Données personnelles Le Cloud Act : origines et conséquences

Le Cloud Act, menace pour le système européen de protection des données personnelles ou opportunité pour créer un mécanisme de reconnaissance réciproque en matière d'interception de données personnelles à l'étranger ?

La ré-application des sanctions commerciales contre l'Iran par les Etats-Unis a causé une tempête de protestations concernant l'application extraterritoriale de la loi américaine. L'adoption exprès, le 23 mars dernier, du Cloud (Clarifying Lawful Overseas Use of Data) Act, dans le cadre d'une loi budgétaire, a généré moins de commentaires mais elle a potentiellement des effets aussi importants pour les fournisseurs de services de communications électroniques implantés à la fois en Europe et aux Etats-Unis, qui vont se retrouver dans la position inconfortable de, soit ignorer un mandat d'un juge américain, soit violer l'article 48 du Règlement général sur la protection des données. Cependant, le Cloud Act contient également des éléments permettant de réels progrès en matière de coopération internationale et d'adaptation des mécanismes d'enquêtes internationales à la disposition des autorités judiciaires à la nouvelle réalité créée par l'Internet et le cloud computing.

Le contentieux USA c/ Microsoft

En décembre 2013, un juge du District Sud de New York a émis un mandat demandant à Microsoft la communication de courriels dans le cadre d'une enquête pour trafic de drogue. Le compte hotmail avait été ouvert aux Etats-Unis sur des serveurs américains puis, Microsoft constatant que l'accès à ce compte se faisait principalement à partir de l'Europe, a pris la décision conformément à ses procédures internes de le migrer vers des serveurs en Irlande et d'effacer la quasi-totalité des données de ses serveurs aux Etats-Unis. Microsoft a communiqué à la justice américaine une copie des courriels encore stockés sur des serveurs situés sur le territoire américain mais a refusé de communiquer une copie des courriels stockés sur ses serveurs en Irlande, demandant l'annulation du mandat en ce qu'il concernait les informations stockées en Irlande.

Après avoir examiné l'article 2703 Code fédéral américain[1] (United States Code ou USC) issu du Stored Communication Act (SCA) sur lequel le mandat était fondé, la juridiction de première instance a refusé d'annuler le mandat. Microsoft a fait appel de cette décision et la Cour d'Appel du Deuxième circuit a jugé, tout d'abord par un panel de trois juges en juillet 2016[2] puis une nouvelle fois en audience en banc (équivalent à peu près à une audience de l'assemblée plénière de la Cour de cassation) le 24 janvier 2017 que le mandat devait être annulé du fait de son caractère extraterritorial.

Cette décision a été prise sur la base de la jurisprudence de la Cour Suprême concernant l'extraterritorialité du droit américain[3] qui demande tout d'abord de vérifier si la loi prévoit qu'elle s'applique hors du territoire américain (ce qui n'était clairement pas le cas) et, dans le cas contraire, si l'espèce impliquait une application locale de la loi, ce qui n'était pas le cas selon la cour d'appel puisque les données étaient situées en Irlande et concernaient un ressortissant irlandais.

La cour d'appel est cependant très claire sur le fait qu'elle ne fait qu'appliquer la jurisprudence de la Cour Suprême et que l'actualisation qu'elle considère nécessaire du SCA est du ressort du Congrès. Malgré l'intervention du Gouvernement d'Irlande et de M. Jan Philipp Albrecht au nom du Parlement européen, aucune mention n'est faite du droit communautaire de la protection des données et la Cour d'appel refuse de considérer le cas sous l'angle de la notion de privacy et du Quatrième Amendement de la Constitution américaine (qui énonce le droit des citoyens

d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées et étendues), se tenant à une stricte interprétation de l'article 2703 du USC. La Cour d'appel rejette en revanche très clairement la théorie de l'absence de territorialité des données électroniques[4], qui considère que les données situées dans le cloud, du fait de leur stockage dans de multiples serveurs, de leur extrême mobilité et de l'absence de contrôle de l'utilisateur sur leur localisation ne peuvent pas être considérées comme des objets physiques auxquels les règles classiques de conflit de loi et de juridiction peuvent s'appliquer. Ce rejet ne peut qu'être approuvé, en particulier au vu du mouvement actuel de reterritorialisation de l'Internet, que ce soit par des moyens juridiques tels que le RGPD ou techniques, tels que la « *Grande Muraille de Chine* » qui permet au gouvernement chinois de contrôler l'information entrant dans la partie chinoise de l'Internet.

Le gouvernement des Etats-Unis a fait appel de cette décision devant la Cour Suprême, arguant que Microsoft étant une société américaine qui pouvait accéder aux données stockées en Irlande très facilement, le mandat pouvait être respecté par des actions ayant lieu aux Etats-Unis, les actions ayant lieu hors des Etats-Unis n'ayant pas à être prises en compte du moment qu'une action locale avait lieu. Au cours de l'audience publique qui s'est tenue le 27 février 2018, les avocats du gouvernement américain, les juges et les avocats de Microsoft sont tous convenus qu'il serait préférable que le projet de loi amendant l'article 2703 du Code fédéral américain soit rapidement adopté, ce qui a été fait dans le cadre d'un cavalier budgétaire signé par le Président Trump le 23 mars 2018. Suite à cette modification de la loi, la Cour Suprême, avec l'accord des parties, a considéré le contentieux sans objet et s'est donc abstenue de statuer.

Le Cloud Act

Le Cloud Act réforme plusieurs aspects du chapitre 121 du US Code consacré aux communications électroniques et par câble enregistrées et à l'accès aux enregistrements des transactions[5]. Il étend effectivement aux données stockées hors du territoire des Etats-Unis les dispositions du chapitre 121 du US Code permettant à une autorité gouvernementale américaine d'ordonner à un fournisseur de services de communications électroniques de préserver, sauvegarder et communiquer le contenu de communications électroniques, ce qui tranche le débat porté devant la Cour Suprême par le contentieux Microsoft.

Il convient tout d'abord de rappeler qu'un tel accès ne peut être accordé, pour les données stockées depuis moins de 180 jours, que par mandat pris après une décision de justice, mais sans information préalable de l'utilisateur. Pour les données stockées depuis plus de 180 jours, cet accès peut se faire également grâce à un mandat sans information préalable de l'utilisateur mais également avec une information préalable de la personne concernée dans le cadre d'une subpoena administrative ou judiciaire ou après une injonction d'un tribunal si l'autorité gouvernementale demanderesse démontre qu'il existe des motifs raisonnable de croire que le contenu de la communication électronique sont essentiels et concernent une enquête pénale. L'accès par les autorités de police américaines à des données électroniques stockées chez un fournisseur de communications électroniques est donc très fortement encadré et toujours soumis à une autorité judiciaire ou à l'information de la personne concernée.

Le Cloud Act prévoit ensuite une procédure spéciale permettant aux fournisseurs de services de communication électronique de contester la demande de communication qui lui est faite s'il estime raisonnablement que le client n'est pas un ressortissant ou un résident américain et que cette communication créerait un risque sérieux de violation des lois d'un Etat avec lequel les Etats-Unis ont conclu un « *Executive Agreement* ». Seuls les ressortissants d'Etats ayant conclu un Executive Agreement avec les Etats-Unis peuvent bénéficier de la protection limitée que peuvent leur offrir leurs fournisseurs de communications électroniques, en utilisant le mécanisme de contestation prévu par l'article 2703.h du chapitre 121 du US Code. En l'absence d'un tel accord, à la date des présentes entre la France ou l'Union européenne et les Etats-Unis, les fournisseurs de services de télécommunication donc obligés de communiquer les données de leurs clients français et européens qu'ils stockent sur leurs serveurs, sans en informer les personnes concernées si le gouvernement américain dispose d'une décision de justice à cet effet.

Le conflit entre les lois américaines et les blocking statutes

Le conflit entre l'extraterritorialité des procédures américaines et la préservation de la souveraineté et des droits des ressortissants européens n'est pas nouveau. Dès 1968, la France a voté une loi[6] interdisant à « *toute personne de demander, rechercher ou de communiquer, par écrit, oralement ou sous toute autre forme, des documents ou renseignement d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci* ».

Toute violation de cette disposition est punie de peines allant jusqu'à six mois de prison et d'une amende de 18.000 €. Cette loi a pour objet de faire obstacle aux procédures de discovery américaines et au contournement des mécanismes de coopération judiciaire prévus par la convention de La Haye du 18 mars 1970. Elle a cependant été très peu appliquée. Dans une décision qui a fait l'objet d'une certaine publicité du fait de son rattachement à l'affaire Crédit Lyonnais/ Executive Life[7], la Cour de cassation a confirmé une amende de 10 000 € infligée à un avocat français qui avait cherché à recueillir des renseignements à la demande d'une autorité administrative américaine.

Deux décisions de première instance[8] et une décision de cour d'appel[9] ont également fait application de cette loi, mais sans prononcer de condamnation. En 1987, la Cour suprême a jugé que la procédure de la convention de La Haye était un moyen parmi d'autres d'obtenir des preuves et que les parties à un

procès aux Etats-Unis pouvaient collecter des preuves à l'étranger par d'autres moyens[10]. Dans cette décision (prise à une faible majorité de cinq juges contre 4), l'opinion de la majorité de la Cour n'a pas évoqué le problème posé par la loi de 1968, mais les juridictions inférieures avaient explicitement écarté le risque qu'elle posait pour la partie française, en notant qu'elle ne semblait pas avoir fait l'objet d'aucune application en France. Plusieurs juridictions fédérales inférieures ont également estimé que le risque de sanctions en France était trop faible pour faire obstacle à l'application des règles américaines de procédure civile[11]. Il faut dire que la Convention de La Haye n'est pas d'un maniement aisé pour les juridictions américaines puisque « *tout Etat contractant peut, au moment de la signature, de la ratification ou de l'adhésion, déclarer qu'il n'exécute pas les commissions rogatoires qui ont pour objet une procédure connue dans les Etats de Common Law sous le nom de 'pre-trial discovery document'* » (article 23). En France, l'exécution des commissions rogatoires en cas de pre-trial discovery n'est autorisée que si les documents sont limitativement énumérés dans la commission rogatoire et ont un lien direct et précis avec l'objet du litige.

Dans les années 1990, avec la forte augmentation des échanges internationaux de données grâce à l'Internet puis au cloud computing, les juridictions américaines ont émis un nombre croissant d'injonctions de e-discovery, demandant à des sociétés implantées aux Etats-Unis de communiquer des données situées sur leurs serveurs situés en Europe ou concernant des personnes physiques européennes.

Avec la réforme de 2004[12] de la loi de 1978, suite à la directive de 1995[13], le problème a commencé à être examiné non plus uniquement sous l'angle de la loi de 1968 mais également sous l'angle du droit Informatique et libertés, le transfert de données personnelles vers les Etats-Unis demandé par les juridictions américaines constituant effectivement un nouveau traitement de données et un transfert hors de l'Union européenne pour lequel les personnes concernées n'ont ni été informées ni donné leur consentement. Dans un Working Paper en date du 11 février 2009[14], le Groupe de l'article 29 a considéré qu'un transfert de données dans le cadre d'une procédure de discovery pouvait être légitimé par trois justifications possibles : le consentement de la personne concernée (qui doit être libre et pleinement éclairé, ce qui le rend très rare), le respect d'une obligation légale par le responsable de traitement (étant rappelé que le respect d'une loi non communautaire ne constitue pas une telle obligation légale) ou l'intérêt légitime du responsable de traitement, sous réserve que cet intérêt ne porte pas atteinte aux droits et libertés fondamentales de la personne concernée (il convient de rappeler que tous les Etats membres de l'Union européenne ne sont pas partie à la convention de La Haye).

Dans tous les cas, la personne concernée doit avoir été informée de la possibilité de ce traitement, pouvoir exercer ses droits d'accès et d'opposition et les données transférées doivent être adéquates, proportionnelles et sécurisées. Le transfert ne peut avoir lieu que si le destinataire américain a signé un accord de transfert de données sur la base des clauses types de la Commission de Bruxelles, adhère au Safe Harbour (désormais le Privacy Shield) ou a conclu des règles internes d'entreprise. Une demande formulée dans le cadre de la convention de La Haye peut cependant justifier une exemption des trois moyens d'encadrement du transfert de données mentionné ci-dessus, puisque cette demande est nécessaire à la constatation, la sauvegarde ou la défense d'un droit en justice.

Dans une délibération du 23 juillet 2009[15], la Cnil a strictement encadré les possibilités de transfert de données vers les Etats-Unis dans le cadre des procédures judiciaires, en imposant que non seulement la convention La Haye soit respectée, le préambule de la recommandation précisant que « *en l'absence de respect de cette procédure en France, les injonctions émises par les autorités américaines concernant des preuves localisées en France sont donc irrégulières* », mais également que la loi Informatique et libertés soit respectée dans ce cadre : la personne concernée doit être informée et pouvoir exercer son droit d'opposition à ce transfert, les données collectées doivent être adéquates, pertinentes et non-excessives au regard des finalités du traitement, la durée de conservation doit être limitée... La Cnil considère cependant que dans le cas d'un transfert unique et non-massif d'informations pertinentes, l'exception concernant la constatation, la sauvegarde ou la défense d'un droit en justice peut justifier de ne pas encadrer le transfert de données par les trois mécanismes cités ci-dessus. En revanche, en cas de transferts massifs et répétés de données, ce transfert doit être autorisé par la Cnil et être encadré.

Le RGPD a réitéré cette interdiction de transférer des données hors du cadre des mécanismes de coopération internationaux, en disposant, dans son article 48 que : « *Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable de 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 Etat membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre.* »

Cette interdiction fait partie des manquements au RGPD les plus lourdement sanctionnés, et expose donc les fournisseurs de services de communications électroniques qui respectent un mandat américain émis en application du Cloud Act à des sanctions égales à 4% de leur chiffre d'affaires mondial ou 20 millions d'euros.

La conciliation entre les deux dispositions n'est cependant pas totalement impossible

Lors de l'audience de plaidoirie devant la Cour suprême des Etats-Unis du 27 février 2018, M. Dreeben, Deputy Solicitor General qui représentait le gouvernement des Etats-Unis, en réponse à une question

du juge Helena Kagan, a laissé entrevoir un moyen pour les fournisseurs de communications électroniques de concilier leurs obligations européennes et américaines. Selon lui, il est essentiel que les juridictions américaines puissent émettre des mandats concernant les communications électroniques situées hors de l'Union européenne mais la question de la contradiction avec une législation étrangère doit être analysée au moment de l'analyse des sanctions du non-respect du mandat.

La décision de 1958[16] citée par le représentant du gouvernement américain à l'appui de son argumentation concernait une demande d'une société suisse, I.G. Chemie, de restitution d'actifs confisqués par le gouvernement américain pendant la Seconde guerre mondiale à la société allemande I.G. Farbenindustrie, la société suisse prétendant avoir été le propriétaire des actifs au moment de leur confiscation. Le gouvernement américain contestait cette demande et accusait la société I.G. Chemie de ne pas être indépendante de I.G Farbenindustrie.

A cette fin, il demandait à ce qu'I.G. Chemie produise un certain nombre de documents bancaires suisses de nature à établir cette absence d'indépendance. La société I.G. Chemie a produit certains documents mais a refusé de produire tous les documents demandés au nom du secret bancaire suisse, soutenu par son gouvernement. Suite à ce refus, la District Court puis la Cour d'appel ont rejeté la demande de restitution d'actifs d'IG Chemie. La Cour suprême a condamné ce rejet, jugeant que lorsqu'il était établi qu'une partie n'a pas respecté une injonction du fait de son incapacité à le faire, sans qu'aucune faute ne puisse lui être reproché, elle ne pouvait être sanctionnée de ce fait et que la crainte de poursuites pénales constituait une réelle incapacité à produire des pièces, même si ces poursuites n'étaient pas américaines. En suivant le raisonnement du gouvernement américain, il semble donc possible qu'un fournisseur de service de communications électroniques puisse refuser de respecter un mandat ordonnant la communication de données situées en Europe et échapper à toute sanction du fait de ce refus aux Etats-Unis, en particulier si l'article 43 du RGPD est réellement appliqué. Cependant, au vu de l'ancienneté de l'arrêt cité par le représentant du gouvernement américain et de la sévérité des sanctions applicables en cas de « *contempt of court* », il semble probable que peu d'entreprises choisissent une telle stratégie.

Le texte du Cloud Act offre cependant une autre possibilité de concilier les législations européennes et américaines, qui serait de plus dans l'intérêt des gouvernements européens. En effet, l'un des aspects les plus ambitieux du Cloud Act est la création d'une procédure permettant aux autorités américaines et étrangères d'accéder à des données électroniques stockées à l'étranger sans utiliser les mécanismes de coopération judiciaire, jugés non sans quelques justifications comme trop lourds et trop lents pour les données électroniques. La conclusion d'un Executive Agreement tel que mentionné dans le Cloud Act requiert tout d'abord que l'Attorney General des Etats-Unis, conjointement avec le Département d'Etat américain, certifie que les lois du pays avec lequel ce traité doit être conclu offrent une protection robuste substantielle et procédurale du droit à la vie privée et des libertés civiles au vu de la collecte de données et des activités des gouvernements étrangers qui seront soumis à cet accord. Il serait assez étonnant que le droit de l'Union européenne et/ou de ses Etats membres ne respecte pas ce critère, tous les pays de l'Union européenne étant signataires de la convention de Budapest sur la cybercriminalité.

L'Attorney General doit ensuite certifier que ce pays a pris des mesures pour minimiser l'acquisition, la rétention et la communication de données concernant les ressortissants américains et que les termes du traité ne créent aucune obligation pour les fournisseurs de services de communication électroniques de décrypter les données (ou limitation de leurs éventuels droits de décrypter les données). Finalement l'Attorney General doit certifier que le gouvernement étranger ne peut pas viser intentionnellement des ressortissants américains, utiliser cette procédure pour fournir au gouvernement américain que ce dernier ne pourrait pas légalement obtenir sur son territoire national, qu'un mandat étranger ne peut concerner que des crimes graves, doit identifier des personnes spécifiques, être soumis au contrôle d'une autorité judiciaire, être pour une durée limitée, ne pas pouvoir être utilisé pour enfreindre la liberté de la presse… Les conditions proposées par le gouvernement américain dans le Cloud Act pour permettre aux autorités judiciaires étrangères, dans le cadre d'actions pénales, d'accéder à des données stockées sur le territoire américain semblent globalement raisonnables et il semble possible, pour les Etats européens de négocier avec les Etats-Unis un accord conforme aux principes de l'article 6 de la convention européenne des Droits de l'Homme et au RGPD. En cas de conclusion d'un tel accord, la communication des données par les fournisseurs de services de communications électroniques au gouvernement américain serait conforme au RGPD, puisqu'effectuée dans le cadre d'un traité d'entraide judiciaire, la base juridique du traitement serait le respect d'une obligation légale à laquelle le responsable de traitement est soumis et la base juridique du transfert de données un motif impérieux d'intérêt public, la seule obligation additionnelle pour les fournisseurs serait une révision de leurs politiques Informatique et libertés informant les utilisateurs que leurs données peuvent être transférées aux autorités américaines en application de ce traité, ce que de nombreuses politiques mentionnent déjà.

De plus, la conclusion d'un tel traité répondrait aux besoins des forces de l'ordre européennes, qui ont beaucoup plus d'intérêt à bénéficier d'un accès aux données stockées aux Etats-Unis que les forces de l'ordre à bénéficier d'un accès aux données stockées en Europe, au vu de la disproportion entre le poids des entreprises américaines de communications électroniques et celui des entreprises européennes.

Il convient finalement de rappeler que confrontées à un cas comme le cas Microsoft, les juridictions françaises ordonneraient probablement la transmission des données stockées

à l'étranger à un fournisseur français de services de télécommunications électroniques. S'il n'existe à la date des présentes à notre connaissance aucune jurisprudence identique, la Cour de cassation a jugé que « *les officiers de police judiciaire, agissant sur commission rogatoire du juge d'instruction ou sur autorisation du juge des libertés et de la détention, peuvent faire procéder par des opérateurs de téléphonie français à l'interception de communications émises à partir de téléphones mobiles étrangers ou situés à l'étranger sans violer les règles de compétence territoriale et de souveraineté des Etats lorsque lesdites interceptions ne nécessitent pas l'assistance technique d'un autre Etat* »[17], ce qui ressemble quand même fortement au dossier Microsoft. Les juridictions américaines ne sont donc pas les seules à avoir des tentations extraterritoriales.

Les communications électroniques et le stockage des données hors de leur juridiction constituent un enjeu majeur pour les autorités judiciaires de tous les pays du monde. Au vu de la rapidité de leur transfert et de leur effacement, la convention de La Haye est un outil totalement inadapté aux besoins légitimes des enquêtes des forces de police. Le Cloud Act offre un moyen pour les autorités judiciaires des Etats-Unis et de l'Union européenne, qui sont malgré tout les États de droit et les démocraties les plus avancées au monde, d'avoir accès aux informations stockées sur le territoire de leurs partenaires. Les Etats-Unis proposent des critères encadrant l'accès aux données stockées sur leur territoire qui répondent aux règles de base des États de l'Union européenne (contrôle du juge, minimisation des données, sécurité, protection de la liberté de la presse...) et peuvent être conciliés avec le RGPD. Il serait dommage que le climat actuel des relations transatlantiques empêche les États membres de l'Union européenne de saisir cette occasion pour négocier un traité réciproque permettant à leurs autorités judiciaires d'accéder légalement aux données stockées aux Etats-Unis.

Marc LEMPÉRIÈRE
Avocat associé
Cabinet ALMAIN

Notes

(1) *18 U.S.C. § 2703*

(2) *Microsoft Corp v United States, 829 F.3rd 197 (2d Circuit 2016)*

(3) *Morrison v National Australia Bank Ltd, 561 U.S. (2010) et RJR Nabisco Inc v European Community, 136 S. Ct. 2090 (2016)*

(4) *Jennifer Daskal, The Un-Territoriality of Data, 125 Yale L.J 326, 390 (2015)*

(5) *18 USC Ch 121 : Stored Wire and Electronic Communications and Transactional Records Access*

(6) *Loi n°68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.*

(7) *Cass. Crim, 12 déc 2007, n°07-83228*

(8) *TGI Nanterre, ref. 22 décembre 1993, Juris Data n°1993-050136 et T.com Paris, 20 juillet 2005, JurisDAta n°2005-288975, cités par Frédéric Echenne dans « Les lois de blocage françaises et les contraintes législatives extraterritoriales US », Village de la Justice, 20 octobre 2016*

(9) *CA Versailles, 16 mai 2001, JCP E 2007, 2330*

(10) *SOCIETE NATIONALE INDUSTRIELLE AEROSPATIALE and Societe de Construction d'Avions de Tourisme, Petitioners v. UNITED STATES DISTRICT COURT FOR the SOUTHERN DISTRICT OF IOWA, 482 U.S. 522*

(11) *Adidas (Canada) Ltd v. SS Seatraint Bennington, WL 432, S.D.N.Y, 30 mai 1984 et IN re Vivendi Universal, WL 3378115, SDNY, 16 novembre 2006*

(12) *Loi n°2004-801 du 6 août 2004*

(13) *Directive 95/46 CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*

(14) *Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, 00339/09/EN WP 158*

(15) *Délibération n°2009-474 du 23 juillet 2009 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédure judiciaires américaines dites de « Discovery »*

(16) *Société Internationale v Rogers, 357 U.S. 197*

(17) *Cass. Crim, 28 mars 2017, n°16-84853*