Dossier spécial

Impact de la directive et du règlement *e-evidence* sur les avocats

Virginie Bensoussan-Brulé*
Avocat, Lexing Alain Bensoussan Avocats, Directrice du pôle Contentieux du numérique

Cyrielle Girard-Berthet*
Auditrice de justice de la promotion 2020, Ecole Nationale de la Magistrature
(* Les observations contenues dans cet article appartiennent à leurs auteurs et n'engagent pas d'autres organismes ou personnes)

Le passage à l'ère du numérique a incontestablement entraîné une évolution de la criminalité et des moyens de lutte contre celle-ci.

Les délinquants ont rapidement perçu tout le potentiel des outils numériques. Les nouvelles technologies leur offrent de nouveaux moyens pour commettre des infraction, et leur permettent de développer de nouvelles formes de fraudes, notamment informatiques.

Pour faire face à ces nouvelles pratiques, les services d'enquête ont dû rapidement faire preuve d'adaptation, en ayant notamment recours aux nouvelles technologies pour procéder à la recherche des auteurs d'infractions.

Les juridictions pénales ont également dû se préparer à l'arrivée du numérique, les preuves électroniques étant de plus en plus fréquentes dans les diverses procédures. Ainsi, on estime que aujourd'hui près de 85 % des enquêtes pénales font intervenir des données numériques. Il s'agit, notamment, de données relatives à la téléphonie, à la géolocalisation, à des données d'identification de comptes en ligne, ou encore au contenu audiovisuel d'appareils électroniques divers.

Le législateur français a su tenir compte de ces évolutions tant dans les modalités de commission d'infractions que dans les incriminations elles-mêmes. En effet, le législateur a, dès 1988, créé des infractions pénales spécifiques aux atteintes aux systèmes de traitement automatisé de données. De même, la loi de programmation pour la justice 2018-2022 témoigne de l'intérêt porté par le législateur aux preuves électroniques en matière pénale.

La preuve électronique peut être définie comme toute donnée numérique utilisée dans le cadre d'une enquête et dans la poursuite des auteurs d'infractions pénales. Ces données numériques permettent de fournir des informations sur la personne poursuivie, mais également sur ses activités. A titre d'illustration, le téléphone portable d'une personne contient de nombreuses données numériques. D'une part, la ligne téléphonique peut être rattachée à un abonnement téléphonique et donc à son titulaire. D'autre part, le téléphone émet des données de géolocalisation, permet d'échanger des appels et des messages électroniques, ainsi que de stocker des contenus écrits et audiovisuels. L'ensemble de ces données permet d'avoir des informations sur le titulaire de la ligne téléphonique, ainsi que sur les activités de ce dernier.

Si les données numériques sont extrêmement précieuses dans le cadre des enquêtes pénales, étant même souvent devenues incontournables en matière probatoire, celles-ci posent néanmoins une difficulté de taille. Les données électroniques sont fréquemment stockées dans des serveurs situés en dehors du territoire de l'Etat dans lequel ont lieu les investigations, voire en dehors de l'Union européenne. L'accès transfrontière à ces données numériques peut donc se révéler être un véritable parcours du combattant pour les services d'enquête, qui se trouvent confrontés à des procédures longues et fastidieuses, variant selon les pays concernés. Ces difficultés ne sont pas anecdotiques, dans la mesure où près de la moitié des enquêtes pénales comportent une demande d'accès transfrontière.

La réglementation « *e-evidence* » s'inscrit donc dans cet esprit, visant à faciliter et fluidifier l'accès aux preuves électroniques au niveau européen, par l'établissement d'un cadre juridique stable et uniforme.

LA NÉCESSITÉ DE REPENSER L'ACCÈS AUX PREUVES NUMÉRIQUES DANS LES AFFAIRES PÉNALES

Une première prise de conscience quant à l'importance de la preuve électronique dans les affaires criminelles les plus graves a vu le jour à la suite des attentats de Bruxelles, en mars 2016. Le Conseil européen, dans ses conclusions sur l'amélioration de la justice pénale dans le cyberespace du 9 juin 2016, a souligné la nécessité d'accélérer et de rendre plus efficaces les moyens permettant d'obtenir des preuves numériques. Un an plus tard, le Conseil rappelait que l'accès à de telles preuves est un élément déterminant dans la lutte contre le terrorisme et les formes graves de criminalité, et appelait à une nouvelle proposition législative afin de doter l'Union européenne d'une « cybersécurité solide ».

Le Conseil appelait alors la Commission européenne à présenter début 2018 une proposition législative destinée à améliorer l'accès transfrontières aux preuves électroniques. Il lui enjoignait également de lui présenter, avant la fin de l'année 2017, un rapport sur l'avancée des travaux entrepris en la matière.

Parallèlement, les Etats-Unis adoptaient, le 22 mars 2018, le « *Cloud Act* »[1]. Ce dispositif permet aux autorités américaines de requérir des fournisseurs de services ou aux hébergeurs les données numériques qu'ils détiennent, même si celles-ci sont stockées à l'étranger, afin de les utiliser dans le cadre d'une procédure pénale. Le *Cloud Act* laisse également la porte ouverte à la conclusion d'accords avec des Etats étrangers, dans un objectif de réciprocité et de simplification des procédures.

Le 4 juin 2018, le Conseil se déclarait ouvert à une approche commune au niveau de l'Union européenne et encourageait en ce sens la Commission à maintenir le contact avec les autorités américaines pour parvenir à un accord bilatéral.

LA RÉGLEMENTATION *E-EVIDENCE*

C'est dans ce contexte que s'inscrit la réglementation *e-evidence*. L'objectif affiché de cette réglementation est de permettre d'accélérer l'accès aux preuves numériques stockées dans un autre Etat membre de l'Union européenne. Ce dispositif devrait permettre aux autorités judiciaires d'un Etat membre de demander un accès direct dans le cadre d'une procédure pénale aux données électroniques détenues par un fournisseur de services ou un hébergeur établi dans un autre Etat membre. Cette nouvelle réglementation s'appuie donc sur le principe du droit de l'Union de reconnaissance mutuelle entre Etats membres.

La réglementation *e-evidence* ne concerne pas l'interception de données en temps réel. En effet, la lettre du texte vise exclusivement « les données stockées ». Ainsi, seules les données figurant dans une base de données au jour de la demande sont concernées par ce dispositif.

Cette réglementation *e-evidence* est une étape importante dans l'accès aux preuves électroniques, car celui-ci rencontre à l'heure actuelle trois principaux écueils. Tout d'abord, la coopération entre les services privés détenant les données numériques et les autorités publiques exerçant des poursuites s'avère relativement inefficace. Ensuite, les procédures pour accéder à ces données sont particulièrement lentes et fastidieuses. Enfin, l'absence de cadre juridique précis et uniforme rend ces procédures floues et hasardeuses.

En l'état actuel, lorsque les services d'enquête d'un Etat membre procèdent à des investigations, ceux-ci peuvent être amenés à demander l'obtention de données numériques. Or, si ces données sont stockées dans un serveur situé à l'étranger, les enquêteurs devront adresser une demande au fournisseur de services ou à l'hébergeur qui les détient. Ce dernier examine la demande au regard du droit en vigueur dans son pays. Ce n'est qu'ensuite que le fournisseur de services ou l'hébergeur décidera de transmettre ou non les données qui lui ont été demandées par les services d'enquête de l'Etat membre. Ainsi, l'obtention des données numériques dépend totalement de la législation applicable dans chaque Etat. En matière de lutte contre le terrorisme, la procédure est encore plus compliquée, celle-ci étant entourée de davantage de garanties imposées aux autorités judiciaires impliquées.

La réglementation *e-evidence* permet de poser des règles claires et harmonisées à destination des fournisseurs de services et des hébergeurs de données numériques. Ce

1. Clarifying Lawful Overseas Use of Data Act, dit « *Cloud Act* » (22 mars 2018).

nouveau cadre juridique doit ainsi permettre une rapidité accrue dans la lutte contre les formes graves de criminalité. Cette réglementation se veut, en outre, respectueuse des droits fondamentaux, et prévoit en ce sens de nombreuses garanties. Ainsi, les demandes d'accès aux données stockées à l'étranger devront nécessairement faire l'objet d'une autorisation de la part de l'autorité judiciaire, et se limiter aux crimes les plus graves. Les règles de procédure pénale trouveront ici à s'appliquer en toutes circonstances, et l'individu concerné recevra la notification de ses droits ainsi que des données ayant été réclamées par les services d'enquête.

Avec la nouvelle réglementation *e-evidence*, la procédure pour obtenir des preuves numériques sera considérablement simplifiée et raccourcie. En effet, l'autorité de poursuite d'un Etat membre formulera une demande d'accès à des données transfrontières, qui devra être approuvée par un juge. Cette demande sera ensuite transmise au fournisseur de services ou à l'hébergeur situé dans un autre Etat membre, lequel sera tenu d'envoyer les données numériques directement à l'autorité de poursuite de l'Etat membre demandeur. Si le fournisseur de services ou l'hébergeur ne respecte pas la demande, alors il reviendra aux autorités judiciaires de l'Etat membre requis de le contraindre à transmettre les données numériques demandées.

La réglementation *e-evidence* se décompose en deux volets, avec, d'une part, un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, et, d'autre part, une directive visant à une harmonisation des règles relatives à la désignation des représentants légaux aux fins de la collecte de preuves en matière pénale.

Le règlement *e-evidence*, qui s'appliquera directement dans tous les Etats membres, prévoit deux types d'injonctions complémentaires. D'une part, une injonction de production, qui permet aux autorités judiciaires d'un Etat membre de demander un accès direct aux données électroniques pouvant servir de preuves et détenues par un fournisseur de services ou un hébergeur dans un autre Etat membre. Les détenteurs des données numériques seront tenus de répondre à cette demande sous un délai de 10 jours, lequel pourra être réduit à 6 heures en cas d'urgence. D'autre part, le règlement prévoit une injonction de conservation destinée à empêcher la suppression des données électroniques servant de preuve par le fournisseur ou l'hébergeur durant la période couvrant l'injonction de production.

La directive *e-evidence*, qui nécessitera une transposition en droit interne, tend à harmoniser les règles relatives à la collecte des preuves électroniques en matière pénale dans les différents Etats membres, en obligeant tous les fournisseurs de services ou hébergeurs à désigner un représentant légal au sein de l'Union européenne. Ce représentant sera tenu de réceptionner et de veiller au respect des injonctions prévues par le règlement *e-evidence* et des décisions judiciaires. Cette directive doit donc permettre d'harmoniser les obligations pesant sur les fournisseurs de services et hébergeurs en matière de preuve numérique en fournissant un cadre juridique clair et uniforme.

LA CONCILIATION AVEC LES AUTRES NORMES APPLICABLES EN MATIÈRE DE DONNÉES NUMÉRIQUES

Une autre vertu de la réglementation *e-evidence* serait de poser les bases d'une législation globale en matière de preuves numériques dans les procédures pénales.

A l'heure actuelle, le recueil des preuves numériques se fait en suivant la voie de traités d'entraides judiciaires bilatéraux en matière pénale, tel que celui conclu entre la France et les Etats-Unis. Le recueil des preuves numériques passe, notamment, par le biais de commissions rogatoires internationales. Or, certains droits nationaux ainsi que certaines règles européennes peuvent venir faire échec aux dispositions du *Cloud Act* américain.

La loi de blocage française du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commerciale ou technique à des personnes physiques ou morales étrangères semble ainsi pouvoir faire obstacle aux dispositions du *Cloud Act* américain. Si cela semble se vérifier sur son volet civil, notamment face à la procédure Discovery, cela semble moins certain sur son volet pénal, dès lors que les données réclamées sont utiles à la manifestation de la vérité.

En revanche, la directive (UE) 2016/943 sur le secret des affaires, et plus encore le règlement (UE) 2016/679, dit « règlement général sur la protection des données, semblent être des obstacles sérieux à l'application des

dispositions du *Cloud Act* pour les données stockées dans l'Union européenne. Ces règles européennes n'autorisent la divulgation de certaines données que sous réserve de l'existence d'un accord international, mais l'invocation du seul fondement du *Cloud Act* parait ici insuffisante.

La règlementation *e-evidence* pourrait devenir le nouveau cadre juridique européen en matière d'accès aux preuves numériques. S'inscrivant dans la lignée du dispositif américain, la proposition de règlementation européenne poursuit le même objectif et repose sur des mécanismes similaires.

Afin d'aboutir à une harmonisation globale des règles en la matière et d'éviter les situations de conflits d'obligations entre la réglementation *e-evidence* et le *Cloud Act*, il parait nécessaire que soit conclu, dans un premier temps, un accord entre l'Union européenne et les Etats-Unis sur l'accès aux preuves numériques. Pour l'heure, un tel accord n'a pas encore vu le jour. Toutefois, les instances européennes appellent à poursuivre les négociations avec les Etats-Unis pour parvenir à la signature d'un accord bilatéral avec l'Union européenne.

Il convient néanmoins de souligner que le projet de réglementation *e-evidence* dépasse amplement un simple accord bilatéral. Si cette législation européenne parvenait à se combiner avec le dispositif américain, un système mondial et homogène de collecte des données à titre de preuves dans les affaires pénales les plus graves pourrait voir le jour. Cela simplifierait considérablement le travail des services d'enquêtes, dès lors que ces données numériques peuvent être stockées n'importe où dans le monde.

En conclusion, le projet de réglementation *e-evidence* démontre que l'Union européenne s'investit pleinement dans la question de l'accès aux données numériques. Les premières bases vers une réflexion globale en la matière semblent ainsi posées.

L'IMPACT DE LA RÉGLEMENTATION *E-EVIDENCE* SUR LA PROFESSION D'AVOCAT

Cette nouvelle réglementation n'évoque pas le rôle que devra jouer l'avocat dans ces procédures, ni même s'il sera averti avant que les demandes ne soient formulées (et donc s'il pourra s'y opposer). Il est toutefois certain que les avocats devront vérifier que les garanties légales dont bénéficient leurs clients ont bien été respectées au cours de la procédure.