

Notre réponse à la consultation de la CNIL relative au Cloud computing

Bird and Bird tient à remercier la CNIL de lui offrir la possibilité de s'exprimer sur l'application des règles de protection des données à caractère personnel au Cloud computing, sujet qui illustre parfaitement l'émergence de nouvelles problématiques et défis liés aux évolutions technologiques et qui seront ainsi au cœur de la révision de la Directive européenne 95/46 relative à la protection des données personnelles.

*L'intégralité de la consultation de la CNIL est disponible à l'adresse suivante:
<http://www.cnil.fr/la-cnil/actu-cnil/article/article/cloud-computing-la-cnil-engage-le-debat/>*

Terminologie / abréviations:

Dans le cadre de cette consultation, la société offrant des services de Cloud computing sera dénommée « prestataire », les entreprises et administrations clientes de prestataires de Cloud seront appelées « client ».

I. Définition du Cloud computing

Le faisceau d'indices [proposé par la CNIL] permet-il selon vous de caractériser une prestation de Cloud computing ? Selon vous, faut-il compléter ce faisceau d'indices ?

Oui mais elle pourrait être complétée.

Ce faisceau d'indices permet de caractériser une prestation de Cloud Computing étant précisé que le critère de la virtualisation qui implique une abstraction des ressources et une dispersion des données nous paraît particulièrement différenciant.

Il est à noter toutefois que la Commission Générale de Terminologie et de Néologie définit le Cloud Computing comme étant le « *mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire* » et précise que « *l'informatique en nuage est une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients* ». (JORF n°0129 du 6 juin 2010 page 10453).

Il serait donc pertinent de compléter le faisceau d'indices par une référence au fait que l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients, puisque telle est la définition officielle.

II. La qualification des parties: vers une présomption de sous-traitance?

L'analyse [présentée par la CNIL 1/ le client est nécessairement responsable de traitement, 2/ le prestataire est présumé sous-traitant à moins que le faisceau d'indices ne fasse tomber cette présomption démontrant alors que le prestataire agit comme responsable de traitement] reflète-t-elle selon vous la spécificité du Cloud computing? Pourquoi?

Non.

Les incertitudes tenant à la qualification des parties (responsable de traitement ou sous-traitant) ne sont pas spécifiques au Cloud Computing, même si le recours au Cloud Computing tend à les accentuer en raison de la difficulté pour le client à assurer le contrôle effectif des moyens mis en œuvre ou encore de l'existence d'offres associées au service de Cloud computing mais détachables de la prestation globale.

Aussi, tout raisonnement sur les notions de responsable de traitement et de sous-traitant ne devrait pas être spécifique au Cloud, mais au contraire être transposable à toutes prestations, et ce, y compris pour toute présomption en faveur d'une qualification ou de l'autre.

Que pensez-vous d'un régime juridique spécifique pour les prestataires?

S'agissant des critères permettant de déterminer la qualité de sous-traitance ou de responsable de traitement du prestataire, une approche factuelle s'impose, celle-ci tenant compte par ailleurs de la réalité des pouvoirs économiques des parties, ainsi que de la nature de la prestation.

Si l'expertise du prestataire, le degré de transparence en ce qui concerne son intervention peuvent jouer un rôle dans la qualification, il apparaît, d'une part, que l'autonomie du prestataire, la capacité du client à lui imposer des instructions précises et détaillées et à assurer le contrôle de l'effectivité de leur mise en œuvre (que ce soit en raison du rapport de force économique ou en raison du caractère standardisé de l'offre) et, d'autre part, la volonté des parties ou leurs pouvoirs économiques respectifs sont plus déterminants.

Sur ces derniers critères, il apparaît que les offres de Cloud « public » placent en réalité le client dans la position d'un « consommateur » de services standardisés offerts via une infrastructure de Cloud Computing, sans que le « client-consommateur » ait un pouvoir de contrôle effectif ni même contractuel sur l'infrastructure. Dans ce cadre la qualification de sous-traitant paraît inappropriée dans la mesure où le prestataire de Cloud Computing ne se trouve pas dans un rôle de subordination vis-à-vis du « client-consommateur », ce dernier ne disposant pas de pouvoirs de direction (contrôle ou audit) sur le dispositif. La position du prestataire de services de Cloud est alors plus proche de celle des fournisseurs de service en ligne telle que prévue par la Directive européenne relative au commerce électronique.

Faut-il pour autant considérer que le prestataire de Cloud Computing puisse être qualifié de responsable de traitement ? La définition prévue par l'article 3 de la loi Informatique et Libertés, selon laquelle le responsable de traitement détermine à la fois les finalités et les moyens, ne paraît pas appropriée. En effet, cette définition va au-delà du contrôle fonctionnel des données, pour réserver la qualification à de responsable de traitement au « donneur d'ordre » lequel définit les finalités (qui ne se limitent pas aux fonctionnalités) et opte pour le recours au Cloud computing en tant que solution technique ou « moyen » de traitement. Néanmoins, la définition de l'article 3 demeure inappropriée pour de très nombreuses prestations, notamment en ce qui concerne l'externalisation, en dehors même de tout Cloud Computing. Comme indiqué ci-dessus, il ne serait ainsi pas justifié de distinguer spécifiquement les prestataires de Cloud Computing des autres catégories de prestataires sur ce point.

A l'inverse, il serait intéressant de distinguer entre les prestataires de Cloud Computing dont les services se bornent à mettre à disposition une infrastructure sans « toucher » aux données et ceux dont le cœur du service inclut une exploitation informatique des données.

En effet, les prestataires de la première catégorie s'apparentent plutôt aux fournisseurs de services en ligne (intermédiaires techniques). Pour cette raison, ces prestataires ne devraient pas être considérés comme des sous-traitants au sens de la loi Informatique et Libertés mais bien au contraire, se voir appliquer un régime spécifique aux intermédiaires techniques.

Par ailleurs, pour la seconde catégorie, si le fait de qualifier le prestataire de Cloud Computing de responsable de traitement est de nature à « soulager » le client en faisant peser directement sur le prestataire les obligations issues de la législation en matière de protection des données personnelles, une telle solution ne ferait que reporter sur le prestataire les difficultés tenant de l'inadaptation du cadre actuel aux solutions de Cloud Computing (notamment s'agissant de l'encadrement des flux internationaux de données). Ceci paraît d'autant plus pertinent que, dans le schéma envisagé par la CNIL, le client reste quant à lui responsable de traitement en tout état de cause.

De même, si le principe d'une présomption de sous-traitance devait être retenu, elle ne devrait pas pouvoir être levée par le prestataire de manière unilatérale au risque pour le client de perdre toute maîtrise sur le traitement des données effectué par le prestataire ou de contrevenir à des obligations particulières lui incombant en raison de son activité (comme par exemple les règles d'audit s'imposant dans le secteur bancaire en cas d'externalisation de prestations essentielles).

En réalité, à côté des concepts de responsable de traitement et de sous-traitant tels que définis dans la loi Informatique et Libertés, les solutions de Cloud Computing sont une invite à mieux définir le concept d'« exportateur » de données personnelles identifié par la Commission européenne dans ses décisions portant adoption de clauses-type relatives aux transferts de données en dehors de l'Union européenne. En effet, selon les clauses types, l'exportateur ne peut être que responsable de traitement : or, le concept d'exportateur pourrait être dissocié de la notion de responsable de traitement, permettant, y compris à un sous-traitant situé dans l'Union Européenne, de conclure ces contrats avec un importateur situé en dehors de l'Union Européenne (ce qui n'est pas possible en l'état actuel des définitions et clauses-types adoptées par la Commission).

Une telle redéfinition pourrait permettre, combinée à des règles d'application territoriale révisées, de réallouer les responsabilités des divers intervenants dans les traitements de données personnelles mis en œuvre dans le cadre de services de Cloud Computing mais pas uniquement.

III. Le droit applicable

Selon vous quels critères pourraient permettre de déterminer la loi applicable aux acteurs du Cloud?

Il nous semble en effet nécessaire d'assouplir les critères actuels, qui présentent l'inconvénient d'une grande complexité d'application dès lors que conformément à l'article 5 de la loi Informatique et Libertés, ils conduisent à lier la loi applicable au lieu d'établissement du client et à retenir cette même loi pour régir non seulement la prestation mais l'ensemble de la chaîne de sous-traitance quel que soit le pays d'établissement du prestataire. Dès lors que le client est établi en France, la loi Française s'applique, et cela même dans les cas où le prestataire est lui-même établi dans l'Union Européenne.

Ainsi, lorsque le client est établi dans plusieurs Etats membres de l'UE, le même prestataire voit régir sa prestation par autant de lois différentes.

Une solution permettant à la fois d'assurer le respect du cadre européenne de protection des données personnelles serait de permettre une option dans la loi applicable au service de Cloud entre la loi du Client ou celle du prestataire lorsque ce dernier est également établi dans l'UE ou dans un pays disposant d'un niveau de protection reconnu comme adéquat par décision de la Commission européenne ou encore de permettre de retenir la loi de l'Etat membre d'exécution principale de la prestation dès lors qu'il est situé dans l'Union Européenne ou dans un pays "adéquat".

Une telle solution aurait le mérite de la prévisibilité pour le prestataire et de l'unicité de la loi applicable au traitement des données dans le cadre de la prestation de sous-traitance, sans pour autant priver les personnes concernées de la protection offerte par la législation puis le Client resterait redevable vis à vis des personnes concernées des obligations de la loi du Client selon les règles actuelles.

Une autre alternative serait de permettre le jeu des mécanismes contractuels classiques, en rendant le prestataire responsable de tous ses sous-traitants successifs, le prestataire se portant garant de leur respect des obligations contractuelles. En cas de défaillance dans la chaîne, le client pourrait demander réparation au premier sous-traitant de la défaillance de ses propres sous-traitants. Si une clause de tiers bénéficiaire était stipulée, ceci serait également possible pour le tiers bénéficiaire - la personne dont les données ont été collectées - ce qui serait protecteur de ses droits au regard de la loi Informatique et Libertés.

Or, avec le nouveau modèle de clause-type relatif au transferts de données d'un responsable de traitement à un sous-traitant adopté en 2010, la mise en œuvre d'une telle clause n'est plus possible puisqu'est imposée l'établissement d'une relation contractuelle directe entre chaque sous-traitant et le client puisque les clauses-type ne sont signés par les prestataire que sur mandat du responsable de traitement. La conclusion des clauses-type a ainsi de façon paradoxale pour effet de déresponsabiliser juridiquement le prestataire en morcelant la responsabilité des sous-traitants de ce dernier. Ceci est particulièrement vrai lorsque le prestataire est établi dans l'Union européenne puisque dans ce cas, n'ayant pas la qualité de responsable de traitement il ne peut pas plus intervenir en tant qu'exportateur et le jeu des clauses type conduit à court-circuiter le prestataire, puisque les clauses doivent être signées entre le client et les divers sous-traitants du prestataire établis en dehors de l'UE.

Par ailleurs, dans un souci de cohérence et de simplification, les critères permettant de déterminer la loi applicable devrait tenir compte des règles définies par le Règlement Rome I. La réflexion sur les critères de détermination de la loi applicable gagnerait ainsi à prendre en compte les règles générales en la matière.

IV. Encadrement des transferts

1. Lequel des instruments existants

[juridiques: clauses contractuelles types, règles internes d'entreprises (ou BCR), Safe Harbor ou exceptions; techniques : recours à des « métadonnées » pour définir ou décrire une autre donnée quel que soit son support (papier ou électronique), ou encore les solutions de chiffrement homomorphe] vous semble le mieux adapté au Cloud computing?

Au regard des approches envisagées, il nous paraît opportun de dissocier les réponses en fonction des situations.

En premier lieu une solution technique devrait être privilégiée. Si des mécanismes techniques permettent de garantir le caractère illisible ou inexploitable des données traitées, il ne serait pas nécessaire pour l'entreprise d'envisager des mécanismes juridiques. En effet, s'il est par exemple possible de fragmenter des données à travers les pays de façon à ce qu'une partie d'une donnée stockée dans un pays A n'ait au aucun sens si elle ne peut pas être associée aux autres parties de cette donnée stockées dans des pays B, C, D (...), le caractère illisible ou inexploitable de la donnée placée dans chaque pays supprime le risque pour l'entreprise et ses clients de voir la donnée compromise.

Dans l'hypothèse où de tels mécanismes techniques ne pourraient être garantis, des solutions juridiques devraient alors être envisagées. Les clauses contractuelles types s'avèrent peu pratiques au regard :

- du nombre de pays qui peuvent être impliquées par le prestataire de Cloud et de la volatilité des infrastructures,
- des nombreuses formalités administratives à satisfaire,
- du temps nécessaire pour obtenir une autorisation de la part de la CNIL, et du caractère incertain de ce mécanisme dans le cadre de la révision de la Directive 95/46/CE 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.

Bien que le mécanisme Safe Harbor ne s'applique que dans l'hypothèse où l'entreprise agit sur le territoire des Etats-Unis, de nombreux acteurs publics européens ont exprimé des réserves et des questions sur le fait de recourir à des entreprises opérant depuis les Etats-Unis en raison des récents développements liés au Patriot Act. S'agissant des Pays-Bas, l'administration a indiqué qu'elle refuserait à l'avenir de recourir au Cloud Computing, dans la mesure où les services seraient fournis par des entreprises américaines.

Enfin les dérogations prévues au titre de la Directive 95/46/CE et reprises par des pays tiers pour leur législation relative aux données à caractère personnel sont trop variables dans chaque Etat Membre de l'Union et pays tiers pour constituer une base commune et unifiée de nature à assurer la fiabilité juridique des dispositifs de Cloud. A ce titre et en l'état des mécanismes actuels, des BCR sous-traitants nous semblent devoir être privilégiées (voir ci-dessus section 3).

Il faut souligner ici que les BCR sous-traitants n'apportent une solution à la question du Cloud Computing que dans la mesure où le Cloud n'est mis en œuvre qu'au sein d'un groupe, sans aucun recours à un prestataire extérieur. Ce qui de plus disqualifie les petits opérateurs et les nouveaux entrants dans le secteur des services de Cloud Computing. Au demeurant, les BCR ne sont toujours pas reconnues par les autorités de contrôle des 27 Etats Membres de l'UE.

2. Comment avez-vous encadré les transferts réalisés dans le cadre de la prestation des Cloud que vous proposez ou auquel vous avez souscrit?

3. Les BCR sous-traitants vous semblent-ils être une solution intéressante ? Quel mécanisme envisageriez-vous pour ces BCR?

Dès lors qu'une solution technique ne pourrait être assurée et qu'un mécanisme juridique s'avérerait nécessaire, les BCR sous-traitants nous semblent devoir être privilégiées. En effet, elles permettent de développer de l'intérieur et avec souplesse des mécanismes de sécurité et de chaîne de l'information harmonisés. Elles font naître un sentiment de responsabilité rendant les entreprises qui les adoptent redevables et transparentes dans leurs actions.

Ce mécanisme est en outre l'un des rares mécanismes que l'Asie (cf. récentes discussions de l'APEC) et le Nord de l'Amérique appréhendent et développent. Face à une internationalisation grandissante des échanges, ce mécanisme aurait l'avantage d'être massivement adopté ou adoptable, ceci afin de répondre le plus largement possible aux législations des différents pays impliqués.

Pour que les BCR puissent se développer correctement, il serait possible d'envisager que ceux qui en bénéficient puissent obtenir une exemption des formalités d'autorisation auprès des autorités compétentes.

Avez-vous déjà réfléchi à des solutions techniques qui permettraient de mieux identifier et contrôler les flux de données dans le cadre des prestations de Cloud?

V. Sécurité des données

Quel commentaire pouvez-vous formuler sur les relations contractuelles entre client et prestataire concernant les mesures de sécurité et le respect des articles 34 et 35 de loi informatique et libertés?

L'instrument contractuel doit demeurer un outil possible permettant au client et au prestataire de déterminer les mesures de sécurité appropriées qui doivent s'appliquer dans le cadre de leur relation. Toutefois, le contrat ne peut pas être le seul instrument, notamment dans la mesure

où le client n'a pas toujours la possibilité de négocier les clauses contractuelles.

La rédaction / mise en place de recommandations (non contraignantes) et/ou normes décrivant les mesures minimum de sécurité et de confidentialité doivent également pouvoir être mises en place.

Les prestataires qui voudraient avoir la confiance des clients devraient appliquer ces recommandations minimums.

De même la mise en place de certification et d'audits pas des organismes extérieurs devraient pouvoir garantir le respect d'un certain nombre d'exigences en matière de sécurité/confidentialité.

1. Des risques spécifiques au Cloud

Quels commentaires pouvez-vous formuler sur la recommandation de mener une analyse de risques avant le passage au Cloud?

Une analyse de risque préalable est une bonne pratique.

Toutefois, cette mesure ne devrait pas avoir de caractère contraignant pour les clients dans la mesure où les clients ne disposent pas systématiquement de l'organisation et/ou des budgets pour procéder à cette analyse. L'analyse de risque doit en outre pouvoir prendre des formes différentes selon la nature des clients (particulier, TPE/PME, grand compte, organisme public, organisme financier et/ou de santé) et les données en jeu.

2. Constats et propositions en matière de sécurité

Quels commentaires pouvez-vous formuler sur cette analyse [*points de sécurité à renforcer, obligations spécifique pour les prestataires proposant des offres à destination d'organismes publics ou de sociétés*]? Selon vous, sur quelles mesures de sécurité la CNIL devrait-elle attirer l'attention des responsables de traitement?

Quelles que soient les mesures de sécurité mises en place, il nous semble que le coût de mise en œuvre des mesures mises en place doit être proportionné à l'objectif poursuivi et à la criticité des données.

a. L'accès des administrateurs et le chiffrement

Quels commentaires pouvez-vous formuler sur le chiffrement dans le Cloud?

Le chiffrement des données stockées dans le Cloud présente l'avantage de renforcer la sécurité et la confidentialité des données. De plus, en limitant de façon certaine l'accès des administrateurs informatiques aux données, il permet de mieux définir le rôle et la responsabilité de chaque acteur du Cloud.

Cependant, il est nécessaire de relativiser les bienfaits de cette solution tant sur un plan technique (i) que sur un plan juridique (ii):

(i) La gestion d'un Cloud entièrement chiffré entraîne en effet des coûts non négligeables, ainsi qu'un alourdissement des procédures tel (notamment en ce qui concerne de simples procédures de recherche dans la base de données) qu'il a conduit certains analystes à en nier la possibilité même (Rapport de l'ENISA sur les risques du Cloud Computing, Benefits, risks and recommendations for information security : « Effectuer une recherche Internet par le biais de mots de passes chiffrés [...] entraînerait un accroissement du temps de calcul informatique par environ 1018 » soit un milliard de milliards). Par ailleurs, il est nécessaire que les prestataires ne fassent pas reposer outre mesure leurs procédures de sécurisation sur le seul chiffrement, eu égard aux lourdes conséquences qu'une mauvaise gestion du chiffrement pourrait entraîner : la divulgation ou pire, la perte de la clé de chiffrement pourrait entraîner de graves fuites ou pertes irréversibles de données.

(ii) De plus, cette solution risque de se heurter à certaines législations nationales qui soumettent l'utilisation du chiffrement à certaines restrictions (déclaration ou autorisation administrative préalable, divulgation de la clé, etc.). Des pays tels que la Chine, la Russie mais également les Etats-Unis et l'Espagne sont par exemple concernés, à des niveaux divers, ce qui augmente d'autant la difficulté de gestion d'un chiffrement plus ou moins mis en œuvre selon les pays de destination ou de transit des données.

b. La destruction des données et la réversibilité

Quels commentaires pouvez-vous formuler sur la restitution des données et la réversibilité?

La restitution et la réversibilité des données est un facteur clé du succès et du développement du Cloud Computing.

S'agissant de la réversibilité des données, la mise en place/l'utilisation de formats standards permettant de conserver l'intégrité devrait être encouragé.

S'agissant de la destruction des données, il conviendrait de modéliser/normaliser les processus de purge des données tout en tenant compte des contraintes techniques du prestataire (par exemple, le prestataire devrait pouvoir conserver des données pendant un temps raisonnable postérieurement à l'extinction du contrat en cas de mutualisation des ressources avec d'autres clients).

Approuvez-vous l'analyse de la CNIL sur l'absence de normes ou de certifications sur la protection des données personnelles dans le Cloud?

Quelles propositions de normalisation ou de certification pouvez-vous formuler à ce sujet?

S'il n'existe pas à ce jour de normes spécifiques au Cloud Computing, il existe en revanche un certain nombre de normes générales (par exemple, les normes ISO 270001 en matière de sécurité).

En toute hypothèse, l'édiction de nouvelles normes prenant en compte le Cloud Computing doit tenir compte des normes déjà existantes au niveau national ou international (notamment afin d'assurer dans la mesure du possible une cohérence avec les normes déjà existantes et permettre tant au client qu'au prestataire de savoir quelle norme doit s'appliquer) et ne peut se faire qu'avec la collaboration des acteurs du marché.

Contacts



Ariane Mole

Avocat associé

T: +33 (0)4 78 65 60 00

ariane.mole@twobirds.com

Contributeurs

Nathalie Métallinos, Julie Ruelle, Lorraine Boche, Gabriel Voisin

The content of this update is of general interest and is not intended to apply to specific circumstances. The content should not therefore, be regarded as constituting legal advice and should not be relied on as such. In relation to any particular problem which they may have readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.

twobirds.com

Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Düsseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Stockholm & Warsaw

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses. Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 15 Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.