USA v. MICROSOFT : QUEL IMPACT?

STATUT DES DONNÉES, SOUVERAINETÉ NUMÉRIQUE ET PREUVES DANS LES NUAGES

AVEC UNE ÉTUDE DE THÉODORE CHRISTAKIS,
PROFESSEUR DE DROIT INTERNATIONAL À L'UNIVERSITÉ GRENOBLE ALPES, MEMBRE SENIOR DE L'INSTITUT UNIVERSITAIRE DE FRANCE, DIRECTEUR ADJOINT DE GRENOBLE ALPES DATA INSTITUTE

DÉCEMBRE 2017

ceis

THE CHERTOFF GROUP

AVANT PROPOS

Le feuilleton judiciaire qui oppose depuis 2013 Microsoft au Gouvernement américain à propos de la validité d'un mandat d'un juge américain sur des données de contenus hébergées par Microsoft en Irlande va bientôt connaître son dénouement. Saisie par le Département de la justice (DoJ) américain, la Cour suprême a décidé en octobre 2017 d'examiner l'affaire et se donne jusqu'à juin prochain pour prendre une décision. Au cœur du débat : un juge américain peut-il, sans passer par les dispositifs prévus en matière d'entraide judiciaire internationale, réquisitionner directement après d'un hébergeur des données situées sur un serveur à l'étranger ?

Si la question posée est simple, les enjeux sont multiples, chacune des parties prenantes cherchant à faire valoir ses propres intérêts. Pour les Etats, il s'agit tout d'abord d'assurer leur sécurité en ménageant aux autorités judiciaires un accès aux données numériques, où qu'elles se situent dans le monde. Et en la matière, force est de constater que les dispositifs actuels, basés sur les MLAT, ou traité d'assistance judiciaire mutuelle, ne permettent pas de répondre à la croissance exponentielle des demandes d'entraide internationale portant sur des données numériques et au besoin de réactivité qu'exige le cyberespace. Pour les entreprises, qu'elles soient utilisatrices ou opérateurs de cloud, il s'agit ensuite de disposer d'une « énergie informatique » performante et au meilleur prix pour assurer la transformation numérique, ce qui implique de « massifier » les activités autour de quelques gros datacenters et d'éviter les conflits de lois et de juridiction. A l'intersection des deux, il s'agit enfin de préserver et même de renforcer, la confiance des citoyens-utilisateurs, essentielle au développement des nouveaux usages, quant à la protection de leurs données personnelles.

La décision de la Cour Suprême américaine sera donc lourde de sens. Si elle donne raison au Département de la justice, elle consacrera *ipso facto* une sorte de compétence mondiale du juge américain qui sera alors fondé, dans le cadre d'une procédure nationale, à demander des données de contenu (et non simplement des données de connexion) à n'importe quel opérateur à la surface du globe. Et cela, sans même prétendre qu'il y a extraterritorialité de la loi, puisque le DoJ considère que les données relèvent du droit américain dès lors qu'elles sont consultables depuis le territoire américain… Un tour de passe-passe qui territorialise potentiellement aux Etats-Unis une bonne partie des données mondiales, les données mises dans le « nuage » étant par définition accessibles depuis n'importe quel endroit à la surface du globe.

Il en résulterait des atteintes répétées à la souveraineté des Etats cibles, une incompatibilité avec les accords et législations européennes protégeant les données personnelles (surtout le Règlement européen sur la protection des données personnelles…) et une insécurité juridique permanente pour les opérateurs numériques contraints à un grand écart impossible. Par ailleurs, d'autres Etats pourraient eux aussi avoir, en réaction, la tentation de l'unilatéralisme et ne plus utiliser les instruments de droit international existants. Avec pour conséquence une multiplication des conflits de souveraineté et une exacerbation des protectionnismes numériques dont personne ne sortirait gagnant. La simple observation des flux de données entre l'Europe et les Etats-Unis montre en effet combien l'Europe est dépendante de la relation transatlantique en matière numérique. C'est une réalité à la fois technologique et économique. Il ne s'agit pas pour autant de crier au loup et d'invoquer systématiquement le spectre de la balkanisation d'internet à chaque fois que des Etats « localisent » ou « relocalisent » certains types de données, que cela soit au bénéfice d'acteurs numériques locaux ou de filiales locales d'entreprises américaines. Cette tendance, déjà largement amorcée, s'inscrit dans une quête de souveraineté parfaitement légitime, *a fortiori* dans un contexte post-Snowden…

Quelques mois avant la décision de la Cour suprême, il nous paraissait donc indispensable de cerner les tenants et aboutissants de cette affaire. Et d'imaginer les solutions permettant de concilier les intérêts des Etats, des entreprises et des individus. C'est tout l'objet de ce livre blanc initié par Microsoft et co-écrit par The Chertoff Group et Théodore Christakis, professeur de droit international et membre senior de l'Institut Universitaire de France.

Guillaume Tissier
Directeur général de CEIS

Ce livre blanc, rédigé par The Chertoff Group, en concertation avec CEIS, souligne notre préoccupation quant au décalage croissant entre les démarches américaine et européenne relatives à l'échange transfrontalier de données à des fins répressives et anti-terroristes, ainsi que les problématiques inhérentes à la protection et à la sécurité des données. Nous tirons la sonnette d'alarme depuis un certain temps déjà quant aux potentielles conséquences néfastes de l'actuelle balkanisation d'Internet[1]. Nous espérons encore améliorer la coopération entre les USA et l'Europe via une compréhension accrue des risques potentiels liés à la direction actuelle de nos politiques.

A cet effet, ce livre blanc souhaite mettre en évidence, pour nos homologues européens, un potentiel point d'inflexion qui se profile : un appel en instance devant la Cour suprême des Etats-Unis. Le dénouement de cette affaire pourrait accélérer la détérioration de la coopération transfrontalière de manière significative. Cependant, nous estimons que cette affaire n'a ni reçu l'attention qu'elle mérite en Europe, ni provoqué la mobilisation attendue. Nous maintenons respectueusement que ce manque d'attention n'est pas dans l'intérêt de l'Europe et des Etats-Unis. Ce livre blanc résume cette affaire, explique pourquoi sa résolution est importante et suggère un moyen de renforcer la mobilisation de l'Europe.

The Chertoff Group

TABLE DES MATIÈRES

MICROSOFT CONTRE LES ETATS-UNIS : UN POINT D'INFLEXION DÉCISIF

par The Chertoff Group

A son retour de la pause estivale à la mi-octobre, la Cour suprême des Etats-Unis a accepté de se saisir d'une affaire qui pourrait avoir un impact direct sur le pays : Microsoft contre les Etats-Unis[2]. L'affaire sera plaidée au début de l'année prochaine et un verdict final sera rendu avant que la Cour ne prenne sa pause estivale fin juin 2018.

D'une manière générale, l'affaire concerne un mandat délivré par le gouvernement américain à Microsoft qui, s'il était appliqué, obligerait Microsoft à rapatrier vers l'Amérique des données de contenu, détenues dans un centre de données irlandais, dans le but de les communiquer aux autorités judiciaires. Il s'agit d'une simple question juridique : les autorités policières américaines peuvent-elles obliger Microsoft à fournir aux États-Unis des données détenues dans un centre de données à l'étranger ? Plus prosaïquement : la loi américaine contrôle-t-elle les données stockées en Europe ?

La réponse à cette question est ou devrait être d'une importance capitale pour les Européens. Le partage des données entre les États-Unis et l'Union européenne est essentiel, tant pour les autorités que pour le secteur privé, tant pour les enquêtes policières que pour tous les types d'échanges. Et de par la nature même du « cloud », le stockage et le transfert de données constituent désormais un problème mondial : les frontières physiques ne sont pas déterminantes.

La mondialisation d'Internet a eu un impact particulièrement profond sur le maintien de l'ordre public. Les enquêtes sur les crimes locaux, qui étaient autrefois limitées à la zone géographique où l'infraction avait été commise, se transforment en enquêtes où la collecte de preuves implique parfois des données qui peuvent être stockées presque partout dans le monde. Le contenu des communications relatives à une infraction, ainsi que les métadonnées associées à ce contenu, peuvent être stockés à

plusieurs endroits et, dans certains cas, être transférés d'un datacenter à un autre pour différentes raisons, tant techniques que pratiques. Les données n'étant plus localisées, les forces de police et autorités judiciaires doivent souvent, *de facto*, franchir les frontières nationales pour enquêter, même sur des cas très courants.

Aux États-Unis et en Europe, ces efforts transfrontaliers de maintien de l'ordre public reposent souvent sur des lois et des politiques désuètes. Les traités d'assistance juridique mutuelle (« MLAT ») en matière de coopération pénale transnationale proposent des solutions fastidieuses et qui ne garantissent pas la sécurité juridique. Les demandes présentées dans le cadre du processus MLAT prennent souvent des mois, et parfois des années à aboutir, ce qui en fait une source de frustration pour les autorités policières des deux côtés de l'Atlantique[3]. C'est la raison pour laquelle les autorités judiciaires américaines, voulant traiter rapidement et efficacement les dossiers, se tournent systématiquement vers une démarche beaucoup plus rapide : les émissions de mandats nationaux. Mais n'oublions pas le revers de la médaille : cette démarche implique que les entreprises américaines confèrent un effet extraterritorial et international aux demandes de la justice américaine. Une pratique qui soulève la question fondamentale de la souveraineté et conduit à des conflits de lois et à des atteintes aux règles de courtoisie internationale.

Cette question juridique précise est maintenant abordée devant la Cour suprême des États-Unis, qui examinera la validité d'un mandat national délivré à Microsoft. Une décision confirmant que le gouvernement peut légalement émettre une telle demande forcerait les États-Unis à affirmer que leurs demandes de production de preuves peuvent avoir un effet extraterritorial. Cela aura à son tour un impact significatif sur la coopération américano-européenne.

"Solutions" unilatérales et conséquences

À une époque où la cybercriminalité et l'ingérence électorale s'intensifient, la coopération transatlantique en matière de lutte contre la cybercriminalité et les attaques cybernétiques est plus importante que jamais. Or, sans une action législative plus large ou un accord international, une décision en faveur du gouvernement dans l'affaire Microsoft aura probablement pour effet pervers de rendre la coopération transatlantique plus difficile pour les autorités en charge du maintien de l'ordre public, les gouvernements et les entreprises. L'application extraterritoriale de la loi aura, à notre avis, une incidence négative sur les efforts de coopération entre les États-Unis et d'autres pays ainsi que sur leur souveraineté.

Pour comprendre pourquoi cette perspective est à ce point dérangeante et déstabilisante, il est utile de se livrer à un exercice de prospective : à quoi ressemblera le partage des données en matière de maintien de l'ordre public si le point de vue du gouvernement américain sur l'extraterritorialité l'emporte ? Le tableau ne sera guère réjouissant et nous pouvons déjà en voir les contours se dessiner dans l'action de différentes nations. En examinant les impacts potentiels, nous voyons en effet plusieurs domaines dans lesquels la coopération internationale entre les États-Unis et l'Europe en pâtira certainement.

Ces impacts sont susceptibles d'inclure :

1) l'application extraterritoriale réciproque d'autres droits nationaux, ce qui permettra à ces pays de bénéficier d'un droit d'accès aux données hébergées sur des serveurs relevant de la juridiction américaine, créant des obligations juridiques contradictoires et incompatibles pour les fournisseurs.

2) l'élargissement, et ce qui pourrait être décrit comme un renforcement, des exigences de localisation des données dans les pays non américains, visant à empêcher le gouvernement américain d'accéder aux données relatives à leurs citoyens.

3) et peut-être ce qui est le plus troublant, de possibles ajustements au « *Privacy Shield* » ou même l'élimination des mécanismes qui permettent aux entreprises de transférer des données de l'autre côté de l'Atlantique.

Aucune de ces perspectives n'est encourageante.

Obligations juridiques contradictoires et incompatibles

L'un des principaux problèmes posés par la position du gouvernement américain dans l'affaire Microsoft - si d'autres pays suivent la même voie - est tout d'abord qu'il transforme un environnement de coopération en matière de maintien de l'ordre public en un environnement où la concurrence prédomine. Si la Cour soutient la position des Etats-Unis quant à l'application extraterritoriale de leur loi afin d'assurer l'accès aux données, nous sommes convaincus que d'autres pays feront rapidement de même. Cette tendance est d'ailleurs déjà patente.

Le Brésil a par exemple récemment arrêté le cadre local d'une entreprise technologique américaine parce qu'il refusait de fournir des données stockées aux États-Unis. Le Brésil avait émis une réquisition locale qui allait apparemment à l'encontre d'une interdiction américaine[4]. De même, au Royaume-Uni, le gouvernement a adopté le Data Retention and Investigatory Powers Act qui, selon ses propres termes, est censé avoir une application extraterritoriale[5]. Et même en Europe, la tendance progresse. La Cour suprême belge a ainsi récemment condamné Yahoo à payer une amende pour ne pas avoir respecté une décision de justice en dehors de la Belgique[6]. L'objectif, comme nous l'avons dit, est compréhensible : le processus actuel des MLAT n'est pas adapté. Mais comprendre la motivation n'implique pas nécessairement d'approuver le résultat.

Si le verdict rendu sur cette affaire est défavorable à Microsoft, la situation va nécessairement empirer, et non s'améliorer. Sur le fond, en consacrant un unilatéralisme triomphant dans le droit américain, la Cour suprême décourage la coopération internationale en faveur d'une action indépendante. Quelle motivation auront les États-Unis pour sensibiliser la communauté internationale au besoin de faciliter l'accès des services de maintien de l'ordre aux données si ces derniers parvenaient à obtenir, de la part de la Justice américaine, l'accès aux données dont ils ont besoin ? Face à une telle décision, nous ne doutons pas que les pays européens répondront aux États-Unis en appliquant leurs propres lois extraterritoriales aux entreprises et aux citoyens européens. En effet, si l'unilatéralisme devient la norme, les autorités nationales n'auront pratiquement aucune raison d'agir dans le respect réciproque des intérêts de l'autre.

Au bout du compte, cette tendance entrainera la prolifération des problèmes de conflits de lois et créera des obligations juridiques contradictoires et incohérentes pour les fournisseurs. Et surtout, cette approche empiétera sur une valeur fondamentale qu'est la souveraineté, mise à mal par les efforts menés, à l'étranger, par les pays qui tenteront d'obtenir des données. Quelle loi s'appliquera, et dans quel cas, si chaque pays est en mesure d'appliquer de façon extraterritoriale sa propre loi ? Comment les gouvernements et les tribunaux règleront-ils ces conflits de lois ? Dans quel pays la loi devra-elle être appliquée ? Dans un tel

environnement, la distinction entre le droit international et le droit national perdra tout son sens et il en résultera une liberté de choix juridique où le seul facteur déterminant sera l'exercice de la puissance brute qui peut être utilisée pour imposer un résultat spécifique[7].

Encore une fois, et bien qu'il soit facile d'imaginer la façon dont cela se produira et pourquoi cela peut sembler justifié aux yeux des acteurs étatiques, à la question « qu'est ce qui est le mieux pour la communauté mondiale », ceci ne peut pas être la bonne réponse. La primauté du droit repose sur un Etat de droit - un domaine basé sur une relative certitude et cohérence. Le règlement de conflits de lois totalement indéterminés ébranle cette valeur fondamentale. Cela aura également pour effet secondaire de saper la coopération entre les services de maintien de l'ordre public américains et européens, ce qui les amènera à rechercher des données par l'intermédiaire de leurs propres tribunaux, plutôt que de travailler ensemble.

Une localisation plus restrictive des données

Deuxièmement, et c'est peut-être ce qui est le plus probable, nous pensons qu'une décision pro-gouvernement américain dans l'affaire Microsoft entrainerait presque certainement une localisation plus restrictive des données. Les pays européens, en particulier, sont susceptibles de poursuivre les exigences de localisation des données pour prévenir ce qu'ils perçoivent comme un préjudice pour leurs citoyens. Il s'agit également d'une impulsion compréhensible : le renforcement de la localisation des données est l'un des seuls moyens de garantir que la législation d'un pays ne s'applique qu'aux données de ses propres citoyens, en exigeant qu'elles soient détenues au niveau national par un fournisseur qui se conformera à la législation locale.

Il s'agirait d'un pas supplémentaire par rapport aux régimes existants de localisation des données, qui se limitent généralement à l'obligation de stocker physiquement les données concernant les citoyens locaux à l'intérieur des frontières d'un pays, sans tenir compte des autres territoires sur lesquels le fournisseur opère. Si la Cour suprême acceptait l'argument du gouvernement, les autorités américaines seraient en mesure d'obliger tout fournisseur de services présent aux États-Unis à fournir des données, peu importe l'endroit où celles-ci seraient stockées, ce qui invaliderait les exigences actuelles en matière de localisation des données. En réponse à cela, les pays seraient incités à établir des exigences beaucoup plus restrictives en matière de localisation des données, ce qui obligerait le fournisseur à n'opérer que dans la juridiction nationale en question. Cela empêcherait ainsi les autorités d'autres pays, comme les États-Unis, d'utiliser la présence du fournisseur dans leur pays comme un moyen de les contraindre à fournir des données en vertu d'une application extraterritoriale de leurs propres lois.

Mais ce régime de localisation de données très contraignant, bien que compréhensible, est une solution secondaire. D'une part, il s'agit effectivement d'un cyberprotectionnisme, qui privilégie les fournisseurs locaux sur les fournisseurs mondiaux, ce qui finit par nuire au consommateur national. Plus important encore, il en résulterait la création d'un Internet extrêmement balkanisé dans lequel les fournisseurs opèreraient à l'intérieur d'un seul pays et seraient obligés d'éviter les activités transfrontalières, et ce, afin d'éviter l'application extraterritoriale des lois nationales. L'Internet mondialisé deviendrait ainsi plus une idée qu'une réalité. Quelle que soit la réponse que l'on préfère, l'argument qui consiste à suggérer que les désaccords entre Etats sur des questions politiques peuvent être résolus au prix de la transformation d'Internet en un vulgaire patchwork de simili-internets locaux, uniquement conçus pour assurer le respect des législations locales, n'est pas défendable.

Modifications apportées au « Privacy Shield » et aux mécanismes de transfert de données similaires

Une victoire du Gouvernement aurait probablement des effets collatéraux. Si les autorités européennes ne pensent pas que le droit américain puisse être compatible avec le droit européen, elles seront donc plus réticentes à autoriser le transfert de données personnelles européennes vers les États-Unis. Corrolaire logique d'une tendance à la localisation des données à l'extrême, cela conduira probablement l'UE à demander des ajustements au *Privacy Shield* et aux autres mécanismes permettant le transfert des données personnelles des citoyens européens vers les USA.

En cas de victoire du gouvernement américain face à Microsoft, nous avons de bonnes raisons de penser que l'UE recevra des garanties quant à la confidentialité offerte par le *Privacy Shield*, les Binding Corporate Clauses ou d'autres mécanismes ne s'opposant pas à l'action gouvernementale, et donc de moindre valeur. De plus, une telle décision de la Cour sera probablement perçue comme une indication claire que les États-Unis n'accordent pas la même importance aux lois étrangères ou à la protection de la vie privée que les Européens. Une décision en défaveur de Microsoft peut également influencer la Cour de justice européenne, alors qu'elle poursuit son examen des défis auxquels le *Privacy Shield* fait face. *In fine*, l'annulation du *Privacy Shield* perturberait les entreprises aux États-Unis et dans l'Union européenne. Si ces mécanismes sont supprimés ou modifiés de façon importante, il serait effectivement impossible pour les entreprises de transférer des données d'un territoire à l'autre. Il est évident que cela aurait des répercussions économiques importantes, les entreprises ne pouvant plus exercer leurs activités dans les deux territoires de façon unifiée.

En résumé, la victoire du Gouvernement américain serait sans doute une victoire « à la Pyrrhus », désavantageant les États-Unis mais avec des conséquences lourdes pour l'Europe. C'est la raison pour laquelle les Européens qui s'intéressent à ces questions devraient dès maintenant envisager de renforcer leur dialogue avec leurs homologues américains, avant que cet avenir dystopien ne devienne une réalité.

Une proposition d'engagement

Plutôt que d'accepter comme inévitables ces sombres perspectives, les Américains et les Européens devraient chercher des opportunités de collaborer sur l'accès légal aux données et de construire un système qui respecte les préoccupations de souveraineté et permette un maintien de l'ordre public efficace, tout en protégeant la vie privée des citoyens. Bien qu'ambitieux, l'objectif n'est pas impossible à atteindre. Les États-Unis et l'Europe devraient être en mesure de parvenir à un consensus, par le biais de la diplomatie et d'un accord international, sur la façon dont les autorités accèdent aux données stockées à l'étranger. Nos valeurs sont fondamentalement les mêmes. En effet, l'accord entre les États-Unis et les pays européens est essentiel si nous voulons établir des normes internationales qui s'alignent sur nos valeurs : un tel accord peut aider à ouvrir la voie à d'autres pays et à former une base solide pour un consensus mondial.

La question est donc de savoir comment trouver un point d'accord, et ce d'autant plus que le verdict de l'affaire Microsoft risque de venir perturber les choses …

Dans un premier temps, les Européens devraient examiner les implications de l'affaire Microsoft et déterminer leurs intérêts de façon plus globale. Le moment est venu pour l'Europe de s'engager sur ces questions et de faire entendre sa voix dans ce débat ; après, il sera trop tard.

Il est peu probable que la Cour suprême comprenne les implications globales de sa décision si celles-ci ne sont pas portées à son attention par les autorités compétentes qui comprennent le problème. En plus d'expliquer clairement quelles seraient les conséquences négatives potentielles, les Européens devraient aussi, à notre avis, s'engager ouvertement dans un dialogue avec le gouvernement américain. Au milieu de cette effervescence juridique, la Cour devrait envisager la possibilité d'aller de l'avant pour parvenir à un consensus transatlantique sur ce que devraient être le cadre juridique et la solution à ces questions. En d'autres termes, la Cour devrait savoir :

a) que les décisions concernant la coopération transatlantique en matière de maintien de l'ordre public devraient être prises conjointement et non par un seul tribunal américain.

b) que l'espoir de trouver une solution potentielle est bien réel et qu'il ne s'agit pas d'un rêve.

Heureusement, certains points permettent d'espérer et de croire qu'une solution mutuellement acceptable est sur le point de voir le jour. Le Congrès américain continue en effet de débattre sur diverses solutions possibles. Plusieurs organisations et entreprises s'emploient à trouver des moyens de régler au moins une partie du problème.

Le Congrès américain étudie par exemple activement la proposition bipartite d'adopter l'International Communications Privacy Act, une proposition qui mettrait fin à l'unilatéralisme américain en échange d'engagements réciproques de la part de nos alliés. Le Congrès et le pouvoir exécutif envisagent également de conclure le premier accord bilatéral du genre entre les États-Unis et le Royaume-Uni[8]. Cette proposition équivaut à une reconnaissance mutuelle de l'adéquation du processus juridique de chacun, en abordant directement les conflits de loi potentiels, tout en préservant la souveraineté des deux pays. Cet accord est considéré comme un modèle potentiel pour d'autres accords bilatéraux entre les États-Unis et les pays européens[9]. Pendant ce temps, des groupes issus de la société civile aux États-Unis et dans l'UE se sont engagés dans des efforts de long terme pour structurer des normes de comportement largement acceptées, qui pourraient donner lieu à un accord en matière d'accès légal et de partage des données.

Bien qu'aucun de ces efforts n'ait encore abouti, tous sont prometteurs. Plus précisément, tous ont l'avantage de s'appuyer sur une base largement représentative qui reflète le point de vue de toutes les parties prenantes. Même si nous n'avons pas de boule de cristal pour prédire le futur, nous pouvons penser que chacun d'eux a plus de chance d'aboutir à un système mondial stable, non unilatéral, d'échange de données que l'impérialisme légal des États-Unis par le biais de la Cour suprême.

En fin de compte, le concept fondamental qui doit sous-tendre nos efforts conjoints est la confiance. L'application extraterritoriale du droit interne, les exigences en matière de localisation des données et les pratiques protectionnistes sapent la confiance. Tout comme le ferait une expression unilatérale du droit par la Cour suprême des États-Unis. Les pays doivent se garder de toute action autonome sur ces questions et s'efforcer d'instaurer cette confiance.

Un premier pas - une étape essentielle - dans ce processus consiste, pour nos collègues européens, à partager leurs points de vue sur ces questions avec leurs homologues américains. Le processus juridique américain a grand besoin d'entendre le point de vue européen sur les questions dont il est saisi dans l'affaire Microsoft. Il ne s'agit peut-être pas de persuader la Cour, mais si l'on ne s'exprime pas, il va de soi que nous ne serons pas entendus.

Conclusion

Si la Cour suprême conclut que les mandats américains peuvent avoir des effets extraterritoriaux, cette décision aura un impact majeur sur la coopération entre les États-Unis et l'Union européenne sur les questions de coopération entre les services en charge du maintien de l'ordre public et de la lutte contre le terrorisme. Une conséquence presque inéluctable sera la recherche de solutions unilatérales pour répondre à certains aspects du problème. Mais ce résultat ne saurait être une solution satisfaisante. Il empêche même l'émergence d'une vraie solution et a de nombreuses conséquences négatives.

Certes, les solutions seront difficiles à trouver, mais de nombreuses personnes travaillent déjà dans ce sens. Leur émergence dépend de la coopération et de la confiance internationales qui seraient sapées par une décision de la Cour suprême en faveur de la position du gouvernement américain. Nous exhortons les Européens à tenir compte des impacts à long terme de leurs actions lorsqu'ils abordent ces questions aujourd'hui car les solutions unilatérales à court terme ruinent les chances de trouver des solutions à long terme plus efficaces. Le moment est venu pour les États-Unis et pour l'Europe de s'engager dans un dialogue constructif sur ces questions essentielles, en s'efforçant de parvenir à un accord international plutôt qu'à des solutions unilatérales.

Références

[1] Voir Michael Chertoff, "Wanted: An International Rule of Law for Cloud Data," The Wall Street Journal, 18 Décembre 2014, Disponible sur https://www.wsj.com/articles/michael-chertoff-wanted-an-international-rule-of-law-to-govern-the-cloud-1418946310

[2] Le titre officiel est In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197 (2d Cir. 2016), reh'g en banc denied, 855 F.3d 53 (2d Cir. 2017), cert. granted, __ U.S. __ (Oct. 16, 2017).

[3] Andrew K. Woods, Data Beyond Borders: Mutual Legal Assistance in the Internet Age (Washington, DC: Global Network Initiative, January 2015): 3, Disponible sur https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf

[4] Jonathan Watts, "Brazilian police arrest Facebook's Latin America vice-president," The Guardian, 1er mars 2016, Disponible sur https://www.theguardian.com/technology/2016/mar/01/brazil-police-arrest-facebook-latin-america-vice-president-diego-dzodan

[5] Daniel Severson, "Taking Stock of the Snoopers' Charter: The U.K.'s Investigatory Powers Bill," Lawfare, 14 mars 2016, Disponible sur https://www.lawfareblog.com/taking-stock-snoopers-charter-uks-investigatory-powers-bill

[6] Stibee, "Court of Cassation definitively confirms Yahoo!'s obligation to cooperate with law enforcement agencies," Lexology, 15 juillet 2014, Disponible sur https://www.lexology.com/library/detail.aspx?g=065e35f1-5e2d-4f9d-9200-e236fcbb9397

[7] Une telle impulsion peut être observée chez certaines autorités en charge de la protection des données lorsqu'elles appliquent l'extraterritorialité de la législation européenne en la matière. L'exemple le plus parlant est la demande que la CNIL a faite à Google d'appliquer ses décisions de déréférencement de façon globale. Ici, l'objectif est compréhensible et le mécanisme similaire. Ce sujet reste un point de désaccord entre les Etats-Unis et l'Europe.

[8] David Kris, "U.S. Government Presents Draft Legislation for Cross-Border Data Requests," Lawfare, 16 juillet 2016, Disponible sur https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests

[9] Joe Uchill, "DOJ pitches agreements to solve international data warrant woes," The Hill, 24 mai 2017, Disponible sur http://thehill.com/policy/cybersecurity/335015-doj-to-sens-bilateral-agreements-could-solve-international-data-warrant

DONNÉES, EXTRATERRITORIALITÉ ET SOLUTIONS INTERNATIONALES AUX PROBLÈMES TRANSATLANTIQUES D'ACCÈS AUX PREUVES NUMÉRIQUES

par Théodore CHRISTAKIS

Professeur de droit international
Université Grenoble Alpes/Institut Universitaire de France
Directeur du Centre d'Etudes sur la Sécurité Internationale et les Coopérations Européennes
Directeur Adjoint du Grenoble Alpes Data Institute

1. Contexte et objectifs de cette étude.

L'auteur a été contacté le 17 novembre 2017 par CEIS afin de préparer une étude juridique sur l'affaire dite « *Microsoft Ireland Warrant* Case» opposant le gouvernement américain à la société Microsoft devant la Cour Suprême des Etats-Unis. Cette étude juridique sera intégrée dans un « livre blanc » sur cette affaire, initié par Microsoft et publié par CEIS, The Chertoff Group et l'auteur de cette étude. L'auteur a bénéficié d'une complète indépendance dans la rédaction de cette étude. Le contenu de celle-ci n'engage ni CEIS, ni The Chertoff Group, ni Microsoft et ne reflète que les opinions de son auteur. La partie I de cette étude présente de la façon la plus accessible possible les paramètres de cette affaire. La partie II examine les questions soulevées devant la Cour Suprême américaine. La partie III s'interroge sur les conséquences négatives qu'un arrêt de la Cour Suprême en faveur du gouvernement américain pourrait avoir. La partie IV, enfin, montre que le droit international offre aux Etats différentes possibilités leur permettant de trouver des solutions au problème de l'accès des services de justice aux preuves numériques lors d'une enquête pénale.

2. Eviter les amalgames dans une affaire complexe.

L'affaire *Microsoft Ireland* soulève des questions fondamentales sur le statut juridique des données dans le monde contemporain et sur la souveraineté des Etats dans le cyberespace, des questions qui intéressent aussi bien les autorités publiques des différentes nations que les entreprises, les individus et la société civile. Les implications de cette affaire ne devraient être sous-estimées par personne. En même temps, l'affaire est complexe. Ses méandres et impressionnantes ramifications pourraient facilement égarer l'observateur et l'induire dans des errements logiques ou de regrettables comparaisons. Il est donc impératif de 'décomplexifier' autant que possible cette affaire en présentant ses tenants et aboutissants, ainsi que les véritables questions juridiques qu'elle soulève.

3. Les faits

En décembre 2013, un Juge américain a ordonné à Microsoft de livrer aux autorités américaines, dans le cadre d'une affaire de trafic de stupéfiants, les emails d'un suspect qui se trouvaient sur un serveur de Microsoft situé en Irlande. Le mandat de perquisition relatif à ce compte de messagerie électronique a été donné par le Juge dans le cadre d'une loi américaine de 1986 sur les communications stockées *(Stored Communications Act, « SCA »).* Microsoft a toutefois refusé de livrer le contenu de cette messagerie électronique considérant que les données en question se trouvaient dans son data center situé en Irlande et que la SCA n'avait pas d'effet extraterritorial. Dans une décision rendue le 14 juillet 2016, une Cour d'appel des Etats-Unis (Second Circuit) a estimé que le gouvernement des Etats-Unis ne pouvait pas contraindre une entreprise à transmettre les courriers électroniques de ses clients conservés sur des serveurs situés hors du territoire des Etats-Unis. La Cour a estimé que le Congrès n'avait pas donné aux dispositions de la loi SCA une application extraterritoriale et qu'un mandat au titre de cette loi « ne pouvait s'appliquer qu'aux données stockées sur le territoire des Etats-Unis ». Le gouvernement américain a contesté cette décision devant la Cour Suprême américaine qui a accepté, en octobre 2017, de se saisir de cette affaire. La procédure est en cours actuellement et sa décision devrait être rendue au mois de juin 2018.

4. Ce qui est en cause ici : des "données relatives au contenu".

Il convient tout d'abord de préciser que, ce qui est en cause dans cette affaire, c'est l'accès du gouvernement américain aux « données relatives au contenu » d'un client de Microsoft, en l'occurrence le contenu de tous les messages électroniques que le suspect aurait échangé avec d'autres personnes. Ceci est important pour la compréhension de l'affaire pour plusieurs raisons. **Premièrement**, parce que les « données relatives au contenu » (emails dans cette affaire précise, mais cela pourrait concerner tous les documents, photos ou films stockés par un suspect dans le cloud) sont au coeur de la vie privée, tant des personnes directement visées, que de personnes tierces (qu'il s'agisse des correspondants du suspect, dont les emails échangés avec celui-ci seront aussi lus par les autorités, ou, dans d'autres hypothèses, des personnes qui figurent sur des photos et des films). **Deuxièmement**, parce que la demande formulée par les autorités américaines à Microsoft, qui est d'accéder de façon unilatérale (et sans passer par les mécanismes internationaux d'entraide judiciaire prévus à cet effet) aux « données relatives au contenu » de l'un de ses clients, distingue cette affaire de celles, nombreuses, qui concernent des demandes formulées par des Etats auprès de fournisseurs pour accéder aux seules « données relatives aux abonnés » - c'est-à-dire aux informations permettant uniquement *d'identifier l'utilisateur* d'une adresse IP précise ou d'un service (sans pour autant avoir accès au contenu de ses communications). En pratique, les Etats demandent fréquemment aux ISP (Internet Service Providers - fournisseurs de service internet et cloud) communication des « données relatives aux abonnés » dans le cadre de procédures d'enquête et les ISP les fournissent le plus souvent (s'ils considèrent que la demande est formulée dans un cadre légal par un pays respectant l'Etat de droit).[1] La demande de produire des « données relatives aux abonnés » s'immisce évidemment moins dans les droits de la personne et les intérêts des tiers que la demande d'accès aux « données relatives au contenu » formulée par le gouvernement américain dans l'affaire Microsoft. Il convient de surcroit de constater que, pour ce qui est des « données relatives aux abonnés », les Etats *pourraient éventuellement s'appuyer sur un titre qui leur est conféré par le droit international* : l'article 18.1.b de la Convention de Budapest sur la cybercriminalité de 2001 permet en effet aux Etats de se doter d'une législation ordonnant aux ISP de communiquer les « données relatives aux abonnés » (et uniquement celles-ci) après injonction des autorités et ceci quel que soit leur lieu de stockage. L'affaire *Microsoft Ireland* n'a donc rien de comparable avec des affaires (comme l'affaire « Twitter » en 2013 en France[2]) où les tenants et aboutissants sont entièrement différents et ne concernent que l'accès aux « données relatives aux abonnés ».

5. Le principe recherché par le gouvernement américain l'autoriserait demain à obtenir les messages électroniques, stockés en France, d'un ressortissant et résident français.

Le deuxième élément important à prendre en considération est que la nationalité du suspect n'a pas été communiquée à la justice par les autorités américaines. Dans son opinion individuelle, le Juge Gerard Lynch a ainsi tenu à souligner que : « Si celui-ci est Irlandais (ce qui semble être le cas), cette affaire pourrait avoir d'inquiétantes retombées sur le plan international : les griefs du Gouvernement irlandais et de l'Union européenne pourraient en effet être nombreux si les Etats-Unis cherchaient à obtenir les messages électroniques d'un ressortissant irlandais, stockés en Irlande, auprès d'une entreprise américaine offrant ses services à des clients irlandais en Irlande ». Ce que le Juge Lynch pointe dans cette affaire, c'est que le principe derrière l'affaire Microsoft, devrait intéresser tous les Etats. Si la Cour Suprême donne en effet raison au gouvernement américain, cela signifie que, demain, les autorités américaines pourront, par exemple, émettre un mandat exigeant de Microsoft ou d'un autre fournisseur de cloud opérant aux Etats-Unis (Apple, Amazon, IBM, Google, Facebook…) de livrer les « données de contenu » d'un ressortissant français suspecté de crime aux Etats-Unis (y compris, par exemple, un journaliste accusé de porter atteinte à la sécurité nationale américaine), alors même que ce français réside en France, que ses données sont stockées par ce fournisseur en France , et ceci sans passer par une commission rogatoire internationale ou une quelconque autre forme de coopération avec les autorités françaises.

6. Le lieu de stockage des données est connu : c'est l'Irlande.

Un autre aspect important de cette affaire est que le lieu de stockage des données a été immédiatement communiqué aux autorités américaines par Microsoft qui assure, d'ailleurs (voir §15) être toujours en mesure d'indiquer aux autorités où se situent les données associées à un compte précis qu'elles recherchent. Quelles que soient donc les réflexions juridiques que l'on pourrait avoir dans l'hypothèse où un ISP ne pourrait connaître et/ou communiquer le lieu où se situent les données[3], ces questions sont sans pertinence pour l'affaire *Microsoft Ireland*. En d'autres termes, dans cette affaire, les Etats-Unis savent à quelle autorité compétente la demande d'entraide judiciaire doit être faite et ont parfaitement la possibilité de s'adresser à l'Irlande avec la quasi-certitude d'obtenir les données. Pourtant, les Etats-Unis n'ont pas eu recours aux mécanismes d'entraide judiciaire, optant plutôt pour une démarche unilatérale en enjoignant Microsoft de livrer ces données.

7. L'accès aux données électroniques est crucial pour les services de justice et de police.

Tant le gouvernement américain que Microsoft s'accordent sur un premier point, qui mettrait d'ailleurs d'accord n'importe quel pays : les évolutions technologiques et la « digitalisation » de la vie des personnes présentent un immense défi pour les services de l'ordre et la justice qui, pour faire efficacement leur travail et protéger la société, doivent sécuriser les preuves sur les serveurs. Au-delà de la « cybercriminalité », des preuves en lien avec *tout type d'infraction* sont conservées sur des systèmes informatiques qui, souvent, se situent à l'étranger. Pour enquêter efficacement et sécuriser des preuves en vue d'un procès, les services de l'ordre doivent donc accéder aux « preuves dans les nuages ». Ceci vaut autant dans la lutte contre le terrorisme et son financement, que pour toute une série d'autres crimes tels que la fraude et les délits financiers, le blanchiment de capitaux, les meurtres, agressions et autres crimes violents, la traite d'êtres humains, le trafic de stupéfiants, la pédopornographie et d'autres formes d'abus à l'encontre d'enfants. Tant le gouvernement américain que Microsoft s'accordent pour reconnaitre qu'il faut garantir la prééminence du droit dans le cyberespace et trouver des solutions permettant l'accès des autorités aux preuves digitales. Ils divergent, néanmoins, sur le comment y parvenir et comment résoudre les nombreux défis juridiques et juridictionnels relatifs à ce problème.

8. La loi SCA n'a pas d'effet extraterritorial.

Un second point qui semble faire l'objet d'un accord entre les parties est que la loi SCA, sur la base de laquelle le mandat a été donné (§3), ne peut pas s'appliquer de façon extraterritoriale. Le gouvernement américain a en effet reconnu, à plusieurs reprises, que « it is undisputed that [the SCA] lacks extraterritorial reach ».[4] La Cour d'appel a aussi conclu que « le Congrès n'a pas donné aux dispositions de la loi SCA une application extraterritoriale » et les juges de la majorité ont même appelé le Congrès à « réviser une loi désuète » rédigée bien avant l'ère des emails et du cloud – ce qui est d'ailleurs en cours, une proposition de loi intitulée « International Communications Privacy Act » (ICPA) ayant été à cet effet introduite en 2016 devant le Sénat américain.[5] Les points d'accord entre les parties s'arrêtent néanmoins là.

9. Y-a-t-il « extraterritorialité » dans cette affaire ?

Un point de désaccord majeur porte sur la question de savoir si cette affaire comporte un élément d'application extraterritoriale de la loi SCA. Si nous sommes en effet dans un cadre d'application extraterritoriale, la Cour devrait alors donner raison à Microsoft. L'espace limité de notre étude ne permet pas d'entrer dans le détail des subtilités du droit américain discutées par les deux parties – et surtout la différence entre un « warrant » et une « subpoena » qui, de toute façon, n'apporte rien à la compréhension internationale de cette affaire et de ses implications importantes. Essayons donc de simplifier. **Pour Microsoft** (et la Cour d'appel) les choses sont simples : un mandat au titre de la loi SCA ne peut pas s'appliquer aux données stockées en Irlande car il ne peut pas avoir d'effet extraterritorial. Or cet effet extraterritorial est clair ici. Si le gouvernement américain souhaite donc accéder à ces données, il n'a qu'à formuler une demande auprès des autorités irlandaises dans le cadre des mécanismes existants d'entraide judiciaire. **Pour le gouvernement américain**, au contraire, il n'y a, dans ce cas, « aucune application extraterritoriale de la loi ». Selon lui, à partir du moment où les données en question sont accessibles depuis les Etats-Unis (même si elles sont stockées en Irlande) tout se passe sur le sol américain et il n'y a donc aucune « extra-territorialité » (interdite selon la loi SCA). Le gouvernement souligne à cet égard que : « *Microsoft's U.S.-based employees could make that disclosure without leaving their desks*".[6] Un clic de souris depuis Washington DC suffit à accéder aux données. **Pour le gouvernement américain**, ce transfert des données opéré par Microsoft de l'Irlande vers les Etats-Unis n'implique par ailleurs aucune atteinte à la vie privée du suspect. Ce n'est en effet qu'au moment de la « disclosure », c'est-à-dire au moment où l'agent du gouvernement américain ouvre les emails transférés par Microsoft aux Etats-Unis qu'il y a atteinte à la vie privée (par ailleurs justifiée car il s'agit d'une enquête pénale). Or, cette « divulgation » ayant lieu sur le territoire américain, seule la loi américaine est applicable à l'exclusion de toute loi étrangère relative à la protection de la vie privée. La question fondamentale à laquelle la Cour Suprême doit répondre est donc relativement simple : *la demande adressée par le gouvernement américain à Microsoft constitue-t-elle une application « extraterritoriale » de la loi sur laquelle cette demande est fondée* ? **Pour le gouvernement américain** la réponse est négative car *le seul critère pertinent est l'endroit d'où les données sont accessibles.* Dans la mesure où Microsoft (comme le suspect lui-même d'ailleurs) peut accéder à ces données depuis les Etats-Unis, tout se déroule sur le sol américain. **Pour Microsoft**, en revanche, *le critère déterminant est le lieu de stockage des données.* Dans la mesure où ces données sont stockées en Irlande, le gouvernement américain demande clairement à Microsoft une action ayant une portée extraterritoriale.

10. Nécessité fait loi ?

Une autre question soulevée par cette affaire et qui semble faire l'objet d'importants désaccords, est celle de savoir si la nécessité, pour les services de l'ordre, d'accéder aux preuves dans les nuages pour faire leur travail et protéger la société (§7) est une raison suffisante pour que la Cour Suprême confère cette possibilité juridique au gouvernement. Dans ses Mémoires, **le gouvernement** accuse la décision de la Cour d'Appel rendue en 2016 en faveur de Microsoft de constituer un « *"unprecedented ruling [which] has put the safety and security of Americans at risk by severely limiting a critical law enforcement tool ».* L'affaire y est présentée comme posant une question « of exceptional importance to public safety and national security ».[7] Le message adressé à la Cour Suprême est clair: la fin justifie les moyens. **Pour Microsoft**, néanmoins, ce raccourci n'est pas acceptable. Selon elle, la demande d'accès à des « données de contenu » stockées dans un pays étranger présente des risques considérables, tant pour les individus concernés (atteinte à leur vie privée, voire à d'autres droits comme nous le verrons §21 et 23), que pour les entreprises elles-mêmes (qui pourraient, notamment, se trouver dans une situation de conflits de lois et de juridictions - §24) et les Etats concernés. Selon Microsoft, donc, la nécessité doit être gérée dans le cadre du droit établi – et en améliorant ce cadre, mais pas de façon unilatérale et anarchique. Cette position semble compatible avec les prémisses du droit international contemporain. Comme nous l'avons expliqué longuement ailleurs, la nécessité est prise en compte par le droit, mais elle est aussi *rigoureusement encadrée* par celui-ci afin d'éviter une utilisation abusive.[8]

11. La pertinence du droit international.

Ceci nous amène à un dernier point. Si les Mémoires de Microsoft prennent aussi en compte le droit international, ceux du Gouvernement américain le font moins (ce qui est cohérent avec l'argument principal selon lequel « tout se passe aux Etats-Unis »). La Cour d'appel ne consacre, parmi les 43 pages de sa décision, qu'un seul paragraphe au droit international (infra §17) et il est probable (même si cela serait regrettable) que la décision de la Cour Suprême n'en comporte aucun. Pourtant, cette affaire intéresse directement le droit international. Si, du point de vue du droit américain, la question est : « existe-t-il ou non, dans cette affaire, une dimension extraterritoriale », du point de vue du droit international la question est de savoir si cette extraterritorialité est problématique et quels pourraient être les effets de cette affaire pour l'ordre juridique international. Dans la suite de cette étude nous aborderons donc aussi ces questions.

II. L'existence claire d'un élément d'extraterritorialité (et la faiblesse du critère de « l'endroit d'où les données sont accessibles »)

12. Le concept d'extraterritorialité en droit international.

Avant de répondre à la question de savoir si le mandat adopté sur la base de la loi SCA comporte un élément d'extraterritorialité (auquel cas la Cour Suprême devrait statuer en faveur de Microsoft en confirmant la décision de la Cour d'Appel), il convient de rappeler rapidement ce que ce terme signifie. Le droit international confère en effet à l'Etat le pouvoir juridique de soumettre des personnes physiques et morales, des activités et des biens, à son ordre juridique. La compétence des Etats se décline en compétence législative (édicter des normes), compétence juridictionnelle (administration de la justice) et compétence exécutive (pouvoir de donner effet aux ordres émanant de leur système juridique par des actes matériels). La grande question qui se pose est de savoir où l'Etat peut exercer ces différents pouvoirs. Selon le droit international, l'Etat peut exercer l'ensemble de ces pouvoirs dans les limites de son territoire – c'est ce que l'on appelle la compétence « territoriale » de l'Etat. L'Etat peut aussi, mais sous certaines conditions, exercer sa compétence à l'égard de personnes (surtout ses nationaux) ou de biens situés sur le territoire d'un autre Etat, voire dans des espaces appartenant à aucun Etat (tels que la Haute Mer). C'est ce qu'on appelle la « compétence extraterritoriale ». Cette dernière est, bien entendu, strictement encadrée par le droit international car il va sans dire que la volonté d'un Etat d'exercer ses compétences (surtout exécutives) sur le sol d'un Etat tiers pourrait violer la souveraineté de ce dernier et créer des vives tensions internationales. On peut donc dire que, de façon générale, il y a extraterritorialité de l'application d'une norme « si tout ou partie du processus d'application se déroule en dehors du territoire de l'Etat qui l'a émise » ou encore chaque fois « qu'un Etat prétend appréhender, à travers son ordre juridique, des éléments situés en dehors de son territoire ».[9]

13. Les impasses logiques du critère de « l'endroit où les données sont accessibles ».

Nous avons vu que le gouvernement américain considère qu'il n'y a « aucune extraterritorialité » dans l'affaire *Microsoft Ireland* car « les données sont accessibles depuis les Etats-Unis ». Cet argument pourrait sembler à première vue logique et traduire une profonde refondation du concept d'extraterritorialité dans le monde digital. Il est, en réalité, très problématique et ceci pour plusieurs raisons. Premièrement, et dans la mesure où pratiquement toutes les données digitales sont « accessibles depuis les Etats-Unis », la loi SCA s'appliquerait à toutes les données au monde : celles des américains, mais aussi celles produites par des étrangers à l'étranger et stockées à l'étranger. En d'autres termes, même s'il n'existe aucun lien entre le suspect et ses données d'une part, et les Etats-Unis

d'autre part (autre que l'existence d'un mandat adopté par les autorités américaines), l'affaire serait toujours censée se produire aux Etats-Unis (car les données sont accessibles depuis le sol américain). Ainsi, même pour un français habitant en France, n'ayant jamais mis les pieds aux Etats-Unis, utilisant un serveur de messagerie stockant ses données en France, il n'y aurait « aucun élément d'extraterritorialité » lors d'une demande adressée à son ISP (ayant son siège ou une filiale aux Etats-Unis) d'accéder à ses emails sur mandat américain à partir du moment où « il peut avoir accès à ses mails depuis un ordinateur aux Etats-Unis ». La loi SCA, dont tout le monde reconnaît qu'elle ne peut avoir d'effet extraterritorial, serait donc miraculeusement en mesure de s'appliquer pour accéder aux emails, photos et documents personnels de pratiquement n'importe quel individu ayant un compte cloud pouvant être consulté théoriquement à partir des Etats-Unis ! Le caractère fallacieux de l'argument semble trop évident pour que l'on s'y attarde. Quant à la tentative de « séquencer » les opérations (§9) en prétendant qu'il existerait deux opérations distinctes : 1) le « transfert des données » par Microsoft aux Etats-Unis et 2) le moment de « divulgation » aux autorités de ces données désormais « américaines » – elle est tout aussi fallacieuse. Nous n'avons pas l'espace de nous attarder sur ce dernier point, mais l'extraterritorialité est évidente dans la mesure où le transfert des données vers les Etats-Unis ne se fait que parce que le mandat contraint Microsoft à le faire et ceci afin de transmettre ces données aux autorités américaines. Il est donc impossible juridiquement et logiquement de « saucissonner » ces opérations.

14. Les limites de la campagne menée contre le critère du « lieu du stockage des données ».

Ceci nous amène à une question clé : est-ce que le critère du « lieu du stockage des données », avancé par Microsoft, a une valeur quelconque ? Le gouvernement américain a beaucoup insisté sur le caractère « arbitraire » d'un tel critère. Les données sont extrêmement mobiles et fluides : elles bougent tout le temps, elles sont partout. Les fournisseurs de cloud eux-mêmes concèdent qu'ils stockent les données non pas à un seul mais à plusieurs endroits (en faisant des copies nécessaires pour éviter une perte des données en cas de problème sur le data center principal) et qu'ils font voyager les données chaque fois qu'une opération de maintenance le nécessite. Le lieu de stockage des données pourrait d'ailleurs être décidé exclusivement sur la base de considérations économiques et changer si des options moins couteuses se présenteraient. Comment est-il possible de priver la justice d'un accès à ces données nécessaires pour faire son travail sur la base d'un critère aussi contestable, fluctuant et arbitraire ? Pourquoi soumettre les autorités étatiques au supplice de Tantale,

les obligeant chaque fois que les données ont « bougé », à lancer de nouvelles procédures, couteuses et chronophages, d'entraide judiciaire vers les nouveaux pays « de stockage » ? N'y-t-il pas un risque de voir alors apparaître des « paradis digitaux » dans des pays peu scrupuleux avec la complicité de certains ISP qui déplaceraient systématiquement les données pour empêcher que la justice y accède ? Tous ces arguments sont importants et pourraient donner lieu à d'interminables débats. C'est la raison pour laquelle l'auteur de cet avis est convaincu que le critère de la localisation des données est seulement un, parmi d'autres critères, à prendre en compte pour construire un régime juridique satisfaisant (infra §28). Il ne faudrait toutefois pas que ces arguments conduisent à une sorte de populisme, découpé des réalités techniques, juridiques et géopolitiques, effaçant complètement de l'équation le critère du « lieu du stockage des données ».

15. Le lieu de localisation des données compte.

Ainsi que l'a très bien montré une remarquable palette de computer et *data scientists* dans un *Amicus Curiae* déposé devant la Cour d'Appel,[10] le lieu de stockage a une grande importance sur le plan technique : les données ont bien une « localisation physique » et sont stockées en utilisant des disques durs qui se trouvent dans des data centers situés dans des pays précis. Quand on accède ainsi à des emails, cela signifie techniquement que l'on récupère des données à partir d'un espace physique précis où elles sont stockées. Les données ont donc une « matérialité » beaucoup plus importante que ce qui est souvent suggéré. Des entreprises comme Microsoft ont investi des centaines de millions d'euros pour construire des data centers dans des endroits précis sur la base tant de considérations de performance (liée surtout à la proximité géographique entre l'usager et le lieu de stockage), qu'à des considérations juridiques liées à la protection des données. Ainsi, après surtout les révélations de E. Snowden, des entreprises comme Microsoft ont créé plusieurs data centers en Europe (Allemagne, France, Irlande, Pays-Bas, Royaume-Uni) et ont décidé de stocker les données des Européens en Europe[11] – afin de leur donner l'assurance que celles-ci seraient couvertes par la protection européenne en matière de données personnelles (y compris par le RGPD) et ne seraient pas accessibles aux autorités américaines sans passer par les procédures formelles prévues par le droit international. Loin donc d'être « fortuit », le lieu du stockage dans l'affaire *Microsoft Ireland* est très important techniquement et juridiquement et le contourner en prétendant « qu'il n'y a aucune extraterritorialité » dans le mandat américain serait grave de conséquences.

16. L'Irlande pense qu'il y a extraterritorialité.

Un autre indice témoignant de l'existence d'un élément d'« extraterritorialité » dans cette affaire est la réaction de l'Irlande où se trouve le data center de Microsoft. Le Juge qui avait donné raison au gouvernement américain (et dont la décision fut renversée par la Cour d'Appel) avait prétendu qu'il n'y avait pas d'effet extraterritorial car le mandat « *does not criminalize conduct taking place in a foreign country* » et « *does not involve the deployment of American law enforcement personnel abroad* ».[12] Bref, l'accès par les autorités américaines aux emails stockés en Irlande n'affecterait nullement l'Irlande, il n'y aurait donc pas d'extraterritorialité. Le problème, néanmoins, est que l'Irlande ne semble pas partager cette analyse. Dans un *Amicus curiae* soumis à la Cour d'Appel américaine, l'Irlande souligne qu'elle a « *a genuine and legitimate interest in potential infringements by other states of its sovereign rights with respect to its jurisdiction over its territory* », tout en indiquant qu'elle serait prête à examiner « de la façon la plus expéditive possible » une demande d'entraide judiciaire, si les Etats-Unis formulaient une telle demande dans le cadre de l'accord d'assistance juridique mutuel (Mutual Legal Assistance Treaty – « MLAT ») conclu entre les deux pays.[13] Même si l'Irlande n'accuse pas les Etats-Unis d'une violation de sa souveraineté (ce qui peut se comprendre aux vues des relations amicales qui prévalent entre les deux pays), son *Amicus curiae* constitue une indication claire du caractère extraterritorial de l'affaire qui devrait, en principe, être réglée par le canal du droit international.

17. L'Union Européenne pense qu'il y a extraterritorialité.

Au-delà de l'Irlande, il convient aussi d'avoir une vue de l'ensemble de la mosaïque. Depuis plusieurs années en effet, l'Union Européenne a développé un régime juridique très protecteur des données personnelles et de la vie privée. L'entrée en vigueur effective du Règlement général sur la protection des données (RGPD) en mai 2018 ; la transposition dans le même temps de la Directive 2016/680 relative à la *protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données* ; la négociation actuelle du règlement ePrivacy sur le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques ; la conclusion de plusieurs accords internationaux (dont *Privacy Shield*) ; et beaucoup d'autres activités encore témoignent de la volonté de l'Union Européenne non seulement de mettre en place une protection forte des données personnelles et de la vie privée en Europe, mais aussi de s'asurer que les données des

citoyens et résidents européens, stockés en Europe, ne puissent être transférées à l'étranger (y compris vers les autorités d'Etats tiers dans le cadre d'une procédure d'enquête) que sous certaines conditions strictes, y compris le respect de certaines procédures et l'existence de garanties suffisantes. Dans ce contexte, il ne faut pas s'étonner que, pour l'Union Européenne, le mandat donné à Microsoft par les autorités américaines est considéré comme « extraterritorial » et pourrait même être perçu comme une tentative de contourner la protection juridique mise en place en Europe. La position européenne à cet égard a été très bien résumée dans une déclaration de 2014 de Viviane Reding, alors Vice-présidente de la Commission Européenne et Commissaire chargée de la justice, des droits fondamentaux et de la citoyenneté, qui avait réagi à la décision du tribunal de première instance américain (donnant raison au gouvernement américain) de la façon suivante :

"The effect of the US District Court order is that it bypasses existing formal procedures that are agreed between the EU and the US, such as the Mutual Legal Assistance Agreement, that manage foreign government requests for access to information and ensure certain safeguards in terms of data protection. The Commission's concern is that the extraterritorial application of foreign laws (and orders to companies based thereon) may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union. […] The Commission has raised this issue with the US government on a number of occasions. The Commission remains of the view that where governments need to request personal data held by private companies and located in the EU, requests should not be directly addressed to the companies but should proceed via agreed formal channels of co-operation between public authorities, such as the mutual legal assistance agreements or sectorial EU-US agreements authorising such transfers".[14]

De manière encore plus explicite, le Vice-Président du Comité LIBE (*libertés civiles, de la justice et affaires intérieures*) du Parlement Européen, Jan Philipp Albrecht, soulignait dans un *Amicus Curiae* soumis à la Cour d'Appel américaine :

"Personal data located in EU territory is subject to strict rules designed to maintain the autonomy of the affected individual (data subject). Those rules apply to the email account covered by the warrant in issue in this case. They balance the protection of the individual's rights with the necessity of data processing for public interests, such as law enforcement. […] The decision of the District Court effectively permits this carefully constructed regime to be sidestepped. […] It is fair to record that there are major differences between the U.S. and European laws on data protection. The European standard is much more severe than the U.S. standard. […] For U.S. law to treat data stored in Europe as if it were stored in the United States is a territorial encroachment without justification, and one which is exacerbated by the sharp differences in the legal status of personal data in the U.S. and the EU. […] This unilateral exercise of jurisdiction over data held in the EU puts into serious jeopardy the level of trust between the EU and U.S. on data protection matters".[15]

A la lumière de tous ces éléments soumis à son attention, on peut comprendre pourquoi la Cour d'Appel américaine a pris une décision en faveur de Microsoft, considérant qu'il y avait une « application extraterritoriale et illégale de la loi » et critiquant sévèrement « la théorie selon laquelle aucune atteinte n'est portée aux intérêts de l'Etat souverain étranger lorsqu'un Juge des Etats-Unis ordonne à un fournisseur de services de « collecter » sur des serveurs situés à l'étranger et d'« importer » vers les Etats-Unis des données pouvant appartenir à un ressortissant étranger… ».[16]

18. Le comportement des Etats-Unis semble indiquer qu'il y a extraterritorialité.

Allant encore plus loin, on pourrait se demander si le comportement américain lui-même ne pourrait pas donner quelques indices sur l'existence d'une situation extraterritoriale chaque fois qu'il y a transfert de données stockées en Europe vers les Etats-Unis. Il faut souligner, à cet égard, que les Etats ont, ces dernières années, multiplié la conclusion d'accords en matière d'entraide judiciaire (« MLAT », v. §16, 22 et 30) afin, surtout, de faire face aux nouveaux défis de coopération transfrontalière et d'accès aux preuves digitales à l'ère du numérique. Ainsi, selon une étude, entre 1977 et 2013, le nombre de MLATs est passé d'un nombre restreint à plusieurs centaines.[17] Les Etats-Unis ont conclu des MLAT's avec plus de 60 pays – dont un bon nombre de pays européens, y compris l'Irlande et la France. Les Etats-Unis ont aussi conclu un MLAT (entré en vigueur en 2010) avec l'Union Européenne elle-même dont l'un des objectifs (article 9) est de prendre en compte les exigences de protection des données à caractère personnel au sein de l'Union Européenne.[18] En concluant cet accord, **les Etats-Unis ont reconnu que les tribunaux américains « lack the authority to subpoena evidence in a foreign country »**[19] ce qui semble aller à l'encontre de l'argumentation actuelle du gouvernement américain devant la Cour Suprême. Ils ont aussi reconnu que, normalement, la production de preuves qui se trouvent situées dans un pays européen, implique un élément d'extraterritorialité et devrait se faire en passant par les canaux d'entraide judiciaire.[20] Au-delà des MLATs, les Etats-Unis ont aussi conclu ces dernières années toute une série d'accords (*Privacy Shield*, PNR, accord sur le transfert des données de messagerie financière...) qui sont tous fondés sur l'idée selon laquelle, non seulement il y a transfert des données stockées en Europe vers les Etats-Unis (et donc clairement extraterritorialité), mais, de plus, que ce transfert ne peut se faire qu'en respectant la protection qui accompagne les données européennes.

19. Conclusion

Les éléments qui précédent montrent clairement que l'argument selon lequel « il n'y a aucune extraterritorialité » dans l'injonction du gouvernement américain aux fournisseurs de transférer des données de l'Europe vers les Etats-Unis ne peut être retenu. Ceci devrait être suffisant pour que la Cour Suprême américaine confirme la décision de la Cour d'Appel en faveur de Microsoft. Il convient, néanmoins, de s'interroger sur les conséquences qu'une décision de la Cour Suprême en faveur du gouvernement américain pourrait avoir.

III. Les conséquences possibles d'un arrêt en faveur du gouvernement américain

20. La malédiction de Cassandre.

Il est toujours difficile et risqué de prédire l'avenir – surtout dans le cyberespace. Il est néanmoins légitime de nourrir quelques inquiétudes quant aux conséquences négatives qu'un arrêt de la Cour Suprême en faveur du gouvernement américain pourrait avoir. Toutes ces conséquences ne se réaliseront pas nécessairement, certaines étant exclusives d'autres. Leur réalisation dépendra d'ailleurs du comportement des divers acteurs impliqués - qui n'est pas toujours facilement prévisible. Il est, par exemple, difficile de prédire si les pays européens et l'Union Européenne réagiront avec ténacité à un tel arrêt de la Cour Suprême – ou s'ils préfèreront faire « profil bas » considérant que, par des chemins sinueux et impénétrables, un tel arrêt pourrait aussi avoir certains effets positifs. Les Européens pourraient, par exemple, espérer qu'un tel arrêt aurait la potentialité de faciliter leur propre accès aux preuves numériques si les Etats-Unis se montraient « généreux » avec leurs alliés européens – encore qu'une telle « générosité » serait non seulement aléatoire (aucune obligation de le faire) mais aussi, par définition, juridiquement limitée.[21] Certains gouvernements européens pourraient aussi nourrir l'espoir qu'un tel arrêt de la Cour Suprême aurait l'effet miraculeux de favoriser l'émergence d'une industrie européenne du cloud. Nous présenterons, néanmoins, quelques brèves remarques concernant des conséquences qui semblent particulièrement plausibles compte tenu des paramètres de l'affaire.

21. Un risque dangereux de mimétisme ?

Il est à craindre que si la Cour Suprême retient l'argumentation du gouvernement américain et le critère « de l'endroit d'où les données sont accessibles », chaque pays puisse être tenté de faire exactement de même. Si l'on considère en effet qu'une opération consistant à demander à un fournisseur internet de « transférer » les emails d'un étranger stockés à l'étranger ne comporte « aucun élément d'extraterritorialité », tous les pays pourraient alors formuler des demandes similaires aux seules conditions que : **a)** le fournisseur ait un bureau sur le sol du pays demandeur (Microsoft, par exemple, a des filiales dans plus de 120 pays…); et **b)** qu'il existe un mandat (voire une simple procédure) contre une personne suspectée de violer le droit national. Du point de vue de la protection des droits de l'homme, la simple perspective qu'une telle procédure puisse être utilisée contre des journalistes accusés de porter atteinte à la « sécurité nationale » par leurs enquêtes ou leurs écrits, ou contre de personnes accusées de « blasphème » pour leur position à l'égard de religions, suffit à montrer l'ampleur du problème. Du point de vue des relations interétatiques, le fait que les Etats contournent les mécanismes de coopération internationale afin de « se servir eux-mêmes » dans les données stockées dans d'autres pays, risque de provoquer de très vives tensions et déstabiliser profondément le droit international.

Les Etats-Unis sont-ils prêts à accepter que des pays étrangers enjoignent à des filiales locales des GAFAM (et autres) de les laisser collecter unilatéralement, et sans rien demander aux autorités américaines, les données des ressortissants américains, stockées aux Etats Unis, mais « accessibles d'un seul clic » depuis leurs capitales respectives ? « *We would go crazy if China did this to us* » a justement remarqué l'avocat de Microsoft devant la Cour d'Appel. Ou bien les Etats-Unis espèrent-ils que le modèle qu'ils essaient de promouvoir devant la Cour Suprême ne bénéficiera qu'à eux et ne sera applicable qu'au pays du « siège » - mais pas aux pays des filiales ? Un tel espoir semble plutôt vain. Le modèle qui consiste à « se servir unilatéralement sur le territoire d'autres pays » fera sans doute des envieux, ne serait-ce que sur la base du principe de réciprocité, et pourrait ouvrir des pages sombres pour la coexistence pacifique et la coopération internationale fondées sur le droit.

22. Un affaiblissement des accords internationaux d'entraide judiciaire ?

Au-delà des tensions qui pourraient naître entre les Etats, un tel unilatéralisme en matière de collecte des données pourrait affecter le fonctionnement de certains accords internationaux et surtout des MLATs conclus entre les Etats-Unis et des pays tiers. Si les Etats-Unis se lancent dans une collecte unilatérale des « preuves digitales » quel que soit le lieu où elles sont stockées, cela signifie qu'ils n'ont plus besoin de recourir aux MLATs (ou à d'autres mécanismes de coopération internationale) pour obtenir ces données. Ceci aura donc pour conséquence : soit **1)** que les MLATs vont connaître un profond déséquilibre - les pays tiers étant toujours obligés de demander aux autorités américaines, par le biais des MLATs, les données stockées aux Etats-Unis alors que les Etats-Unis n'ont plus besoin de ces pays pour accéder aux données stockées sur le territoire de ces derniers ; soit **2)** si tous les pays suivent le modèle unilatéraliste américain, que les MLATs deviendront obsolètes dans leur dimension « preuves numériques ».

23. Un affaiblissement de la protection de la vie privée et des droits de l'homme ?

Si les observations précédentes concernent les relations interétatiques, il convient aussi d'intégrer l'*individu* dans la problématique. Quel serait l'effet d'une décision de la Cour Suprême favorable au gouvernement américain ? Que se passerait-il si d'autres pays (voire tous les pays) s'inspiraient d'une telle jurisprudence en exigeant des filiales des ISP de leur livrer des données personnelles qui se trouvent dans d'autres juridictions ? Une telle situation pourrait affecter sérieusement la protection des données et de la vie privée. Les protections développées en Europe par un réseau dense d'instruments pour protéger les données personnelles contre les éventuels abus des autorités dans le monde post-Snowden, pourraient être contournées par des pays étrangers déterminés à accéder unilatéralement aux données personnelles produites et stockées en Europe sans que les autorités des pays européens puissent être consultées dans le cadre des

mécanismes traditionnels du droit international. D'autres droits pourraient aussi être affectés, tels que la liberté d'expression et la liberté de la presse (voir les exemples mentionnés supra § 21), y compris la protection des sources de journalistes, ou encore le secret professionnel entre les avocats et leurs clients. Par ailleurs, les voies de recours pourraient être sérieusement affaiblies. Un ressortissant français sait, par exemple, que l'Etat français peut accéder à ses emails et autres documents stockés dans des serveurs en France, s'il fait l'objet d'une enquête judiciaire, ou que la France pourrait transmettre ses données personnelles à un pays étranger dans le cadre d'un MLAT ou d'une commission rogatoire. Mais il sait aussi que, si les autorités agissent de façon abusive, il peut saisir les tribunaux français et que, si les tribunaux français manquent à leur devoir, il peut saisir la Cour européenne des droits de l'homme (CEDH). Si, en revanche, les Etats-Unis accèdent de manière unilatérale à ses données, le ressortissant français (à supposer même qu'il en ait connaissance – ce qui est loin d'être garanti) ne pourra pas déposer de recours contre son pays car celui-ci n'est pas impliqué dans la transmission des données. Il ne pourra pas non plus saisir les tribunaux américains car, au-delà du caractère impraticable d'un tel recours, les étrangers habitant à l'étranger ne sont pas protégés par le Quatrième Amendement qui prévoit « le droit des citoyens d'être garantis […] contre les perquisitions et saisies non justifiées ». Le seul remède possible sera donc de se tourner contre le fournisseur d'internet et de cloud qui se trouvera alors dans une situation de conflits de lois quasi-inextricable.

24. Conflits de lois.

Imaginons que la Cour Suprême se prononce dans cette affaire contre Microsoft et que l'entreprise se trouve demain, dans une affaire similaire, contrainte de fournir aux autorités américaines les données personnelles d'un français stockées en France. Dans la mesure où ce transfert est opéré par Microsoft, ceci constituera une violation tant du droit français que du droit européen. Certes, tant le droit français que le droit européen autorisent le transfert de données personnelles vers des autorités étrangères, mais à la condition que cela se fasse dans un cadre reconnu par le droit international, européen ou national (le « national » signifiant le droit du pays où se trouvent les données). Pour comprendre le régime juridique dans ce domaine, il convient de se référer à l'article 48 du RGPD ainsi rédigé :

*« Article 48 **Transferts ou divulgations non autorisés par le droit de l'Union.** Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre ».*

Dans son Mémoire devant la Cour Suprême,[22] le gouvernement américain a soutenu que si Microsoft transférait les données personnelles aux Etats-Unis dans le cadre de son mandat, il n'y aurait aucune violation du RGPD. Selon lui, la dernière phrase de l'article 48 (« sans préjudice d'autres motifs de transfert en vertu du présent chapitre ») montre qu'il existe des exceptions, surtout celle de l'article 49(§1d) du RGPD qui prévoit une dérogation à l'article 48 si « le transfert est nécessaire pour des motifs importants d'intérêt public ». L'argument américain semble donc être que, dans la mesure où le mandat de transfert des données a été délivré dans le cadre d'une enquête judiciaire, « le transfert est nécessaire pour des motifs importants d'intérêt public ». Il nous semble qu'il s'agit là d'une lecture erronée du RGPD. La dérogation relative aux « motifs importants d'intérêt public » prévue dans l'article 49 ne renvoie nullement à l'appréciation de ce qui constitue un tel motif pour un pays étranger. Une telle lecture serait d'ailleurs absurde, car n'importe quel pays pourrait alors arguer de l'existence d'un « motif important d'intérêt public » pour mettre la main sur les données personnelles des Européens. La dérogation en question se réfère, en réalité, au droit en vigueur dans l'Union Européenne. Elle signifie qu'un transfert des données personnelles vers un pays tiers qui ne se fonde pas « sur une base juridique en vigueur dans l'UE, […] entraînerait une violation de la législation de l'Union européenne en matière de protection des données ».[23] Le RGPD lui-même explique, sans ambigüité, ce point dans son considérant 115.[24] L'argument du gouvernement américain ne peut donc être retenu. La conclusion est que si Microsoft obtempérait et donnait suite au mandat américain lui demandant de livrer les données d'un Européen stockées en Europe sans passer par les voies juridiques prévues par le RGPD, Microsoft violerait tant le RGPD que la législation nationale du pays concerné. Ceci l'exposerait à des poursuites civiles et pénales et au risque d'une amende administrative qui, pour ce motif, pourrait s'élever, selon l'article 83§5 du RGPD, à 20 000 000 EUR ou à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent. Une décision de la Cour Suprême en faveur du gouvernement américain exposerait donc non seulement Microsoft, mais aussi tous les ISP situés tant aux Etats-Unis qu'en Europe à d'inextricables conflits de lois. A moins que… les ISP trouvent les moyens de priver d'effets la décision de la Cour Suprême.

25. Une balkanisation de l'internet ?

Considérant qu'il est préférable d'éviter de se voir infliger des amendes allant jusqu'à 4% du chiffre d'affaires mondial par les autorités de contrôle européennes (ou de se voir infliger des amendes similaires aux Etats-Unis) les ISP pourraient adopter des stratégies destinées à contourner la décision de la Cour Suprême. Comme expliqué supra, la Cour Suprême ne pourra adopter une décision en faveur du gouvernement que si elle retient l'argument de ce dernier, à savoir que seul est pertinent « l'endroit d'où les données sont accessibles ». Or, pour éviter l'applicabilité de ce critère, il suffira de développer des solutions techniques pour que les

données ne soient plus accessibles par l'ISP en dehors du pays où elles sont stockées. Ceci se fait déjà d'ailleurs, de façon anticipée, dans certains pays. En Allemagne, Microsoft a imaginé un mécanisme de « data trustee », fondé sur des ententes commerciales qui permettent de confier à un tiers la responsabilité de ses data centers afin de se protéger contre toute procédure juridique venant de l'extérieur. Microsoft a ainsi ouvert des data centers à Frankfurt et Magdeburg puis a confié à T-Systems le soin d'en être le « data trustee » et de contrôler tout accès aux données qui y sont stockées. Juridiquement donc, Microsoft « n'a pas accès » à ces données depuis les Etats-Unis car seule T-Systems a l'autorité légale de divulguer les données qui sont stockées dans ces data centers.[25] IBM a récemment repris cette idée tout en imaginant un montage différent mais qui aboutit au même résultat : ce qui se fait en Allemagne (en termes de données) reste en Allemagne – et son Cloud n'est pas accessible au personnel d'IBM en dehors de l'Europe.[26] D'autres ISP envisagent aujourd'hui de crypter les données dans les data centers européens et de confier les clés aux clients qui seraient donc les seuls capables de déchiffrer leur données personnelles et d'y accéder. Les solutions techniques ne manquent donc pas pour priver de tout effet le critère de « l'endroit d'où les données sont accessibles ». On pourrait alors se demander à quoi servirait une décision de la Cour Suprême favorable au gouvernement. A la limite, elle pourrait se révéler contre-productive en incitant, entre autres, à un chiffrement généralisé des données dans le Cloud, ce qui serait évidemment préjudiciable à l'activité des autorités judiciaires des pays. Une telle décision pourrait aussi nourrir un mouvement extrême de cyber-protectionnisme et de « data localisation », bien expliqué dans l'étude de The Chertoff Group[27], marqué par une « nationalisation » non seulement du stockage des données mais aussi des fournisseurs de stockage. Le mouvement de « balkanisation » de l'Internet qui pourrait en découler ne ferait, en réalité, les affaires de personne : ni des autorités publiques, qui pourraient avoir beaucoup plus de difficultés qu'aujourd'hui à accéder aux « preuves dans le cloud » ; ni des fournisseurs de cloud et des acteurs de l'Internet, dont le business model pourrait être affecté ; ni des individus pour qui le développement continu de « grandes murailles numériques » porterait atteinte à ce qui profondément fait la force de l'internet.

26. Conclusion

Une « victoire » du gouvernement dans la bataille juridique contre Microsoft devant la Cour Suprême pourrait n'être qu'une « victoire à la Pyrrhus ». *Tout le monde* devrait en sortir perdant, y compris les Etats-Unis et leurs entreprises technologiques. Plutôt que de persister dans des voies risquées et unilatérales, les Etats-Unis et tous les Etats devraient s'engager dans la recherche de solutions *multilatérales* à ces problèmes transnationaux, solutions qui sont les seules capables de trancher le nœud gordien de l'accès aux preuves dans les nuages.

IV. Quelles solutions ?

27. A la recherche d'un régime juridique nouveau.

Si la Cour Suprême rejetait, sur la base des éléments présentés dans la partie II de cette étude, la demande du gouvernement américain, ceci éviterait certaines conséquences négatives évoquées en partie III. Mais un tel rejet ne résoudrait pas les difficultés auxquelles sont confrontées les services de police et de justice dans l'accès aux données et preuves numériques (§7). Des solutions compatibles avec le droit international et la protection des droits de l'homme doivent donc être recherchées pour permettre aux services de l'ordre et à la justice de remplir leurs missions. La grande question est de savoir quel pourrait être ce régime juridique. La réponse à cette question est particulièrement complexe et dépasse largement les objectifs de cette étude. Nous souhaiterions, néanmoins, avancer quelques idées pour montrer qu'il existe bel et bien des alternatives aux solutions unilatérales prônées par le gouvernement américain devant la Cour Suprême. Nous commencerons par une réflexion globale sur les critères qui devraient être pris en compte pour construire la substance de ce régime juridique (§28) avant de consacrer quelques réflexions (§29-32) aux mécanismes et procédures qui pourraient être actionnés.

28. Autour de quels critères construire ce régime juridique ?

Il est impératif pour les Etats de mener une réflexion approfondie sur les types des données et les critères autour desquels un régime juridique cohérent pourrait être construit. Premièrement, il convient de se demander si ce régime juridique ne devrait pas être différencié en fonction des types de données recherchées lors des enquêtes pénales. Le problème, comme nous l'avons vu (§4), ne se pose pas de la même façon pour les « données relatives aux abonnés » et les « données relatives au contenu » - et il est impératif de faire aussi entrer dans l'équation les « données relatives au trafic » (ou « metadata »). Deuxièmement, il apparaît assez évident que ni le critère avancé par Microsoft devant la Cour Suprême (celui du « lieu de stockage » des données), ni -et encore moins- le critère du « *lieu d'accessibilité des données* » avancé par le gouvernement américain, ne suffisent à construire un régime juridique satisfaisant. D'autres critères devraient entrer dans l'équation, ce qui permettrait de replacer l'individu au centre de la réflexion. Ainsi, *la nationalité du propriétaire des données* et *le lieu où réside/se trouve le propriétaire des données*, devraient être des critères importants dans la construction de ce régime juridique. Il est vrai que ces critères peuvent être difficiles à établir au début d'une enquête pénale – dans la mesure où des malfaiteurs pourraient utiliser des techniques de *spoofing* et « cacher » leur identité, adresse IP ou le lieu d'où ils opèrent. Mais très souvent ceci n'est pas le cas et ces

critères pourraient alors trouver toute leur importance. D'autres critères pourraient aussi inclure le lieu du siège du fournisseur de services ou de son sous-traitant ; le pays où un fournisseur de services dans le cloud offre ses prestations ; l'importance de l'activité du fournisseur de services dans ce pays ; ou encore la législation de l'Etat dans lequel le suspect s'est abonné à un service.[28] Dans tous les cas, le régime juridique construit autour des types de données et de ces critères devrait introduire des « checks and balances » pour éviter les abus et intégrer la protection des droits de l'homme.

29. Des lois nationales pour résoudre des problèmes de droit international ?

Tournons-nous maintenant vers les processus qui pourraient soutenir de telles solutions. On pourrait, tout d'abord, s'interroger sur l'opportunité de solutions qui ne seraient portées que par des lois nationales. D'un point de vue opérationnel, les Etats pourraient souhaiter favoriser cette voie dans la mesure où elle est plus rapide que les mécanismes du droit international et leur permet de préserver leur autonomie. Le problème, néanmoins, est « qu'il faut être deux pour danser le tango ». Adopter unilatéralement des lois qui affectent la compétence et la souveraineté d'autres pays ne permettra de résoudre pratiquement aucun des problèmes évoqués dans la partie III de cette étude. Lors des procédures devant les juridictions américaines, beaucoup de discussions ont tourné autour de l'introduction récente, devant le Congrès américain, de la loi « ICPA » (§8). Même Microsoft a suggéré que cette loi « permettrait de résoudre les problèmes ». Il est toutefois permis d'avoir un avis plus nuancé. Sans pouvoir entrer dans une analyse de cette proposition législative qui se trouve au tout premier stade de son examen par le Congrès et dont le processus d'adoption pourrait prendre des années, il suffit ici de noter ses caractéristiques principales. L'ambition de la loi ICPA est de combler les lacunes de la loi SCA en donnant clairement une portée extraterritoriale à un mandat similaire à celui délivré dans l'affaire *Microsoft Ireland*. La loi ICPA essaie, néanmoins, d'atténuer les risques d'atteinte à la souveraineté des Etats (ou, plus exactement de certains Etats qui devraient figurer dans une liste jointe à cette loi) où sont stockées les données en prévoyant que l'obligation pour les ISP de fournir des données à l'administration américaine ne s'imposerait que si les autorités du pays en question ont reçu une notification à cet effet et n'ont pas objecté au transfert des données (généralement dans un délai de 14 jours). Il s'agit, donc, juridiquement, d'une procédure internationale de consentement tacite instaurée de façon unilatérale par les Etats-Unis. La loi prévoit, d'ailleurs, des dérogations à cette procédure, y compris si un Juge américain « *determines that the interests of the United States in obtaining the information outweigh the interests of the qualifying foreign government in preventing the disclosure* ». Même si cette loi ICPA constitue

une évolution par rapport à ce qui est demandé par le gouvernement à la Cour Suprême, elle risque de créer de nombreux problèmes parmi ceux évoqués en partie III. Ceci montre les limites d'une solution passant par l'adoption de lois nationales : les Etats-Unis ne peuvent pas imposer leur loi – ni les procédures de consentement tacite qui y figurent- aux autres nations, tout en se réservant le droit de ne pas respecter la volonté des autres nations chaque fois que le Juge américain le considère nécessaire. Ce genre de choses ne peut se faire qu'en passant par les mécanismes du droit international : négociation et concertation entre les pays et conclusion (d'une façon plus ou moins formelle) d'accords internationaux pour résoudre les problèmes. Les procédures de consentement tacite prévues par la proposition de loi ICPA ne pourraient avoir d'effectivité internationale, ni éviter les conflits de lois que si elles étaient acceptées par les autres pays et si elles comportaient un élément de réciprocité. Le droit international semble donc incontournable. Trois solutions (qui pourraient par ailleurs se combiner) pourraient alors être envisageables.

30. Une amélioration des MLATs ?

Dans un rapport détaillé sur la question, le « Groupe de travail sur les preuves dans le cloud » du Conseil de l'Europe conclut que « l'entraide judiciaire reste le principal moyen d'obtenir des éléments de preuve électroniques auprès de juridictions étrangères pour les utiliser lors de procédures pénales sur le territoire national ».[29] Un premier moyen de renforcer l'entraide judiciaire serait d'améliorer les accords bilatéraux d'entraide judiciaire, les fameux MLATs (§18 et 22). Ces accords sont souvent accusés d'être peu efficaces pour l'obtention de preuves électroniques. Selon une étude du Comité de la Convention sur la Cybercriminalité (T-CY)[30], les délais de réponse à une demande d'obtention de telles preuves peuvent aller de six à 24 mois. Bon nombre de demandes et donc d'enquêtes sont abandonnées de ce fait et « ceci pénalise l'obligation positive des gouvernements de protéger la société et les personnes contre la cybercriminalité et d'autres crimes impliquant des preuves électroniques ». Le Comité a ainsi adopté une série de recommandations visant à rendre le processus plus efficace. Des études académiques ont, par ailleurs, formulé d'importantes suggestions en vue de leur amélioration. Toutefois, tous les observateurs pointent les limites du système des MLATs . Le nombre de demandes d'entraide judiciaire pour accéder à des données augmente de façon spectaculaire d'année en année. Comme s'interroge le Groupe de travail du T-CY : « Est-il réaliste d'envisager que le nombre de demandes d'entraides judiciaires adressées, reçues et traitées puisse être multiplié par cent, mille ou dix mille ? Les gouvernements ont-ils la capacité d'augmenter considérablement les ressources disponibles pour assurer un traitement efficient des demandes d'entraide judiciaire au niveau des autorités centrales compétentes, mais aussi des tribunaux locaux et des services de poursuite et de police où les

demandes sont préparées et exécutées ? ».[31] Par ailleurs, si la solution ne devait venir que des accords bilatéraux d'entraide judiciaire, il faudrait… 18528 MLATs pour traiter le problème au niveau des 193 pays de l'ONU ![32] Il est donc évident que les MLATs ne sont pas une panacée.

31. L'invention d'un nouveau type d'accords : des MLATs aux DSAs ?

Une deuxième solution, qui pourrait être combinée à la première, pourrait être d'initier un nouveau type d'accords : les « Data Sharing Agreements » (DSAs) dont le seul objectif serait de faciliter l'accès des services de l'ordre aux communications et preuves numériques – tout en prévoyant des garanties suffisantes, tant substantielles que procédurales, en matière de droits de l'homme. L'an dernier, la presse a annoncé que les Etats-Unis négociaient avec le Royaume-Uni un tel accord.[33] Peu d'informations ont filtré sur le contenu de cet accord mais il semblerait que celui-ci pourrait autoriser les autorités du Royaume-Uni à obliger les ISP situés sur le territoire des Etats-Unis à fournir des données personnelles visées par une enquête pénale. Une telle demande ne pourrait toutefois concerner que les ressortissants de pays tiers – et non les données d'un ressortissant ou résident permanent américain pour lesquelles le Royaume-Uni serait toujours dans l'obligation de passer par le MLAT en demandant ces données aux autorités américaines elles-mêmes. On ne sait pas, par contre, si cet accord DSA est soumis à une condition de réciprocité (avec les mêmes garanties pour les ressortissants britanniques). Dans tous les cas, et quelles que soient pour l'instant les interrogations que ce projet d'accord soulève[34], y compris en matière de garanties de protection des droits de l'homme, on peut imaginer que ce précédent sera suivi attentivement par la communauté internationale et que d'autres pays pourraient se lancer dans la négociation de tels DSA. Le problème, néanmoins, est que la piste bilatérale connaît, ici aussi, ses limites. La même règle mathématique que pour les MLATs s'applique, exigeant la conclusion de 18528 DSAs pour traiter le problème au niveau des 193 pays de l'ONU (à moins de supposer que seuls les DSAs avec les Etats-Unis auraient un intérêt pratique). Il est donc nécessaire de trouver des solutions plus rapides pour mettre en œuvre des DSAs efficaces. A cet égard, l'Union Européenne est actuellement en train de travailler sur un nouveau paquet législatif intitulé « e-evidence » dont l'objectif est, précisément, de faciliter l'accès aux preuves numériques entre les pays de l'UE.[35] On pourrait imaginer que si ce projet devait aboutir, la prochaine étape pourrait être la conclusion d'un DSA entre les Etats-Unis et l'UE – DSA qui devrait inclure des garanties en matière de droits de l'homme[36] et de « protection équivalente ».

32. Un Protocole à la Convention de Budapest ?

Last, but not least, les Etats pourraient envisager de résoudre ces questions par la conclusion d'une seule convention internationale multilatérale. Dans la mesure où le problème est urgent et concerne tous les Etats, la négociation d'une convention à vocation universelle sur l'accès aux preuves numériques semble être une solution logique : nul besoin de conclure 18528 accords, un seul suffit ! Mais la conclusion d'un tel accord universel semble, pour l'heure, totalement irréaliste. Les divergences, controverses et méfiances entourant les questions cyber/data sont si importantes entre les Etats que la conclusion d'un tel accord international semble impossible. En revanche, il est beaucoup plus réaliste d'avancer rapidement dans certains cadres multilatéraux où des progrès très importants ont déjà été accomplis par les Etats. Nous pensons, plus précisément, aux pays parties à la Convention de Budapest de 2001 sur la cybercriminalité. Cette convention lie déjà 56 pays, y compris les Etats-Unis et un très grand nombre de pays de l'UE et du Conseil de l'Europe. Elle est, d'ailleurs, en train de prendre une nouvelle dimension avec son acceptation progressive par certains pays d'Amérique latine et d'Afrique mais aussi Israël et le Japon. Le Comité créé par cette convention a récemment institué un Groupe qui porte, peut-être, le nom le plus poétique de toutes les institutions internationales : « Groupe sur les preuves dans les nuages ».[37] Ce Groupe a conduit des travaux intéressants sur la question et se trouve au centre de l'initiative annoncée en juin 2017[38] par le Conseil de l'Europe concernant la conclusion d'un protocole à la convention de Budapest sur les preuves dans le cloud, protocole qui permettra de résoudre une grande partie des difficultés évoquées dans notre étude. Les négociations pour la conclusion de ce protocole devraient durer « au moins deux ans et demi » - mais rien n'empêche les Etats d'accélérer le processus pour faire face aux besoins urgents signalés par leurs services de justice et de police.

33. Conclusion.

Le droit international offre aux Etats différentes possibilités leur permettant de trouver des solutions mutuellement acceptables, respectueuses de leur souveraineté et compatibles avec la protection des droits de l'homme au problème important de l'accès des services de justice aux preuves numériques lors d'une enquête pénale. Les Etats ont le choix entre un unilatéralisme hasardeux et la voie multilatérale qui a montré son efficacité à maintes reprises dans l'histoire du droit international.

Abréviations

ICPA : International Communications Privacy Act (proposition de loi américaine)

ISP : Internet Service Providers (fournisseurs de service internet et cloud)

MLAT : Accord d'entraide judiciaire (Mutual Legal Assistance Treaty)

RGPD : Règlement général sur la protection des données de l'UE (GDPR en anglais)

SCA : Stored Communications Act (loi américaine de 1986)

Références

[1] *Par exemple, les Parties à la Convention de Budapest ont soumis 227.962 demandes en 2015 aux fournisseurs de services américains de premier plan (Apple, Facebook, Google, Microsoft, Twitter et Yahoo) et ont reçus des données (au moins partielles) dans environ 67 % des cas. La très grande majorité des demandes et surtout des divulgations concerne des « données relatives aux abonnés ». Voir Rapport final du « Groupe de travail sur les preuves dans le cloud » du Comité de la Convention sur la cyberscriminalité du Conseil de l'Europe, T-CY (2016)5, 16 septembre 2016, p. 30.*

[2] *Par une ordonnance de référé du 24 janvier 2013, le tribunal de grande instance de Paris a ordonné à Twitter de communiquer les données d'identification des auteurs de messages racistes ou antisémites. Alors que Twitter avait soutenu qu'il ne pouvait pas le faire car les informations en question « étaient stockés aux États-Unis », le Tribunal a insisté sur le fait que Twitter avait l'obligation de les produire car il ne s'agissait que de données relatives à des abonnés, qui étaient des français résidant en France, soumis selon le droit français et les propres règles d'utilisation de Twitter à la loi française. Dans une communication au Conseil de l'Europe* **la France** *a précisé que, si elle considèrait avoir un titre pour demander des données techniques/ déclaratives,* **« les demandes de contenus ne sont possibles que par demande de coopération judiciaire internationale ».** *Voir Cybercrime Convention Committee (T-CY) Cloud Evidence Group, Application of Article 18.1.b Budapest Convention on "production order": Compilation of replies to the questionnaire, 18 February 2016, T-CY(2015)22), p. 15.*

[3] *Dans une telle hypothèse pourrait-on, par exemple, envisager une présomption selon laquelle les données sont conservées dans le pays où le crime est commis ?*

[4] *Cf., entre autres, U.S. Government reply to Microsoft's brief in opposition of cert, p.4.*

[5] *https://www.congress.gov/115/bills/s1671/BILLS-115s1671is.pdf*

[6] *U.S. Government reply to Microsoft's brief in opposition of cert, p.4.*

[7] *Ibid., pp. 1-2.*

[8] *T. Christakis, « «Nécessité n'a pas de Loi» ? Rapport général sur la nécessité en droit international », in La nécessité en droit international, colloque de la Société française pour le droit international, Paris, Pedone, 2007, pp. 9-62.*

[9] *Propos de Brigitte Stern, cités in Jean Salmon (ed.), Dictionnaire de droit international public, Bruylant, 2001, p. 211.*

[10] *Amicus brief from computer and data science experts*

[11] *Voir par exemple: https://blogs.office.com/en-us/2017/10/27/delivering-a-faster-and-more-responsive-outlook-com/?eu=true qui explicite que : "if you are in Europe when setting up your account, your email will be stored in Europe". Pour les données "business" voir https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located qui précise*

[12] *https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2017/02/Magistrate-Judge.pdf p. 21.*

[13] *Amicus brief from the Republic of Ireland, p. 1.*

[14] *Letter by Viviane Reding, then Vice President of the European Commission Justice, Fundamental Rights and Citizenship, 24 June 2014 https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2017/02/Scan-Ares-MEP-int-Veld-.pdf*

[15] *Amicus brief from MEP Jan Phillip Albrecht, pp.7-8.*

[16] *https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2017/08/Second-Circuit-Majority-Opinion.pdf , p. 42, notre traduction.*

[17] *Sarah Cortes, "MLAT Jiu-Jitsu and Tor: Mutual Legal Assistance Treaties in Surveillance", 22 Rich. J.L. & Tech. 1, 26 (2015)*

[18] *Voir https://www.state.gov/documents/organization/180815.pdf*

[19] *https://www.congress.gov/110/crpt/erpt13/CRPT-110erpt13.pdf*

[20] *Selon les Etats-Unis : "[MLATS] generally address the production of records located in the requested State". Cité in https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2014/12/DigitalRightsIreland-AmiciBrief.pdf, p. 16.*

[21] *De toute façon, la « générosité » en question ne pourrait pas concerner les données de contenu localisées sur le sol américain car la loi SCA y fait obstacle. Les Européens ne pourraient pas ainsi espérer y accéder sans passer par les procédures des MLATs avec les Etats-Unis. Il n'y aura donc aucune « réciprocité » dans ce domaine et on glissera au contraire vers une asymétrie juridique dans les relations transatlantiques.*

[22] *Supra, note 4, p.8*

[23] *Comme l'avait déjà souligné le Groupe de Travail « Article 29 » sur la protection des données dans son Avis 05/2012 sur l'informatique en nuage (adopté le 1er juillet 2012).*

[24] *« Certains pays tiers adoptent des lois, des règlements et d'autres actes juridiques qui visent à réglementer directement les activités de traitement effectuées par des personnes physiques et morales qui relèvent de la compétence des États membres. Il peut s'agir de décisions de juridictions ou d'autorités administratives de pays tiers qui exigent d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel, et qui ne sont pas fondées sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre. L'application extraterritoriale de ces lois, règlements et autres actes juridiques peut être contraire au droit international et faire obstacle à la protection des personnes physiques garantie dans l'Union par le présent règlement. Les transferts ne devraient être autorisés que lorsque les conditions fixées par le présent règlement pour les transferts vers les pays tiers sont remplies. Ce peut être le cas, entre autres, lorsque la divulgation est nécessaire pour un motif important d'intérêt public reconnu par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis. »*

[25] *Voir https://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/ et https://www.meritalk.com/articles/u-s-cant-touch-microsofts-overseas-data-centers/*

[26] *Voir http://www.datacenterknowledge.com/regulation/ibm-cloud-hands-german-users-control-their-data ainsi que http://www.zdnet.com/article/cloud-computing-ibm-overhauls-data-access-rules-at-euro-data-centre/*

[27] *Comme le souligne The Chertoff Group: "trends toward data localization will almost certainly accelerate, likely to the point of what one could term "extremely restrictive data localization" p.4.*

[28] *Pour une discussion de l'ensemble de ces critères voir l'excellent Rapport final du « Groupe de travail sur les preuves dans le cloud » du Comité de la Convention sur la cyberscriminalité du Conseil de l'Europe, T-CY (2016)5, 16 septembre 2016.*

[29] *Ibid., p. 42.*

[30] *https://rm.coe.int/16802e726d p. 45.*

[31] *Rapport final du Groupe de travail sur les preuves dans le cloud, supra note 27, p. 13.*

[32] *Le calcul est à nous, mais pour l'idée voir P. Swire, J. D. Hemmings, "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program", 71 N.Y.U. Ann.Surv. Am. L. 687, 738 (2016).*

[33] *https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html*

[34] *Pour une vision américaine voir https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/*

[35] *Cf. https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en*

[36] *Dans son dernier Rapport sur la lutte contre la cybercriminalité, publié le 25 juillet 2017, la Commission LIBE du Parlement Européen souligne ainsi : « qu'il est nécessaire que le cadre pour les preuves électroniques contienne des garanties suffisantes concernant les droits et les libertés de toutes les parties concernées; précise qu'un tel cadre doit comporter une exigence prévoyant d'adresser en premier lieu les demandes de preuves électroniques aux propriétaires des données ou aux responsables de leur traitement, afin de garantir le respect de leurs droits, mais aussi des droits de toute autre partie concernée par les données en question (par exemple, leur droit au respect du secret professionnel et à demander réparation dans le cas d'un accès aux données disproportionné ou illicite); souligne également la nécessité de veiller à ce que tout cadre juridique protège les prestataires et toutes les autres parties contre les demandes susceptibles de créer des conflits de lois ou de porter atteinte à la souveraineté d'autres États ». http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0272+0+DOC+PDF+V0//FR , §65.on-evidence-in-the-clo-1?desktop=false*

[37] *https://www.coe.int/fr/web/cybercrime/ceg.*

[38] *https://www.coe.int/fr/web/human-rights-rule-of-law/-/cybercrime-towards-a-protocol-on-evidence-in-the-clo-1?desktop=false*

PRÉSENTATION DE THE CHERTOFF GROUP

The Chertoff Group est une société de conseil spécialisée en sécurité et en management des risques. Fondée en 2009, The Chertoff Group aide ses clients à accélérer leur croissance et à sécuriser leurs actifs en assurant des prestations de conseil en stratégie, en M&A et en management des risques.

Mettant un accent particulier sur la sécurité et la technologie, The Chertoff Group fournit une large gamme de services professionnels pour aider ses clients à chaque étape du cycle de vie de l'entreprise. L'entreprise tire parti de ses connaissances approfondies de l'environnement politique et des questions de sécurité pour élaborer et mettre en œuvre des stratégies efficaces qui permettent aux entreprises de saisir de nouvelles opportunités et de créer un avantage concurrentiel durable. Pour les organisations qui ont besoin d'un soutien en matière de sécurité opérationnelle, The Chertoff Group travaille main dans la main avec ses clients afin de mieux comprendre les menaces actuelles et d'évaluer, d'atténuer et de surveiller les dangers potentiels et les risques en évolution, afin de créer des environnements sécurisés pour leurs opérations commerciales.

Basé à Washington D. C., The Chertoff Group a des bureaux à Menlo Park (Californie) et à New York City (New York). Pour plus d'informations, visitez www.chertoffgroup.com.

PRÉSENTATION DE CEIS

Fondée en 1997, CEIS est une société de conseil en stratégie et en management des risques intervenant principalement au profit des institutions françaises et européennes et des secteurs stratégiques.

Ses missions portent à la fois sur des questions de sécurité et d'intelligence économique (conformité éthique et financière, lutte anti-fraude, pré-contentieux, risques concurrentiels…) et de sécurité numérique, tant au plan stratégique qu'opérationnel. Elle mène ainsi de nombreuses missions d'études prospectives et de conseil en matière de cybersécurité et de transformation numérique en s'appuyant sur un fort socle opérationnel dédié à la Cyber Threat Intelligence. Avec la société Diateam, CEIS a en outre cofondé en 2017 BlueCyForce, premier centre d'entrainement européen dédié à la Cyberdéfense (www.bluecyforce.com)

CEIS est par ailleurs le co-organisateur du Forum International de la Cybersécurité (FIC) depuis 2013 (www.forum-fic.com). Elle anime enfin de nombreux observatoires sur les questions de sécurité numérique (Observatoire FIC , Observatoire du Monde Cybernétique pour le compte du Ministère des Armées…).

Basée à Paris, CEIS dispose également d'un bureau européen à Bruxelles. Elle compte aujourd'hui 80 consultants ainsi qu'une vingtaine d'experts associés. Pour plus d'information, consultez le site www.ceis.eu

THÉODORE CHRISTAKIS

Théodore Christakis est professeur de droit international à l'Université Grenoble Alpes et membre Senior de l'Institut Universitaire de France (IUF). Il est directeur du Centre d'Etudes sur la Sécurité Internationale et les Coopérations Européennes (CESICE) et directeur adjoint du Grenoble Alpes Data Institute. Il est fondateur et co-responsable de l'Interest Group on Peace and Security de la European Society for International Law, membre de l'International Committee on Use of Force de l'International Law Association, membre du Comité éditorial de la Leiden Journal of International Law (Cambridge University Press) ainsi que du Conseil scientifique de la Revue Belge de Droit International et de l'Australian Yearbook of International Law. Il a été aussi durant 12 ans membre du conseil exécutif et du bureau de la Société Française pour le Droit International (SFDI). Depuis 2005 il enseigne aussi le droit international à la Paris School of International Affairs (Sciences-Po Paris).

Au cours de ces dernières années il a été professeur invité dans différentes universités étrangères et a présenté à 70 reprises ses travaux dans des conférences, colloques et séminaires internationaux dans 27 pays. Il a publié ou co-édité 9 ouvrages et il est l'auteur ou co-auteur de plus de 60 articles scientifiques et chapitres d'ouvrages. Son dernier livre constitue l'étude préparatoire à la conférence internationale cyber organisée par le gouvernement français à l'UNESCO les 6 et 7 avril 2017 (co-rédigée avec Karine Bannelier, « Cyberattaques - Prévention-Réactions : Rôles des Etats et des acteurs privés », Les Cahiers de la Revue Défense Nationale, Paris, 2017, disponible ici : https://ssrn.com/abstract=2957795)

Théodore Christakis est régulièrement conseiller et expert juridique pour des gouvernements, organisations internationales et entreprises sur des questions relatives au droit international, au droit de la cyber-sécurité et à la protection des données y compris la mise en œuvre du Règlement général sur la protection des données (RGPD). Il intervient comme consultant externe pour CEIS.

DÉCEMBRE 2017