

Améliorer l'accès à la preuve numérique : un objectif européen et international



Myriam QUEMENER

Magistrat

Docteur en droit

Selon la commission européenne, les preuves électroniques sont nécessaires dans près de 85 % des enquêtes pénales et, dans les deux tiers des cas, il faut obtenir des preuves auprès de prestataires de services en ligne implantés dans une autre juridiction. L'accès à la preuve numérique EST rendu complexe en raison de législations étrangères différentes. Tel est le cas avec les États-Unis notamment puisque la plupart des grands opérateurs y sont basés. En effet, l'internationalisation des enquêtes et de la *cyberpreuve* illustre la problématique classique de la contradiction entre plusieurs normes de fond dans un espace commun.

La localisation des preuves, qui peuvent se trouver dans une juridiction différente de celle où l'infraction a eu lieu ; dans ce cas, l'obtention de preuves étrangères nécessitera un travail juridique supplémentaire. Il est essentiel que les travaux européens et internationaux aboutissent sur le plan juridique pour recueillir la preuve dans des conditions satisfaisantes et harmonisées afin de sécuriser les procédures.

Le projet de règlement e- évidence

La Commission européenne¹ a présenté un projet de directive et un projet de règlement sur l'accès aux preuves électroniques en matière pénale qui devront être adoptés par le Conseil de l'Union européenne et par le Parlement européen. Ce texte², dont la version finale doit encore être négociée avec le Parlement européen, vise à accélérer les enquêtes transfrontalières en donnant à la justice un accès plus direct aux preuves électroniques à des données de connexion ou de contenus (adresses IP, courriels, vidéos), souvent difficiles ou trop longues à obtenir auprès de prestataires basés à l'étranger. Il peut s'agir aussi de mails ou autres documents situés dans le cloud utiles aux enquêtes pénales. Ce texte devrait permettre aux autorités répressives des États membres de pouvoir accéder à des preuves se trouvant dans le « nuage » des fournisseurs de services, indépendamment de la localisation de celui-ci sur le territoire européen. Mais il devrait concerner aussi des États tiers, ce qui signifie alors un effet d'extraterritorialité. Le règlement « E-evidence » apparaît de la sorte comme une réponse, pour ne pas dire une riposte, au « Cloud Act » promulgué par le

¹ <https://ec.europa.eu/info/sites/info/files/placeholder.pdf>

² http://europa.eu/rapid/press-release_IP-18-3343_fr.htm

Président américain Donald Trump le 23 mars 2018. Ce projet intervient dans un contexte complexe de relations transatlantiques marqué par la tentative, de la part des États-Unis, d'accéder aux données à caractère personnel entre les mains des GAFAM (Google, Amazon, Facebook, Apple, Microsoft) où qu'elles se trouvent. La pratique du cloud computing complique toutefois un tel projet.

La Commission européenne propose la mise en place des mécanismes suivants :

une injonction européenne de production : elle devrait permettre à une autorité judiciaire d'un État membre de demander des preuves électroniques (telles que des courriels, des SMS ou des messages échangés dans des applications) directement auprès d'un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre, indépendamment de la localisation des données. Ce prestataire sera alors tenu de répondre dans un délai de **10 jours**, et dans les **6 heures** en cas d'urgence (contre 120 jours pour la décision d'enquête européenne existante ou 10 mois pour une procédure d'entraide judiciaire) ;

une injonction européenne de conservation, permettant d'empêcher l'effacement de données : elle devrait permettre quant à elle à une autorité judiciaire d'un État membre de contraindre un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre à conserver certaines données afin que ladite autorité puisse demander ces informations ultérieurement par voie d'entraide judiciaire ou au moyen d'une décision d'enquête européenne ou d'une injonction européenne de production.

Les mécanismes précédents doivent être assortis de **la mise en place de garanties solides ainsi que de voies de recours**. Les deux types d'injonctions ne peuvent être émis que dans le cadre de procédures pénales, et toutes les garanties procédurales de droit pénal sont applicables. Les nouvelles règles garantissent l'intervention d'autorités judiciaires et posent des exigences supplémentaires pour l'obtention de certaines catégories de données. Elles comportent

également des garanties concernant le droit à la protection des données à caractère personnel. Les prestataires de services et les personnes dont les données sont demandées bénéficieront de plusieurs garanties, parmi lesquelles la possibilité, pour le prestataire de services, de demander un examen si, par exemple, l'injonction constitue une violation manifeste de la charte des droits fondamentaux de l'Union européenne.

Une disposition du projet de règlement apparaît ensuite comme correspondant à l'effet extraterritorial du *Cloud Act* américain. Il est en effet prévu de **contraindre les prestataires de services à désigner un représentant légal dans l'Union**. De la sorte, tous les prestataires qui proposent leurs services dans l'Union européenne seraient soumis à des obligations identiques, même si leur siège est situé dans un pays tiers. Le représentant légal dans l'Union désigné nécessairement par le prestataire de services assurerait ainsi la réception, le respect et l'exécution des décisions et injonctions émises par les autorités compétentes des États membres à des fins de collecte de preuves en matière pénale.

Enfin, il est prévu par ce nouveau texte de procurer une sécurité juridique aux entreprises et aux prestataires de services. Encore souvent, les autorités répressives sont tributaires du bon vouloir des prestataires de services à leur remettre les preuves dont elles ont besoin. Avec le nouveau règlement, s'il est adopté, les autorités et prestataires de services bénéficieront d'une plus grande sécurité juridique grâce à la mise en œuvre de règles identiques pour tous en matière de fournitures de preuves électroniques. Il reste à cerner les enjeux de cet ambitieux texte, qui devra franchir toutes les étapes du processus législatif avant les élections du Parlement européen en 2019.

L'aboutissement de ces travaux est désormais urgent car les enjeux sont très forts afin de lutter plus efficacement contre la délinquance qui s'est pleinement adaptée au numérique.