Chronique du droit des nouvelles technologies - La rubrique mensuelle ICT de Vincent Wellens

Cloud computing et protection des données à caractère personnel – vers une plus grande normalisation internationale ?

Toute entreprise, grande ou petite, dépend de l'informatique, domaine sujet à un renouvellement constant. Ces nouveautés techniques entraînent inévitablement de nouvelles questions juridiques impactant le quotidien des salariés et des employeurs. La présente rubrique, à paraître tous les mois, a pour objectif de couvrir les sujets d'actualité et les évolutions en droit des nouvelles technologies au niveau de la législation luxembourgeoise et européenne.

Le *cloud computing* est une des nombreuses innovations ayant vu le jour suite à la création de l'Internet. Il a permis de révolutionner la manière dont est traitée et stockée l'information ces dernières années. Souvent utilisé à tort et à travers, le terme cloud computing désigne «*l'accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées configurables*» (définition du *National Institue of Standards and Technology*). Ainsi, une personne peut, par exemple, accéder et stocker des données, voire utiliser une solution logicielle via Internet sur des serveurs situés à un endroit géographiquement distant.

Le fait de recourir au *cloud* présente de nombreux avantages, particulièrement pour les entreprises. Le *cloud* offre une certaine flexibilité à l'entreprise, qui peut facilement et rapidement adapter les ressources informatiques commandées auprès du fournisseur par rapport à ses besoins plutôt que de devoir investir elle-même dans des infrastructures informatiques et dans des services de développement, de support et de maintenance coûteux.

Malgré cette multitude d'avantages, il convient de noter que peu d'entreprises décident aujourd'hui d'avoir recours à des services de *cloud*. Selon un rapport Eurostat daté du mois de décembre 2014, seulement une entreprise sur cinq dans l'Union européenne a actuellement recours à de tels services. La non-utilisation s'explique, entre autres, par les risques que représente l'utilisation de services de *cloud* pour une entreprise.

Parmi ces risques, figure incontestablement celui du manque de visibilité quant à la protection des données à caractère personnel, lesquelles sont souvent traitées dans le cadre de services *cloud*. Conformément à la législation applicable – la Directive 95/46/CE, telle que transposée au Luxembourg, par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel («Loi Protection de Données») –, en cas de traitement de données à caractère personnel dans le cadre d'un service *cloud*, le client du fournisseur sera généralement considéré comme «*responsable*» du traitement, alors que le fournisseur de service sera considéré comme un «*sous-traitant*» agissant au nom et pour le compte de son client.

La quasi-totalité des obligations en matière de protection des données à caractère personnel incombant de manière générale au responsable du traitement – le client – et ce dernier n'ayant souvent pas la garantie de pouvoir les respecter lorsqu'il a recours à des services *cloud*, peu d'entreprises sont, encore à l'heure actuelle, enclines à recourir à de tels services.

Pendant longtemps, les pouvoirs publics et organisations internationales n'ont porté que peu d'attention au problème. Face à l'amplitude que prennent les risques, et au besoin de plus en plus présent des entreprises de recourir à des services de *cloud computing*, des organismes internationaux de diverse nature se sont récemment penchés sur la question.

Le Groupe de Travail Article 29 («Groupe Article 29»), a été un des premiers à prendre le pas, en publiant le 1er juillet 2002 un opinion sur le *cloud computing*, dans lequel il définit notamment les risques inhérents au *cloud* pour les données à caractère personnel, le cadre légal applicable en la matière, et donne bon nombre de recommandations (**1.**).

Plus récemment, l'Organi-sation internationale de normalisation («ISO») a publié sa norme ISO/IEC 27018 définissant des standards à respecter par les fournisseurs de services *cloud* en matière de protection des données à caractère personnel (**2.**).

Plusieurs principes énoncés dans ces deux documents se retrouvent également dans la Proposition de règlement générale sur la protection des données dont l'adoption est attendue pour 2016.

L'opinion 05/2012 du groupe article 29

Constitué d'un représentant de chacune des autorités pour la protection des données à caractère personnel des États membres de l'Union européenne, le Groupe Article 29 a rendu son opinion 05/2012 sur le *Cloud Computing* le 1er juillet 2012. Bien que cet avis ne constitue qu'un document consultatif, il ne reste pas sans conséquences sur le plan luxembourgeois, dès lors que la Commission Nationale pour la protection des Données («CNPD») en tiendra nécessairement compte lors de l'application de la Loi Protection des Données.

Les risques liés au Cloud Computing

Le Groupe Article 29 a mis en exergue plusieurs risques liées à des services *cloud* pour la protection des données à caractère personnel. Il faut tout d'abord citer le fait que les données envoyées par le client dans le *cloud* sont généralement hors de son contrôle. Ainsi, le client ne peut plus prendre lui-même les mesures nécessaires pour protéger ces données, ce qui peut se manifester par une perte d'accès, de portabilité, d'intégrité, ou de confidentialité des données, voire par la perte de toute possibilité d'intervention sur les données.

Ensuite, le Groupe Article 29 souligne un manque flagrant d'information du client quant au traitement des données réalisé par le fournisseur *cloud*. Le client n'est notamment généralement pas informé sur la chaine exacte de traitement mise en place, sur le lieu où sont effectivement traitées les données, ou sur l'éventuel transfert transfrontalier de données pouvant avoir lieu.

Pour les même raisons, la CSSF n'est pas en faveur d'un recours aux services *cloud* par les professionnels du secteur financier luxembourgeois.

L'insertion de garanties contractuelles supplémentaires

Afin de remédier à ces risques, le Groupe Article 29 recommande, en plus des dispositions contractuelles qui sont légalement requises, la mise en place d'une série de clauses permettant d'apporter plus de sécurité juridique, telles que les clauses suivantes :
- une clause précisant les instructions du client au fournisseur et le niveau de service applicable (service-level agreement - «SLA»),
- une clause précisant les mesures techniques et organisationnelles de sécurité,
- une clause stipulant que le fournisseur a ou non le droit de sous-contracter les services prestés,
- une clause imposant une obligation de restitution des données à la fin du contrat,
- une clause accordant un droit d'audit au client ou encore imposant au fournisseur de livrer de façon détaillée de l'information quant aux différents endroits géographiques où seront effectivement traitées les données du client.

Bon nombre de ces clauses deviendront par ailleurs obligatoires lors de l'entrée en vigueur de la Proposition de Règlement général sur la protection des données

Concernant les transferts de données, il est important de noter qu'en cas de déploiement du service *cloud* via des serveurs établis aux États-Unis, un pays en dehors de l'UE et sans niveau adéquat de protection de données, le Groupe Article 29 considère comme insuffisant le fait pour le fournisseur de se certifier comme adhérant aux principes du *safe harbor*. Le Groupe Article 29 conseille ainsi de recourir en plus, dans ce cas, à d'autres moyens permettant d'assurer un niveau adéquat de protection notamment par le biais de clauses contractuelles ou des *binding corporate rules* (si les échanges ont lieu à un niveau intra-groupe).

Les mesures techniques et organisationnelles de protection des données

Le Groupe Article 29 rappelle également que le client des services *cloud* doit veiller à ce que le fournisseur mette en place des mesures techniques et organisationnelles notamment capables d'atteindre des objectifs de transparence, de séparation, de portabilité, de disponibilité, d'intégrité et de confidentialité des données.

la Norme ISO/IEC 27018

L'ISO est une organisation internationale et non-gouvernementale de normalisation, dont le rôle est de produire les célèbres normes internationales «ISO», principalement dans les domaines commerciaux et industriels. Très récemment, l'ISO a joint ses forces avec la Commission électrotechnique internationale pour émettre la norme 27018 «Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII».

Celle-ci établit des lignes directrices destinées à tout type d'organisations proposant à d'autres organisations des services de traitement de l'information en tant que sous-traitant via des services *cloud*, avec une attention toute particulière à la question de la protection des données à caractère personnel. Elle est basée sur les normes ISO/IEC 27001 et 27002, qui posent des standards en matière de gestion de la sécurité de l'information et qui servent, par ailleurs, de base pour la future règle technique que devront respecter les prestataires de services de dématérialisation et de conservation dans le cadre de la loi future sur l'archivage électronique.

Il s'agit du premier standard international traitant de la question de la protection des données dans le contexte du *cloud*.

Les objectifs de la norme ISO/IEC 27018

La norme ISO/IEC 27018 poursuit 4 objectifs :
Premièrement, elle a pour fonction de servir d'outil aux fournisseurs de services *cloud* afin de veiller au respect des obligations applicables en matière de protection des données.
Deuxièmement, elle doit permettre à ces mêmes fournisseurs d'être plus transparents vis-à-vis de leurs clients, afin que ces derniers puissent réaliser une décision éclairée lors du choix de fournisseur de services *cloud*.
Troisièmement, elle doit faciliter les entrées en relations contractuelles des fournisseurs et de leurs clients.
Quatrièmement, la norme a pour objectif de fournir aux clients de services *cloud* des mécanismes d'audit afin de vérifier le respect de leurs obligations par les fournisseurs.

Afin de réaliser ces objectifs, des lignes directrices spécifiques à la protection des données sont adressées aux fournisseurs de services de *cloud computing* dans l'Annexe A de la norme ISO/IEC 27018.

Les principes de la norme ISO/IEC 27018

En termes de contrôle, d'accessibilité et de portabilité des données tout d'abord, les fournisseurs de services *cloud* sont tenus de ne traiter les données à caractère personnel que sur la seule instruction de leur client. Ils doivent ensuite s'assurer que, dans les contrats qui les lie avec leurs clients, soit prévue la mise en place de mesures minimales organisationnelles et techniques afin d'assurer la sécurité des données. Le fournisseur doit également mettre des outils à disposition des utilisateurs finaux leur facilitant l'accès à leurs données.

Le fournisseur devra en outre mettre en place une politique claire gouvernant le retour, le transfert ou la destruction de données à caractère personnel. La norme ISO prévoit également une obligation pour le fournisseur de ne dévoiler des données à caractère personnel à des autorités uniquement s'il en a l'obligation légale. Dans ce cas, il a également l'obligation d'avertir le client de cette communication.

Concernant les usages secondaires de données ensuite, le fournisseur de services *cloud* ne peut utiliser les données à caractère personnel pour ses besoins propres, et doit obligatoirement obtenir le consentement expresse du client avant d'utiliser des données à caractère personnel à des fins de marketing et de publicité. Le fournisseur de services *cloud* est encore obligé de communiquer au client les pays dans lesquels les données à caractère personnel seront traitées.

Finalement, en cas de violation de données, le fournisseur de services *cloud* est tenu de notifier ses clients. Il est en outre tenu de mettre en place une politique prévoyant notamment le délai dans lequel une telle notification doit être réalisée. Enfin, le fournisseur doit enregistrer le type, le timing et les conséquences de toute violation de données.

Les avantages de la norme ISO/IEC 27018

Le fait pour un fournisseur de services *cloud* d'adhérer à la norme ISO/IEC 27018 présente de nombreux avantages, pour lui-même mais également pour ses clients.

Concernant les clients, le fait que le fournisseur soit certifié permet tout d'abord d'obtenir plus de confort sur les plans pratiques et contractuels. Le client a ainsi plus de certitude que ses obligations propres en matière de protection des données seront respectées, sans pour autant devoir conclure un contrat exhaustif sur le plan de la protection des données.

Le client va également considérablement réduire ses coûts dans l'évaluation et la recherche d'un fournisseur fiable. Ceci est particulièrement intéressant pris dans le contexte de la Proposition de règlement sur la protection des données à caractère personnel, dès lors que ce dernier érige en obligation le fait pour le responsable du traitement de choisir un fournisseur proposant un niveau de sécurité adéquat.

En effet, dès lors qu'un fournisseur est certifié ISO/IEC 27018, le client peut considérer que celui-ci est effectivement fiable en matière de protection des données. Enfin, les clients actifs dans le secteur des assurances ou des banques pourront offrir plus de garanties à leurs régulateurs respectifs lorsqu'ils auront recours à des sous-traitants certifiés ISO/IEC 27018.

Du côté du fournisseur, les avantages de la certification sont également nombreux. Elle permet tout d'abord d'obtenir plus de transparence et de confiance par rapport aux services offerts. Elle permet également de réduire le temps des négociations contractuelles, dès lors que le fournisseur affiche a priori un certain respect de la législation sur la protection des données à caractère personnel. Enfin, en cas de prestation de services transnationales, le respect de la norme assure au fournisseur la garantie du fait qu'il agit en accord avec une partie importante des différentes législations nationales en matière de protection des données à caractère personnel potentiellement applicables. Le fait d'adhérer à la norme ISO ne remplace néanmoins pas la nécessité de respecter les lois et régulations applicables.

Conclusion

Les initiatives visant à encadrer le traitement de données à caractère personnel dans le cadre de services *cloud* commencent à fleurir au niveau international et s'ajoutent aux initiatives au niveau national (telles que la modification récente de l'article 567 du Code de commerce luxembourgeois afin de prévoir un droit pour le client d'un fournisseur *cloud* failli de récupérer ses données). Ainsi, l'Opinion du Groupe Article 29 sur le *Cloud Computing* et de la norme ISO/IEC 27018 visent généralement à affermir les obligations des sous-traitants, ce qui a pour but de rendre les responsables de traitement plus enclins à recourir à des services *cloud*, dès lors qu'ils ont plus de garanties du fait qu'ils pourront toujours respecter leurs obligations en termes de protection des données.

Cette tendance à la responsabilisation des sous-traitants s'inscrit dans la lignée du futur règlement général sur la protection des données à caractère personnel. Celui-ci contient en effet une multitude de dispositions visant à partager davantage les responsabilités en matière de protection des données à caractère personnel entre le responsable du traitement et son sous-traitant.

Vincent WELLENS (cf. portrait)
Avocat à la Cour
Partner chez NautaDutilh Avocats Luxembourg S.à r.l.
vincent.wellens@nautadutilh.com

Nicolas RASE
Associate chez NautaDutilh Avocats Luxembourg S.à r.l.
nicolas.rase@nautadutilh.com
www.nautadutilh.com