/fr/press/press-releases/2019/06/19/joint-eu-u-s-statement-following-the-eu-u-s-justice-and-home-affairs-ministerial-meeting/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Joint+EU-US+statement+following+the+EU-US+Justice+and+Home+Affairs+Ministerial+Meeting.

[103] Stanislaw TOSZA, *op. cit.*, pp. 274-277.

[104] Cette recherche porte sur la collaboration des fournisseurs de services dans le cadre des enquêtes pénales et englobe neuf États membres de l'UE et les États-Unis. Elle est financée par le Fonds de la Recherche Scientifique – FNRS de la Fédération Wallonie-Bruxelles en Belgique (subvention n° CDR J.0293.17) et par l'Université de Liège. Les résultats de cette recherche seront présentés à une conférence internationale les 25 et 26 novembre 2019 et publiés dans un ouvrage collectif début 2020.

textes semblent peu ambitieux : ils abordent la question de l'emploi des langues dans la procédure d'entraide judiciaire et prévoient une procédure d'urgence mais sans imposer des délais contraignants[105]. Bien sûr, on n'est pas encore au bout des négociations et les questions les plus délicates (comme celle concernant la collaboration directe avec des fournisseurs de services étrangers pour obtenir des données relatives au trafic et/ou au contenu) ne seront tranchées qu'à la fin. Espérons donc que les négociateurs auront le courage de vraiment avancer dans ce dossier et d'adresser les défis exposés ci-dessus. Ces négociations constituent une opportunité unique pour l'Europe de jouer, à nouveau, un rôle précurseur en allant à l'encontre du repli sur soi-même qu'on constate dans de nombreux pays.

Du côté de l'UE, la proposition *e-evidence* de la Commission européenne est très prometteuse, malgré plusieurs lacunes et le besoin d'améliorer la protection des personnes concernées, mais un accord des trois institutions n'est pas à portée de main. Les points de vue du Conseil de l'UE et du Parlement européen divergent considérablement, entre autres, et nous l'avons déjà mentionné, sur le rôle attribué aux fournisseurs de services dans le cadre du contrôle de la conformité des injonctions de production et de conservation avec les droits fondamentaux. Il faudra voir quelle sera la position du Parlement européen recomposé après les élections européennes de mai 2019[106]. En outre, le succès de cette proposition dépend également de l'accord à négocier avec les États-Unis – autre élément d'incertitude.

Toutefois, même dans l'hypothèse la plus optimiste où ces nouveaux instruments seraient adoptés et constitueraient un réel progrès, il reste des défis importants pour les années à venir. Nous nous limitons, en guise de conclusion, à en évoquer deux.

D'un côté, comment faire face à l'**emploi accru du chiffrement** et à des techniques de chiffrement puissantes ? Cette question est analysée de plus près par la Commission européenne mais, à ce jour, celle-ci n'a pas exprimé l'intention de produire un instrument législatif sur ce sujet[107]. Plusieurs réponses peuvent être envisagées. On pourrait, par exemple, obliger les fournisseurs de services et les entreprises technologiques à créer des portes dérobées. Mais cette solution est-elle compatible avec les exigences imposées par la règlementation relative aux données à caractère personnel et, plus fondamentalement, est-elle souhaitable dans une société libre et démocratique ? Ou, autre solution proposée par certains, le législateur pourrait imposer une obligation aux suspects de rendre, sous certaines conditions, la clé de déchiffrement aux autorités judiciaires. Mais cette démarche pose, à notre sens, question à la lumière du privilège contre l'auto-incrimination[108]. Finalement, ces remèdes causent plus de problèmes qu'ils n'en résolvent.

De l'autre, comment résoudre les problèmes créés par la jurisprudence de la CJUE relative à la **conservation des données de communications électroniques** ? Dans l'arrêt *Tele2 Sverige* précité, la Cour a, en effet, conclu que le respect des droits fondamentaux s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique. Toutefois, cette jurisprudence crée des obstacles presque insurmontables pour les autorités policières et judiciaires[109]. Raison pour laquelle plusieurs cours nationales ont posé de nouvelles questions préjudicielles à la CJUE, dont l'*Investigative Powers Tribunal* à Londres[110], la Cour

---

[105] T-CY, Provisional draft text of provisions : Languages of requests, Emergency MLA, Video conferencing, T-CY (2018)23, Strasbourg, 29 novembre 2018, disponible sur https://rm.coe.int/t-cy-2018-23rev-protoprov-pub-text-v4/16808ff490 (uniquement disponible en anglais).

[106] Si les discussions sur la proposition *e-evidence* ont repris depuis la recomposition du Parlement européen et que Mme Birgit SIPPEL a été redésignée comme rapporteur le 4 septembre 2019, il faudra encore un peu de temps pour connaître la route du nouveau Parlement. Voy. la fiche de procédure, disponible sur : https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2018/0108(COD) (consulté le 9 septembre 2019).

[107] Commission européenne, Onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 608, Bruxelles, 18 octobre 2017, disponible sur http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-608-F1-FR-MAIN-PART-1.PDF.

[108] Pour un autre point de vue, voy. Charlotte CONINGS et Jan KERKHOFS, « U hebt het recht te zwijgen. Uw login kan en zal tegen u worden gebruikt ? Over ontsleutelplicht, zwijgrecht en *nemo tenetur* », *Nullum Crimen*, 2018, pp. 457-472.

[109] Sur ces problèmes, voy. François MOLINS, « La protection des citoyens européens dans un monde ultra-connecté », *Fondation Robert Schuman*, 8 avril 2019, disponible sur https://www.robert-schuman.eu/fr/questions-d-europe/0510-la-protection-des-citoyens-europeens-dans-un-monde-ultra-connecte.

[110] *Privacy International*, affaire C-623/17, *J.O.U.E.*, C 22, 22 janvier 2018, p. 29.

constitutionnelle belge[111], le Conseil d'État français[112] et, plus récemment, en janvier 2019, *Riigikohus*, la cour suprême estonienne[113]. La CJUE sera ainsi amenée à confirmer ou nuancer son approche. Une première audience dans ces affaires a eu lieu le 9 septembre 2019 ; l'avis de l'avocat général ne devrait pas beaucoup tarder. Sans toutefois attendre l'aboutissement de ces affaires, le Conseil de l'UE a entre-temps demandé à la Commission de recueillir des informations supplémentaires sur les besoins concrets des autorités compétentes des États membres, d'organiser des consultations ciblées avec des acteurs concernés et de préparer une étude approfondie sur les solutions possibles en matière de conservation des données, tout en tenant compte de la jurisprudence de la CJUE[114]. Cette étude pourrait, le cas échéant, aboutir à une nouvelle initiative législative afin de combler le vide et de dissiper l'incertitude juridique qui a été créée depuis l'annulation de la directive 2006/24/CE en 2014[115]. Un premier rapport sur l'état d'avancement des travaux de la Commission est prévu pour décembre 2019. Clairement, l'automne/hiver de 2019 s'annonce chaud.

[111] *Ordre des barreaux francophones et germanophone e.a.*, affaire C-520/18; C.C., 19 juillet 2018, n° 96/2018. Pour une première analyse de cet arrêt, voy. Frank VERBRUGGEN, Sofie ROYER et Helena SEVERIJNS, « Reconsidering the Blanket-Data-Retention-Taboo, for Human Rights' Sake ? », *European Law Blog*, 1er octobre 2018, disponible sur http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/.

[112] *French Data Network e.a.*, affaires jointes C-511/18 et C-512/18.

[113] *H.K.*, affaire C-746/18.

[114] Conseil de l'UE, « La conservation des données pour lutter contre la criminalité : le Conseil adopte ses conclusions », communiqué de presse, 6 juin 2019, disponible sur : https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/data-retention-to-fight-crime-council-adopts-conclusions/.

[115] Conclusions du Conseil de l'Union européenne sur la conservation des données aux fins de la lutte contre la criminalité – adoption, 9663/19, 27 mai 2019, disponible sur : http://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/fr/pdf.