ARTICLE

LA LOCALISATION TERRITORIALE DES DONNÉES : QUELLES RÉALITÉS POUR QUELLES GARANTIES ?

IT et données personnelles ANNULE - Concurrence, régulation européenne et FDI Contrats commerciaux et internationaux | 15/10/14 | Florence Chafiol

L'affaire PRISM a suscité de nombreuses inquiétudes quant à la sécurité des données personnelles dans le Cloud. Entre localisation territoriale des données et renforcement des garanties, les gouvernements peinent à trouver des solutions pérennes alors que des outils existent déjà. Par Florence Chafiol (photo de gauche) et Mathilde Gérot, Avocats August & Debouzy.

1 - Les conséquences de l'affaire PRISM

Suite aux révélations de l'ancien employé de la CIA et de la NSA, Edward Snowden, relatives au programme américain de surveillance PRISM, de nombreux Etats – dont des Etats membres de l'Union Européenne – ont tenté de répondre aux inquiétudes de leurs citoyens face aux soupçons d'utilisation massive et dissimulée par les services de renseignement américains des données à caractère personnel générées par ces derniers sur Internet.

Parmi ces Etats, la Russie a adopté cet été une loi qui impose aux sociétés de l'Internet, russes ou étrangères, à compter du 1er septembre 2016, d'implanter leurs serveurs en Russie, dès lors que transitent par ces derniers des flux de données à caractère personnel d'utilisateurs russes.

Des initiatives similaires ont été par ailleurs lancées par certains opérateurs de télécommunication tels que l'allemand Deutsche Telekom, qui a ouvert son propre Data Center en Allemagne et lancé la campagne « *E-mail made in Germany* ». En Suisse, le leader des opérateurs de télécommunication Swisscom, a construit un Data Center sur le territoire et vante aux internautes suisses la sécurité des données qui y sont stockées en garantissant leur conservation exclusive sur le territoire.

Dans la même veine, le gouvernement français a décidé en 2011 de subventionner la création de services d'hébergement de données sur le territoire. C'est ainsi que les sociétés Numergy et Cloudwatt, qui proposent des services de cloud public, garantissent le stockage et le traitement des données en France. Afin de mettre en avant le haut niveau de sécurité garanti par sa solution, Cloudwatt se qualifie de « cloud public souverain ».

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a quant à elle publié le 30 juillet 2014 une version non définitive et soumise à commentaires d'un référentiel dont l'application semble limitée à l'Etat et à ses administrations régaliennes et qui contient des exigences et des recommandations à destination des prestataires de services de cloud et dont le champ d'application reste à définir. Ce référentiel indique en particulier que « *le stockage et le traitement des données doivent être opérées en France* ».

Au-delà des arguments politiques sur le thème de la souveraineté, se pose alors la question de savoir si la localisation sur le territoire des utilisateurs des données à caractère personnel qui les concernent est de nature à leur garantir une plus grande sécurité ainsi qu'une plus grande protection de leurs droits ou si ces initiatives de localisation sur un territoire donné ne sont en réalité qu'un « effet de mode » à l'efficacité contestable.

2 - Les écueils d'une localisation territoriale des données

L'affirmation selon laquelle la localisation des données sur le territoire dans lequel opère un prestataire de services de cloud constitue une garantie de sécurité des données stockées est sujette à caution.
En effet, on peut tout d'abord imaginer que certains gouvernements, peu respectueux des droits fondamentaux tels que les libertés individuelles, la liberté d'expression et la vie privée, en profitent pour accroître leur contrôle sur les activités en ligne de leurs citoyens (une telle crainte peut par exemple s'exprimer face au décret n° 72/2013/ND-CP adopté par le gouvernement vietnamien pendant l'été 2013 qui impose aux fournisseurs d'accès à Internet de conserver au Vietnam une copie de l'ensemble des données des internautes vietnamiens afin de permettre aux autorités de les consulter si nécessaire). On constate également que certains Etats démocratiques, dans un but légitime de protection nationale, s'arment de lois tendant à rendre possible l'immixtion dans les systèmes d'informations d'entités publiques et privées. Ce fut le cas en France avec la loi de programmation militaire n°2013-1168 du 18 décembre 2013 qui étend de manière significative et sans le contrôle d'un juge, les modalités d'accès aux données qui avaient été créées par la loi de 2006 relative à la lutte contre le terrorisme. A l'instar du Patriot Act aux Etats-Unis, ce type de mesures est susceptible d'altérer durablement la confiance des utilisateurs dans le Cloud Computing et plus largement dans le numérique. Or, comme l'a rappelé le Conseil National du Numérique, « l*a confiance est le socle sur lequel construire la société et l'économie numériques* ». On peut par ailleurs s'interroger sur la conformité de la localisation territoriale des données à la Directive 95/46/CE du Parlement européen et du Conseil qui énonce dans son préambule que « (…) *l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7 A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à*

caractère personnel puissent circuler librement d'un Etat membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardées » et que « (…) *le renforcement de la coopération scientifique et technique ainsi que la mise en place coordonnée de nouveaux réseaux de télécommunications dans la Communauté nécessitent et facilitent la circulation transfrontalière de données à caractère personnel* ».

Ensuite, même si cette question reste à ce stade hypothétique, on peut également s'interroger sur la légalité d'une telle solution face aux principes de la libre prestation de services et de la concurrence libre dans le cas où un Etat membre de l'Union Européenne décidait de rendre obligatoire le stockage des données de ses ressortissants sur son territoire.

L'efficacité d'une telle solution en termes de sécurité est en tout état de cause largement remise en cause par le fait que même si le contenu d'une messagerie électronique ou un document est stocké sur le territoire d'un Etat ayant opté pour la localisation nationale, les données et en particulier les emails transiteront toujours par les réseaux de fibre optique. Or, toutes les interceptions de données effectuées par les agences de surveillance américaines et révélées lors de l'affaire PRISM ont été réalisées via les réseaux de fibre optique. Ainsi, les données contenues dans ces emails restent vraisemblablement toujours susceptibles d'interception. En outre, il est très peu probable que la localisation nationale des données soit de nature à faire obstacle aux attaques des hackers.

Enfin, l'impact économique de la localisation nationale des données est à considérer avec attention. Certes, les investissements nationaux pourraient s'en trouver stimulés, mais qu'en est-il du coût de la construction de telles infrastructures ? Le coût du recours à un prestataire de services de cloud augmentera nécessairement, mettant en difficulté les petites et moyennes entreprises dont le budget limité constituera certainement un obstacle à l'acquisition de tels services. A n'en pas douter, certains opérateurs renonceront par ailleurs à investir dans l'ensemble des pays qui auront opté pour une localisation nationale des données de leurs citoyens. On doit même s'interroger sur le modèle des « *Cloud souverains* » qui auront d'autant plus de mal à s'internationaliser pour assurer leur compétitivité en raison de leur approche « *localiste* ».

3 - Le renforcement des garanties apportées en termes de sécurité, seule solution

Face à ces réactions nombreuses en faveur de plus de sécurité, le Parlement européen a lui aussi réagi en proposant en mars 2014 d'amender la proposition de Règlement européen sur la protection des données à caractère personnel. L'amendement prévoit que tout responsable de traitement ou sous-traitant destinataire d'une demande de communication de données à caractère personnel de la part d'une juridiction ou d'une autorité administrative d'un pays tiers doit demander l'autorisation préalable à l'autorité de contrôle de son pays (en France la CNIL) avant toute divulgation des données (cf. proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données – Amendement 140, Article 43 bis (nouveau). Si cette mesure semble de nature à garantir plus de sécurité aux données à caractère personnel des citoyens européens, il est toutefois peu probable qu'elle permette de lutter efficacement contre les programmes de surveillance mis en œuvre par certains pays tiers.

En tout état de cause, le renforcement des garanties apportées en termes de sécurité des données doit être privilégié face à la tentation des Etats de créer des barrières virtuelles en imposant la localisation territoriale des données à caractère personnel de leurs citoyens.

L'adoption de telles restrictions serait d'ailleurs de nature à contredire la volonté du législateur européen qui plaide au contraire pour une plus grande harmonisation de la protection des données au sein des Etats membres. Le choix par la Commission Européenne de s'orienter vers un Règlement -et donc d'un texte d'application directe- en guise de futur cadre uniforme de protection des données à caractère personnel plutôt que celui d'une Directive démontre bien sa volonté de favoriser une application homogène de cette réglementation.

Cet effort d'harmonisation est également le fait de nombreux Etats qui y participent notamment au moyen de la normalisation, en encourageant les prestataires à adopter des bonnes pratiques de sécurité dans leurs infrastructures et leurs services (mise en œuvre de contrôles dédiés et de processus de suivi réguliers). A cet égard, le Sous-Comité 27 de l'Organisation Internationale de Normalisation (ISO), dont la délégation française est représentée par l'AFNOR, s'attache spécifiquement à créer des normes sur les « *Techniques de sécurité des technologies de l'information* » et en particulier les normes ISO/IEC 27001 et ISO/IEC 27002 sur le management de la sécurité de l'information, la norme ISO/IEC 27034 sur la sécurité des applications ou encore la norme ISO/IEC 27018 sur la sécurité des informations personnelles traitées par un prestataire de Cloud. Cette dernière a d'ailleurs été spécialement adoptée par 14 pays et 5 organisations internationales afin de répondre à la problématique de sécurisation des données à caractères personnel dans le Cloud. Elle prévoit un certain nombre de contrôles à mettre en œuvre par les prestataires garantissant un niveau de sécurité optimale des informations stockées et échangées dans leurs infrastructures (obligation d'information sur les lieux et la manière dont les services sont opérés, actions à mener et information de l'utilisateur en cas de failles de sécurité, audit de tiers permettant à l'utilisateur de justifier du respect du cadre légal etc.).
On constate d'ailleurs que les principaux acteurs du marché du Cloud, qu'ils soient français ou étrangers, quelle que soit leur localisation, ont recours aux certifications, faisant de ces normes internationales l'« *état de l'art* » en la matière. En d'autres termes, ce corpus de recommandations, que l'on qualifierait aisément de « *soft law »,* semble être à ce jour le seul référentiel à pouvoir garantir un niveau de protection des données idoine et évolutif pour des environnements aussi complexes que ceux du Cloud Computing.

En définitive, ce n'est pas parce qu'un prestataire est situé sur le territoire national qu'il sera en mesure de garantir un niveau de protection suffisant aux données qui lui auront été confiées par ses clients publics ou privés. Si le prestataire

de Cloud ne réalise pas les investissements financiers nécessaires permettant (i) la mise en œuvre de contrôles de sécurité, (ii) l'audit régulier de ces derniers et (iii) l'obtention de certifications, alors le mythe de la localisation des données s'avérera ainsi une bien maigre garantie pour l'utilisateur face aux risques, quant à eux bien réels, de failles de sécurité et de perte de son patrimoine informationnel.

Florence Chafiol-Chaumont, associé

Mathilde Gérot, avocat