Les Cloud Microsoft 'adoubés' par les CNIL européennes : pourquoi c'est exagéré (tribune)

La presse Internet s'est faite l'écho d'un billet posté par **Brad Smith**, le directeur juridique et vice-président exécutif de Microsoft, sur le blog officiel de Microsoft, aux termes duquel il déclare que les services Cloud de Microsoft (Azure, Office 365, Dynamics CRM et Intune) seraient conformes aux « high standards of EU privacy law ».

Au soutien de cette déclaration, Microsoft fait circuler sur le Net une lettre du 2 avril 2014 d'Isabelle Falque-Pierrotin – Présidente de la CNIL française – en sa qualité de Présidente du G29, groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales de l'Union européenne (le « G29 » ou « WP29 » pour Article 29 Working Party).

La question à laquelle les directions juridique et informatique d'une entreprise française doivent répondre est de savoir si elles peuvent **prendre cette communication marketing pour argent comptant** ?

On comprend, à travers ce billet et la diffusion de la lettre du G29, que la volonté de Microsoft est de rassurer la clientèle européenne alertée par les révélations d'Edward Snowden qui n'en finissent pas de mettre à jour l'étendue colossale, au nom de la lutte antiterroriste, de la surveillance opérée les agences de sécurité américaines des données provenant d'entreprises et d'institutions européennes. Ces révélations ont d'ailleurs conduit le Parlement européen à se saisir de la question de la violation de la vie privée, dans une résolution non législative adoptée le 12 mars dernier, aux termes de laquelle le Parlement a clairement exprimé sa défiance à l'égard du Safe Harbor auquel Microsoft a adhéré.

Pour autant, il apparaît que le contenu de la lettre du G29 dont se prévaut Microsoft **ne permet pas, contrairement à ce qu'affirme la société américaine, de conclure** que les clients Microsoft peuvent utiliser ses services et transférer leurs données librement depuis l'UE vers le reste du monde (sans distinction de pays) en toute sécurité.

Aux termes du courrier du 2 avril 2014 publié sur le blog Microsoft, le G29 indique seulement que le « MS Agreement » (i.e le contrat Microsoft remis pour signature aux clients des services Office 365, Microsoft Azure, Microsoft Dynamics CRM et Windows pour les aspects données à caractère personnel) modifié par Microsoft, « *sera conforme aux clauses contractuelles types 2010/87/EU et ne devrait dès lors pas être considéré comme des causes 'adhoc' ».*

L'absence de publication du « MS Agreement » par Microsoft interdit de savoir de quel document il s'agit et d'en connaître le contenu.

La CNIL dans son communiqué du 24 avril 2014, rappelant que le G29 n'ayant fait qu**'une « *évaluation partielle* »** du contrat de Microsoft, estime que les annexes devant décrire le transfert de données et les mesures de sécurité techniques et organisationnelles devant être mises en

œuvres par l'importateur de données devront faire l'objet d'une **vérification au cas par cas par Microsoft et ses clients** afin de veiller *« à ce qu'[elles] répondent à leurs besoins spécifiques et aux exigences légales en matière de protection des données »*.

La CNIL rappelle par ailleurs que *« l'issue positive de cette évaluation partielle ne signifie pas que le G29 considère que les dispositions contractuelles de Microsoft dans leur ensemble sont conformes avec l'intégralité des règles de protection des données de l'UE, ni que Microsoft respecte ces règles dans la pratique »*.

Ainsi, tout client français doit aller au-delà des déclarations de communication de Microsoft et vérifier que toute offre Cloud de fournisseurs, notamment américains, répond aux contraintes légales qui pèsent sur lui.

1) Est-ce que le fournisseur Cloud déclare se conformer à la loi informatique et liberté de 1978 ?

La loi informatique et libertés dispose ainsi, dans ses articles 34 et 35, que le responsable du traitement et son sous-traitant (c'est-à-dire en l'occurrence le fournisseur de Cloud) doivent prendre *« toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »*

Bien que cette obligation pèse également sur les épaules du sous-traitant, le responsable du traitement doit veiller au respect de telles mesures par son sous-traitant, par tous moyens, qui peuvent notamment consister en des audits dudit sous-traitant.

Certaines dispositions de la loi informatique et liberté s'avèrent être plus contraignantes que celles de la directive européenne 95/46/CE.

D'une part, en cas de transfert de données à caractère personnel vers un sous-traitant établi en dehors de l'UE ne bénéficiant pas d'une protection suffisante, au moyen de la signature des clauses contractuelles types de la Commission Européenne, la loi informatique et libertés impose au responsable du traitement de **déposer une demande d'autorisation préalable auprès de la CNIL**. Cette autorisation de la CNIL, qui valide au cas par cas les clauses contractuelles types signées par le responsable du traitement et son sous-traitant, conditionne le transfert des données vers ledit sous-traitant hors UE.

D'autre part, la loi informatique et liberté sanctionne civilement et pénalement le responsable de traitement en cas de non-respect de ses obligations même si leur origine se trouve dans une défaillance du fournisseur Cloud, selon le principe que le donneur d'ordre reste responsable de son sous-traitant.

Par conséquent, afin que le client français d'un fournisseur Cloud établi à l'étranger soit certain d'être en conformité avec de telles dispositions nationales et également avec le régime mis en place par la directive 95/46/CE, le fournisseur ne doit pas seulement se conformer au droit européen mais également à la loi informatique et libertés.

La conformité aux exigences européennes de Microsoft reconnue par le G29 n'est pas significative de leur conformité à la loi française, qui est la seule opposable aux clients français sur le territoire français.

2) Est-ce que le fournisseur Cloud américain est en mesure de garantir la confidentialité des données provenant de l'UE face à l'étendue de la surveillance des données européennes par les agences de surveillance américaines ?

La validation du « MS Agreement » Microsoft par le G29 **n'écarte pas la question délicate de l'accès aux données étrangères** permis par les lois américaines (Patriot Act, FISA et FAA) sans que les prestataires Cloud américains, dont Microsoft, puissent s'y soustraire, ni même en informer leurs clients. Ces lois américaines autorisent les autorités américaines à surveiller les appels et courriers électroniques de citoyens étrangers sans mandat délivré par un tribunal (FISA), élargissent considérablement les pouvoirs des autorités répressives américaines s'agissant de la collecte de renseignements à l'intérieur des États-Unis (Patriot Act) et créent un pouvoir de surveillance de masse spécialement conçu pour la captation des données des citoyens des pays étrangers et vivant en dehors du territoire des États-Unis (FAA) qui s'applique notamment aux fournisseurs Cloud. Il est fait **interdiction aux sociétés américaines**, dont les données sont collectées, **de notifier à leurs clients les requêtes** couvertes par le FISA.

Déjà en 2012, le G29, dans son opinion 05/2012 sur le Cloud Computing (WP196), avait recommandé aux entreprises européennes voulant bénéficier de services Cloud qu'il soit interdit aux responsables de traitement au sein de l'UE de divulguer des données à caractère personnel à un pays tiers lorsque cela est requis par les autorités judiciaires ou administratives de ce pays, à moins qu'ils n'y soient expressément autorisés par un accord international ou des traités d'entraide judiciaire qui sont selon lui indispensables. Dans cette même opinion 05/2012, le G29 recommandait une **évolution législative qui obligerait le prestataire Cloud à notifier à son client toute requête légale** l'obligeant à transmettre des données à caractère personnel, à l'exception des demandes relevant du secret de l'instruction en matière pénale. La CNIL, dans son communiqué du 24 avril 2014 relatif à l'évaluation partielle du contrat de Microsoft par le G29, rappelle, en conclusion de son communiqué, à tous les fournisseurs de Cloud qu'ils doivent prendre en compte cet avis afin de veiller à la conformité de leurs dispositions contractuelles avec les exigences de l'UE en matière de protection des données.

Si le G29 a effectivement validé (partiellement) le dispositif contractuel de l'entreprise Microsoft en indiquant que le MS Agreement était conforme aux clauses contractuelles types 2010/87/EU, il ne faut pas oublier que le même G29 a, concomitamment, fait savoir, dans une opinion adoptée le 10 avril 2014, que ni le Safe Harbor, ni les clauses contractuelles types 2010/87/UE, ni les BCR (Binding Corporate Rules) ne sauraient servir de base légale pour justifier le transfert de données à caractère personnel vers une autorité d'un pays tiers dans un but de surveillance massive et systématique. Le G29 a ajouté que les opérateurs Cloud pourraient **agir en contravention avec la loi européenne** si les services d'intelligence de pays tiers devaient avoir accès aux données de citoyens européens stockées sur leurs serveurs ou devaient se conformer à une requête en communication de données à caractère personnel à grande échelle.

Dans une lettre adressée le même jour à la Commission européenne, le G29 a réitéré auprès de la Commission la **caractère « *hautement nécessaire* » de l'amélioration du Safe Harbor**, en rappelant qu'en tout état de cause (et notamment en cas de suspension du Safe Harbor) les autorités de protection des données européennes pouvaient suspendre les flux de données conformément à leurs compétences nationales et européennes.

Les réserves émises par le G29 tant à l'égard des clauses contractuelles types 2010/87/UE que du Safe Harbor ainsi que, s'agissant de ce dernier, par le Parlement européen, du fait de la menace représentée par la surveillance massive des données à caractère personnel de citoyens européennes par les agences d'intelligence américaines, nuancent donc considérablement l'impact de la validation du MS Agreement Microsoft.

L'affaire publiée par la BBC sur son site Internet en date du 29 avril 2014 en est une nouvelle illustration puisqu'elle fait état de l'injonction d'un juge américain à Microsoft de remettre aux autorités américaines les données de ses clients (notamment leurs e-mails), bien que ces dernières soient stockées dans son datacenter irlandais. Les juges américains arguent que ce mandat de perquisition étant relatif aux données en ligne qui relèvent du Stored Communications Act, diffère des mandats classiques et n'est pas tenu par des limites territoriales. Microsoft a déclaré qu'elle continuerait à s'opposer à cette divulgation des données stockées à Dublin en espérant que la décision soit cassée par un juge fédéral.

3) Est-ce le fournisseur Cloud est en mesure de garantir la sécurité, le transfert, la localisation et la restitution des données ?

Dans son opinion 05/12 sur le Cloud computing du 1er juillet 2012 (WP196), le G29 a formulé des recommandations qu'une entreprise européenne souhaitant opter pour un fournisseur Cloud basé en dehors de l'Union européenne devrait prendre en compte dans son choix, que ce fournisseur ait ou non ratifié le Safe Harbor et/ou se conforme aux clauses contractuelles types 2010/87/UE :

– le **recours par le fournisseur Cloud à des sous-traitants** ne doit être rendu possible qu'après un consentement du client au début de l'exécution du contrat et à la condition que le fournisseur informe le client en cas de changement de ses sous-traitants, ajoutant qu'il devrait être prévu une obligation d'information de toutes intentions de changer de sous-traitants et la possibilité pour le client de les refuser ou de résilier librement le contrat ;

– les contrats entre le client et le fournisseur Cloud doivent fournir **la liste des lieux où peuvent être traitées les données** ;

– **l'obligation d'audit** des opérations de traitement du prestataire Cloud ainsi que de ses propres sous-traitants doit être prévue dans le contrat.

En effet, bien que les fournisseurs Cloud mettent en place de plus en plus d'actions pour rassurer la clientèle européenne, il est nécessaire de vérifier que les dispositifs contractuels mis en place prévoient des **engagements précis et transparents** en termes de sécurité, de transfert, de localisation et de restitution des données :

– le client a-t-il un pouvoir de contrôle sur le transfert des données et leur traitement ?

– le client peut-il localiser les données et le fournisseur Cloud se réserve-t-il le droit, notamment pour des raisons d'organisation, de changer la localisation de ses datacenters sans notification et acceptation préalable du client ?

– le client est-il en mesure de savoir où ses données sont réellement traitées ?

– le client a-t-il un droit de refuser des sous-traitants de son fournisseur ?

– le client dispose-t-il d'un véritable droit d'audit ou ce droit est-il limité par des modalités imposées par le fournisseur ? ce droit d'audit est-il étendu aux sous-traitants du fournisseur Cloud ?

Sans compter **la question de la réversibilité des données** à la cessation des services Cloud. Cette réversibilité est-elle aménagée sans créer de dépendance technique du client vis-à-vis du fournisseur ? Le client a-t-il l'assurance que ses données seront détruites ?

Ce n'est qu'à l'issue de ces vérifications que le client pourra déterminer que l'offre Cloud qui lui est proposée présente les garanties rappelées ci-avant et qu'il disposera d'une réelle visibilité sur le traitement de ses données.

A l'heure où de nouvelles révélations concernant les programmes de surveillance mis au point par la NSA sont publiées, il convient de **ramener l'impact de la lettre** adressée par le G29 le 2 avril dernier à Microsoft, relative à la validation partielle de ses documents contractuels types, **à sa juste valeur**.

Crédit photo : produktionsbuero TINUS / Shutterstock

En complément :

Lire notre dossier » Tout sur l'arsenal secret des espions de la NSA »