L'affaire « Microsoft » : la localisation des données et l'extraterritorialité en question

Le 14 juillet 2016, la cour d'appel fédérale de Manhattan aux Etats-Unis a décidé qu'un mandat de perquisition ne permettait pas aux autorités américaines d'obtenir des données stockées par Microsoft en Irlande, car un tel mandat ne peut avoir d'effets en dehors des frontières des Etats-Unis. Quel impact en Europe ?

Par Winston Maxwell, avocat associé, Hogan Lovells

L'arrêt « Microsoft » a le mérite de préciser l'étendue territoriale des pouvoirs de police aux Etats-Unis et de relancer le débat sur la localisation des données.

Cette affaire commence en décembre 2013 lorsqu'un magistrat ordonne à la firme de Redmond de livrer aux services du procureur de l'Etat de New York le contenu de courriers électroniques appartenant à une personne suspectée de trafic de drogues.

Perquisitions et frontières

Microsoft a livré les métadonnées concernant le compte e-mail du suspect, mais a refusé de livrer le contenu des e-mails, car celui-ci était hébergé en Irlande. Selon Microsoft, les effets de l'ordonnance du magistrat s'arrêtaient aux frontières des Etats-Unis. En première instance, le magistrat a sanctionné Microsoft en 2014 pour avoir désobéi à son ordonnance. Après une procédure d'appel médiatisée et impliquant de nombreuses interventions volontaires, la cour d'appel fédérale a donné raison à Microsoft.

La loi américaine permet à la police d'accéder au contenu d'e-mails uniquement après la délivrance par un juge d'un « mandat de perquisition » *(warrant)*. Il s'agit du même outil juridique que celui utilisé pour la fouille d'une maison, par exemple. Selon Microsoft, un mandat de perquisition émis par un juge américain ne pouvait pas produire d'effets en dehors des Etats-Unis. Le gouvernement américain soutenait, au contraire, qu'aucune fouille n'était nécessaire en dehors des Etats-Unis puisque Microsoft pouvait – à partir de son siège à Redmond (Etat de Washington) – récupérer les données irlandaises par un simple manœuvre technique. Pour le gouvernement américain, la localisation des données n'était pas importante dès lors que le fournisseur de service était situé aux Etats-Unis, et il pouvait donc accéder à ces données.

La position du gouvernement américain converge avec l'article 57-1 du Code de procédure pénale en France, lequel permet à la police, sous certaines conditions, d'accéder à des données hébergées à l'étranger si un accès à ces données est autorisé en France.

La cour d'appel américaine n'a pas voulu rentrer dans la logique du gouvernement des Etats-Unis. La cour s'est focalisée avant tout sur l'intention du législateur américain. Selon l'arrêt du 16 juillet, une portée extraterritoriale ne peut découler implicitement d'une loi : il faut que la loi prévoie cette portée extraterritoriale explicitement. C'est le cas de certaines lois américaines qui visent de manière explicite des actes commis à l'étranger (actes de terrorisme, ou tourisme sexuel impliquant des mineurs, etc.). Cependant, si la loi ne dit rien sur l'extraterritorialité, la loi doit être lue comme étant limitée au territoire national. Selon la cour d'appel, seul le législateur est habilité à gérer les questions délicates d'extraterritorialité et des relations internationales. L'extraterritorialité doit être explicite. La loi américaine sur la protection des communications électroniques est silencieuse sur la question territoriale. Pour la cour fédérale, la loi ne peut donc produire d'effets au-delà de la frontière des Etats-Unis. Par conséquent, le gouvernement ne peut pas utiliser un mandat de perquisition pour forcer Microsoft à livrer des données hébergées en Irlande (1).

Le débat n'est pas clos pour autant, car le gouvernement américain pourrait porter cette affaire devant la Cour Suprême.

Plusieurs enseignements

La décision nous livre plusieurs enseignements. Le premier est qu'en matière d'enquêtes judiciaires, la loi américaine fournit autant de protections aux individus que la loi française. L'intervention d'un juge est nécessaire, comme pour la fouille d'un domicile. En matière de protection des données à caractère personnel, la loi américaine sur les enquêtes criminelles ne peut guère être considérée comme étant « inadéquate », car elle fournit autant de garanties que la loi française.

Certes, les services de renseignement américains ne sont pas tenus, eux, d'obtenir un mandat avant de collecter des données, y compris hors des Etats-Unis. Ce point est reproché aux Etats-Unis dans le contexte du nouveau « Privacy Shield » (2). Cependant, aucun pays européen n'impose une telle exigence à ses agences du renseignement. En France, par exemple,

Notes

(1) - Brad Smith, directeur juridique de Microsoft, s'est félicité le 14 juillet 2016 de cette décision *« importante pour trois raisons : elle garantit que les droits à la vie privée des gens sont protégés par les lois de leur propre pays ; elle aide à garantir que les protections légales du monde physique s'appliquent dans le secteur numérique ; et elle prépare la voie pour de meilleures solutions afin de répondre à la fois aux besoins de la protection de la vie privée et de la police ».*

(2) - Le Privacy Shield a remplacé le Safe Harbor invalidé en 2015 par la Cour de justice de l'Union européenne (CJUE). Lire *EM@145, p. 8 et 9.*

les agences du renseignement peuvent collecter des données concernant des communications internationales avec la seule autorisation du Premier ministre. L'erreur serait de comparer l'encadrement des activités de renseignement aux Etats-Unis avec l'encadrement des enquêtes judiciaires en France. Les deux ne sont pas comparables. Seule une comparaison « renseignement-renseignement » serait pertinent.

L'extraterritorialité ne se présume pas

Le deuxième enseignement de l'affaire Microsoft concerne localisation des données. Est-ce que la localisation physique des données compte ? En juillet, la Russie a adopté une loi qui étend considérablement l'obligation de stocker des données sur le territoire russe. Un amendement au projet de loi « République numérique » adopté au Sénat aurait créé une obligation de stocker des données sur le territoire français. Cet amendement n'a pas été repris dans la version du texte adoptée en juillet 2016 (3). Certaines lois chinoises prévoient l'obligation de stocker des données sur le territoire chinois. Face aux risques de la mondialisation, certains Etats voient dans la localisation des données un moyen de réaffirmer leur souveraineté. La décision Microsoft semble confirmer que la localisation physique des données peut avoir un impact sur les pouvoirs des autorités nationales.

Mais ce n'est pas si simple. Une loi nationale peut prévoir la possibilité pour les autorités d'accéder à des données hors de son territoire s'il existe un accès dans le territoire (en France, article 57-1 Code de la procédure pénale), voire la possibilité d'intercepter des données à l'étranger (article L854-1 du Code de la Sécurité intérieure). La leçon de l'affaire Microsoft est que la loi doit être précise sur ce point, car l'extraterritorialité ne se présume pas.

Sur la question de la localisation des données, le nouveau règlement européen du 27 avril 2016 sur la protection des données à caractère personnel (4) est ambivalent, voire contradictoire. D'un côté, la localisation des données n'est pas importante, car tout traitement effectué dans le cadre des activités d'un établissement en Europe – ou lié à l'offre de services en Europe – est couvert par ce règlement, même si les données sont stockées en dehors de l'Europe. Le règlement précise d'ailleurs que le lieu du traitement est sans importance. De l'autre côté, le règlement impose des contraintes particulières pour tout transfert de données en dehors de l'Union européenne, ce qui du coup donne une importance à la localisation. Les prestataires de *cloud* expliqueront que les données sont stockées partout, et que cette architecture contribue à la sécurité, à la fiabilité, et au faible coût du service.

Mais après l'affaire « Snowden » (5), les fournisseurs de *cloud* mettent en avant des solutions de stockage 100 % européen, voire 100 % français. Les lois russes et chinoises vont dans le sens d'une localisation forcée des données sur le territoire, sans parler de lois turques ou iraniennes (6). Dans le cadre de ses travaux sur le marché numérique unique, la Commission européenne dresse un inventaire sur les cas de « localisation forcée » des données (7), et souligne la nécessité de permettre la libre circulation des données afin de favoriser l'innovation, la croissance, et la liberté d'expression. Le débat sur la localisation des données s'accompagne d'un débat sur le chiffrement, car une donnée stockée localement n'est guère utile si elle ne peut être déchiffrée. La loi française oblige les fournisseurs de moyens de cryptologie à décrypter des messages, sauf si les prestataires *« démontrent qu'ils ne sont pas en mesure de satisfaire à des réquisitions »* (article L871-1 du Code de la Sécurité intérieure). Au moment où les gouvernements français et allemand plaident pour des pouvoirs accrus en matière de déchiffrement (8), la présidente de la Commission nationale de l'informatique et des libertés (Cnil) rappelle, dans une tribune qu'elle a cosignée (9), l'importance du chiffrement dans la protection des données à caractère personnel. @

Notes

(3) - L'Assemblée nationale a définitivement adopté le 20 juillet 2016 le projet de loi *« République numérique »*. Pour être adopté par le Parlement, le projet, doit encore faire l'objet d'une lecture définitive au Sénat, programmée le 27 septembre 2016.

(4) - Règlement européen n°2016/679 du 27 avril 2016 sur la protection des données : lire Christiane Féral-Schuhl, *EM@l46, p. 8 et 9.*

(5) - Affaire « Snowden », du nom de l'ancien collaborateur informatique de la CIA et de la NSA qui a révélé mi-2013 l'espionnage mondial pratiqué illégalement par les États-Unis.

(6) - Question : https://lc.cx/Q-localisation

(7) - Enquête : https://lc.cx/LE-localisation

(8) - https://lc.cx/FR-ALL-CQ

(9) - https://lc.cx/IF-P22-08-16

Zoom

Microsoft résiste encore et toujours à Washington

La firme de Redmond, dans l'Etat de Washington, a décidément maille à partir avec l'administration de Washington. En effet, en avril 2016, Microsoft a porté plainte – devant un tribunal fédéral de Seattle – contre le gouvernement américain en l'accusant de violer la Constitution des Etats-Unis en empêchant le géant américain de l'informatique et du Net d'informer ses milliers de clients des requêtes *« secrètes »* de l'administration américaine – sous couvert de l'Electronic Communications Privacy Act (ECPA) – pour avoir accès à leurs e-mails et données personnelles.

Cette affaire rappelle celle de l'iPhone qu'Apple avait refusé de débloquer à la demande la police fédérale (FBI) – finalement abandonnée – à la suite de la tuerie de San Bernardino en décembre 2015. @