Synthèse des réponses à la consultation publique sur le Cloud computing lancée par la CNIL d'octobre à décembre 2011 et analyse de la CNIL

1. *Définition du Cloud computing*

Dans la consultation publique, la CNIL avait défini le Cloud computing en s'appuyant notamment sur diverses définitions et sur les critères définis par le NIST[1] suite à un long travail de concertation. Les critères retenus étaient les suivants :

- simplicité d'un service à la demande ;
- extrême flexibilité ;
- accès « léger » ;
- virtualisation des ressources ;
- paiement « à l'usage ».

De plus, la consultation distinguait les services de Cloud computing selon trois modèles de services :

- SaaS : « Software as a Service », c'est-à-dire la fourniture de logiciel en ligne ;
- PaaS : « Platform as a Service », c'est-à-dire la fourniture d'une plateforme de développement d'applications en ligne ;
- IaaS : « Infrastructure as a Service », c'est-à-dire la fourniture d'infrastructures de calcul et de stockage en ligne.

En vue de l'alléger, la consultation ne portait pas sur les différents modèles de déploiement de ces services, à savoir le « Cloud public », pour un service partagé et mutualisé entre de nombreux clients, le « Cloud privé », pour un service dédié à un client et le « Cloud hybride », quand les deux modèles précédents sont combinés. De nombreuses contributions ont rappelé l'importance de ces distinctions.

La consultation ne remet pas en cause la définition du Cloud computing proposée par la CNIL. Néanmoins, quelques ajustements de vocabulaire peuvent être proposés afin de tenir compte des contributions, comme le remplacement de « virtualisation » par « mutualisation », que beaucoup ont mis en avant, et qui est en effet un terme préférable.

Si la consultation avait vocation à couvrir toutes les modalités du Cloud computing, de nombreuses réponses ont surtout pris en compte les offres de Cloud public à destination des entreprises et notamment les offres SaaS (logiciel en ligne). Les analyses des acteurs

[1] Liste de caractéristiques établie par le *National Institute of Standard and Technology*, USA, dans le document « *The NIST definition of Cloud computing* », http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

présentées dans le présent document sont donc souvent focalisées sur le cas particulier de cette modalité de Cloud computing (caractérisée par des offres standard, une certaine mutualisation, une absence d'information sur la localisation, et des contrats d'adhésion).

2. Qualification du prestataire de Cloud computing

Rappelons qu'aux termes de l'article 3 de la loi de 1978 modifiée, le responsable de traitement est défini comme la personne physique ou morale qui détermine les finalités et les moyens du traitement de données à caractère personnel. Le sous-traitant quant à lui, traite les données à caractère personnel pour le compte du responsable de traitement et selon ses instructions.

Afin d'aider les acteurs du Cloud à déterminer le rôle de chacun, la CNIL proposait la solution suivante :

- Client : il sera toujours responsable de traitement. En effet, en collectant des données et en décidant d'en externaliser le traitement auprès d'un prestataire, il est responsable de traitement en ce qu'il détermine les finalités et les moyens de traitement des données.

- Prestataire : en principe, il agit pour le compte et sur les instructions du client responsable de traitement. Dès lors, il semble possible d'établir une présomption de sous-traitance dans la relation qu'entretiennent le client et le prestataire.

Une telle présomption est particulièrement effective lorsque le client a recours à un Cloud privé, c'est-à-dire propre à un client, qui implique une grande maîtrise de la réalisation de la prestation du Cloud par le prestataire. En revanche, lorsqu'un client a recours à un Cloud public, où par nature le prestataire définit le fonctionnement et les objectifs de l'application en ligne accessible à différents clients, les rôles respectifs du client et du prestataire peuvent s'avérer difficiles à déterminer, et dépendent également du type de services souscrit par le client. La CNIL proposait donc que la présomption de sous-traitance puisse tomber en application d'un faisceau d'indices qui doit permettre de déterminer la marge de manœuvre dont dispose le prestataire pour réaliser la prestation de services.

Ce faisceau d'indices est composé des critères suivants :

1. Le **niveau d'instruction** donné par le client au prestataire : ce critère peut permettre d'évaluer dans quelle mesure le prestataire est tenu par les instructions du client responsable de traitement. Dès lors, si le client laisse une grande autonomie au prestataire dans la réalisation de sa prestation, le prestataire agira également comme responsable de traitement, sous réserve que les autres critères évoqués ci-après se réalisent également.

Exemple : Une société de cours à domiciles a recours à un prestataire afin de partager les supports de cours qu'elle propose à ses élèves. Pour avoir accès aux supports de cours, les élèves doivent s'enregistrer sur la plateforme de la société de cours à domicile.

Cette société, qui agit comme responsable de traitement, a accepté les conditions d'utilisation de la société prestataire. Le contrat de prestations de services signé entre la société de cours à domicile et le prestataire ne précise pas expressément les conditions de stockage, le volume de données stockées et le périmètre géographique de stockage des données. Le prestataire dispose donc d'une grande autonomie et pourrait à ce titre être également qualifié de responsable de traitement et non comme sous-traitant sous réserve que les indices évoqués ci-après se

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

réalisent également. En revanche, si le contrat de prestation de services est extrêmement précis et s'il s'avère que la société de cours à domicile maîtrise la réalisation de la prestation telle qu'elle l'a préalablement définie dans le contrat de service, alors la société prestataire sera considérée comme sous-traitant.

2. Le **degré de contrôle** de l'exécution de la prestation du prestataire par le client responsable de traitement : ce critère est un indicateur efficace de la façon dont le prestataire met en œuvre les instructions données par le client. Il convient en effet de s'interroger sur le degré de « surveillance » du client en tant que responsable de traitement sur la prestation de son prestataire.

Exemple : Une société cliente qui agit comme responsable de traitement ne contrôle pas le prestataire auquel elle a recours et ce dernier n'a aucune obligation de rapporter régulièrement l'état d'avancement de ses missions. Dans ce cas, le prestataire devrait également être considéré comme responsable de traitement et non comme sous-traitant sous réserve que les indices évoqués ci-après se réalisent.

3. La **valeur ajoutée** fournie par le prestataire sur le traitement des données du client : ce critère permet de savoir dans quelle mesure le prestataire maîtrise le traitement de données. En effet, plus le prestataire disposera d'une expertise approfondie dans un domaine, plus il sera à même de décider des moyens de traitement à mettre en place dans le cadre de la réalisation des prestations et sera donc susceptible d'être également qualifié de responsable de traitement.

Exemple : Un salon de coiffure utilise une application de consultation et d'édition de documents en ligne pour gérer son fichier clients : à ce titre, il est responsable de traitement, puisqu'il détermine les finalités du traitement (gestion de son fichier client) et les moyens de traitement (recours à un prestataire). Toutefois, lorsque les données sont transférées au prestataire qui fournit cette application, ce dernier en maîtrise les conditions dans lesquelles il réalise la prestation de services qui lui est confiée par le client. Il semble donc que dans ces conditions le prestataire puisse également être considéré comme responsable de traitement et non comme sous-traitant, sous réserve que les indices évoqués ci-après se réalisent.

4. Le **degré de transparence** sur le recours à un prestataire : ce critère pourra donner une indication quant à la qualification du prestataire. En effet, si l'identité du prestataire est connue par les personnes concernées qui utilisent les services du client, le prestataire pourra être présumé comme agissant également comme responsable de traitement.

Exemple : Dans le cadre de la gestion des fiches de paye des employés d'une société X, finalité pour laquelle elle est considérée comme responsable de traitement, la société X a recours aux services de stockage en ligne d'un prestataire. Lorsque les employés ont accès à l'interface sur laquelle sont placées leurs fiches de paye, il est clairement indiqué que ce service est géré par la société du prestataire. Une telle présentation constituera un indice permettant de présumer que dans une telle hypothèse le prestataire agit également comme responsable de traitement et non comme sous-traitant.

L'application de ce faisceau d'indices permettrait notamment de prendre en compte la nature particulièrement standardisée des offres de Cloud computing dont il résulte généralement une très grande maîtrise de la prestation par le prestataire.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Les contributeurs ont eu des avis partagés sur la proposition d'une présomption de sous-traitance : une moitié l'approuve, l'autre non. Les remarques formulées révèlent que la qualification du prestataire ne s'appuierait pas sur une présomption, mais dépendrait de l'offre proposée par le prestataire :

- l'analyse doit être faite en fonction de la nature du Cloud (public ou privé) et des modèles de services (IaaS, SaaS, PaaS) ;

- les critères composant le faisceau d'indices doivent être clarifiés (notion d'expertise et degré de transparence) ou ne sont pas adaptés au Cloud computing (contrats standards) ;

- la majorité des offres de Cloud étant des contrats d'adhésion, les responsables du traitement n'ont pas réellement la possibilité de négocier avec les prestataires, donc la plupart de ces derniers sont fortement susceptibles d'être responsables du traitement ;

- la coresponsabilité est source d'insécurité juridique.

Par ailleurs, les avis des contributeurs sont partagés en terme de sécurité juridique, concernant la pertinence d'instaurer une présomption de sous-traitance qui pourrait tomber en application du faisceau d'indices, et plus favorables à la proposition de créer un régime juridique spécifique aux sous-traitants.

Position de la CNIL

Lorsqu'un client fait appel à un prestataire de services, il est généralement admis que le premier est responsable de traitement et le second sous-traitant.

Toutefois, la CNIL constate que dans certains cas de PaaS et de SaaS public, les clients, bien que responsables du choix de leurs prestataires, ne peuvent pas réellement leur donner d'instructions et ne sont pas en mesure de contrôler l'effectivité des garanties de sécurité et de confidentialité apportées par les prestataires. Cette absence d'instruction et de moyens de contrôle est due notamment à des offres standards, non modifiables par les clients, et à des contrats d'adhésion qui ne leur laissent aucune possibilité de négociation.

Aussi, dans ces situations, le prestataire pourrait *a priori* être considéré comme conjointement responsable en vertu de la définition de « responsable du traitement » fournie à l'article 2 de la Directive 95/46/CE, puisqu'il participe à la détermination des finalités et des moyens des traitements de données à caractère personnel.

Afin de prévenir tout risque de dilution des responsabilités dû à la présence de responsables de traitement conjoints, ces derniers devront procéder à un partage clair des responsabilités dans le contrat de prestation qui les lient, afin d'éviter notamment que les personnes concernées ne soient affectés par la présence de responsables conjoints du traitement.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

A cet effet, la CNIL propose un tableau du partage des responsabilités entre le client et le prestataire :

Hypothèse	Formalités déclaratives	Information des personnes	Obligation de confidentialité et sécurité	Exercice des droits des personnes concernées auprès du …
Le prestataire est conjointement responsable du traitement	**Client**[2]	**Client**[3]	**Client + Prestataire**	**Client (avec le concours du prestataire)**[4]

Par ailleurs, la CNIL rappelle qu'un prestataire ne peut utiliser les données personnelles qui lui ont été confiées par ses clients que sur les instructions de ces derniers. En conséquence, un prestataire qui souhaiterait traiter des données pour d'autres finalités que celles déterminées par ses clients (un exemple courant étant la publicité ciblée) outrepasserait les instructions de ses clients s'il ne les informe pas de son intention et n'obtient pas leur autorisation au préalable. Si le prestataire obtient une telle autorisation, il sera alors responsable du traitement qu'il met en œuvre pour une finalité distincte de celle du traitement du client. Dans une telle situation, le client et le prestataire seront chacun responsables des traitements qu'ils effectuent. Aussi, il sera notamment dans l'obligation d'informer les personnes concernées de la mise en œuvre de manière d'un tel traitement, conformément à l'article 32 de la loi de 1978 modifiée.

Enfin, il est à noter que depuis la consultation publique lancée par la CNIL, la Commission européenne a publié son projet de règlement relatif à la protection des données personnelles le 25 janvier 2012, lequel instaure un régime légal du sous-traitant dans son article 26, prévoyant notamment une liste non exhaustive des éléments devant figurer dans le contrat de prestation.

Le projet de texte soumet le sous-traitant à un certain nombre d'obligations communes avec le responsable de traitement. Ainsi, le sous-traitant serait soumis aux obligations de documentation (article 28), de coopération avec l'autorité de contrôle (article 29), de sécurité des traitements (article 30), de notification au responsable du traitement en cas d'une violation de données personnelles (article 31), d'analyse d'impact (article 33), d'autorisation ou de

[2] Le client et le prestataire auront des obligations déclaratives auprès des autorités de protection compétentes concernant le traitement dont ils sont conjointement responsables. Ils devront alors déterminer qui d'entre eux effectuera ces formalités. La CNIL recommande que ce soit le client qui s'en charge, puisque le recours à un prestataire de Cloud peut s'inscrire dans un traitement plus général, mais il est tout à fait envisageable que ce soit le prestataire qui s'acquitte des formalités. Dans tous les cas, la partie en charge de ces formalités déclaratives devra être en mesure de fournir la preuve, sur demande de l'autre partie, qu'elles ont été dûment effectuées auprès des autorités compétentes.

[3] Bien que l'obligation d'information incombe à la fois au client et au prestataire tous deux responsables de traitement, il est souhaitable qu'en pratique ce soit l'entité à laquelle la personne concernée a communiqué ses données qui l'informe des moyens de traitement auxquels le prestataire a recours. Par conséquent, le prestataire doit fournir au client toutes les informations nécessaires au respect de cette obligation d'information. Toutefois, le prestataire doit rester la personne de contact à laquelle la personne concernée devra s'adresser pour obtenir davantage d'information sur le traitement pour lequel le prestataire agit comme responsable conjoint du traitement.

[4] La dissémination possible des données sur différents serveurs localisés dans divers pays peut rendre plus compliqué l'exercice de leurs droits par les personnes concernées. Il convient alors de s'assurer que le prestataire et le client mettent en œuvre les garanties nécessaires pour permettre aux personnes concernées d'exercer leurs droits d'accès, de rectification, de modification, de mise à jour ou d'effacement.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

consultation préalable de l'autorité de contrôle (article 34), de désignation d'un délégué à la protection des données (article 35) et d'encadrement des transferts (articles 40, 42, 43).

Par conséquent, la création d'un tel statut légal soumettant le sous-traitant à un nombre important d'obligations est une solution intéressante permettant de rééquilibrer la balance des pouvoirs, et donc des responsabilités.

5. Détermination de la loi applicable

La consultation posait une question ouverte aux contributeurs, afin de savoir quels critères pourraient permettre de déterminer la loi applicable aux acteurs du Cloud computing.

Une part importante des contributeurs a proposé de ne retenir que la loi du responsable du traitement pour déterminer la loi applicable. Toutefois, cette proposition écarte le critère lié aux moyens de traitement tel qu'actuellement envisagé par l'article 5-I-2° de la loi Informatique et Libertés (selon lequel la loi Informatique et Libertés est applicable lorsque le traitement est réalisé par un responsable de traitement qui n'est pas établi au sein de l'Union européenne, mais qui a recours à des moyens de traitement situés sur le territoire français), restreignant alors le champ d'application territorial de la loi française et risquant d'accentuer le phénomène de « *forum shopping* »[5] auquel les législations européennes se trouvent déjà confrontées. Par conséquent, il ne paraît pas envisageable de s'orienter vers une telle solution.

En revanche, compte tenu de la difficulté à déterminer le droit applicable en fonction du responsable du traitement, le critère du ciblage a été cité comme un critère intéressant, permettant de garantir une meilleure protection des données personnelles des individus. Cependant, les entreprises ont mis en avant que le choix d'un tel critère pourrait conduire à l'application cumulative de plusieurs droits, ce qu'elles ne souhaitent pas.

Ce critère de ciblage a d'ailleurs été retenu dans le projet de règlement, lequel prévoit son application aux responsables du traitement non établis au sein de l'Union européenne, mais qui offrent des biens ou des services à des personnes ayant leur résidence sur le territoire de l'Union (article 3 du projet de règlement).

6. Encadrement des transferts

Dans la consultation, la CNIL proposait les solutions juridiques et techniques suivantes pour encadrer les transferts de données en-dehors de l'Union européenne :

- ❖ <u>Sur un plan juridique</u>

La multiplication des lieux potentiels de stockage des données rend difficile la mise en œuvre des instruments juridiques garantissant un niveau de protection adéquat.

[5] Dans le cas présent, « *forum shopping* » désigne le fait qu'une entreprise choisisse de s'implanter dans un pays plutôt que dans un autre en considération d'avantages liés à la législation de celui-ci. Par exemple, l'absence d'autorisation préalable de l'autorité anglaise pour les transferts à destination de pays situés en-dehors de l'Union européenne pourrait inciter un groupe américain souhaitant ouvrir une filiale en Europe à choisir le Royaume-Uni.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

La CNIL propose d'une part, d'appeler les prestataires de services à intégrer les clauses contractuelles types dans leurs contrats de prestations de services, d'autre part, de réfléchir à la faisabilité de BCR[6] sous-traitants.

Ces « BCR sous-traitants » permettraient à un client du prestataire de confier ses données personnelles à ce sous-traitant en étant assuré que les données transférées au sein du groupe du prestataire bénéficient d'un niveau de protection adéquat.

- Sur un plan technique

L'encadrement des transferts pourrait également reposer sur des solutions techniques utilisées. Certains prestataires évoquent par exemple le 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.

Le recours au chiffrement pourrait également apparaître comme une solution satisfaisante pour garantir l'envoi de données vers certains pays uniquement.

Dans un tel cas, le client pourrait alors endosser véritablement son rôle de responsable de traitement en déterminant précisément, avant même la réalisation de la prestation, les pays destinataires de données.

La CNIL a interrogé les participants à la consultation publique sur la question de savoir quel est l'instrument, parmi ceux existants, le mieux adapté au contexte du Cloud computing.

Alors que les contributeurs relèvent de manière générale que les mécanismes de transferts actuels ne sont généralement pas adaptés au contexte du Cloud computing, il ressort de cette consultation que les BCR sont considérés comme l'outil le mieux adapté. Par ailleurs, la proposition de reconnaissance de BCR sous-traitants a été accueillie très favorablement par les acteurs du marché.

S'agissant du projet de règlement publié par la Commission européenne, les articles 42 (« Transferts moyennant des garanties appropriées ») et 43 (« Transferts encadrés par des règles d'entreprise contraignantes ») prévoient que les transferts de données vers des pays tiers sont possibles si le responsable du traitement ou le sous-traitant ont mis en place des instruments permettant d'offrir des garanties de protection appropriées, sous réserve d'une autorisation préalable de l'autorité nationale lorsque les instruments mis en place ne sont pas juridiquement contraignants. Aussi, le projet de règlement reconnaît expressément les BCR sous-traitants.

Par ailleurs, à la demande de prestataires, et suite à une étude de faisabilité réalisée par la CNIL en 2011, le sous-groupe BCR du Groupe de travail de l'Article 29 travaille actuellement à la rédaction d'un avis sur les BCR sous-traitant, qui devrait être publié prochainement.

[6] Binding Corporate Rules ou règles d'entreprise contraignantes

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Dans l'attente de la publication de cet avis, il est recommandé d'encadrer les transferts de données par la signature de clauses contractuelles types. Les solutions diffèrent selon la qualification et la localisation du prestataire :

- Si le client transfère les données à un prestataire de Cloud localisé hors UE agissant en qualité de sous-traitant : signature des clauses contractuelles types de 2010, qui prévoient notamment les chaînes de sous-traitance.

- Si le client transfère les données à un prestataire de Cloud localisé au sein de l'UE agissant en qualité de sous-traitant, lequel transfère lui-même les données à un sous-traitant situé hors UE : plusieurs mécanismes sont possibles (signature des clauses contractuelles types de 2010 entre le responsable du traitement et le sous-traitant hors UE, mandat ou contrat tripartites).

- Si le client transfère les données à un prestataire de Cloud localisé hors UE agissant en qualité de responsable du traitement : signature des clauses contractuelles types de 2001 ou 2004. Si le prestataire transfère ultérieurement les données de son client à un sous-traitant hors UE, deux solutions sont envisageables :

    - soit le **client** signe directement les clauses contractuelles types de 2010 avec ce sous-traitant,

    - soit le **prestataire de Cloud** signe un contrat avec le sous-traitant qui reprend les mêmes obligations que celles des clauses types de 2010, à condition qu'il soit prévu dans le contrat de prestation conclu entre le client et le prestataire de Cloud l'obligation de ce dernier de signer un contrat équivalent aux clauses contractuelles types avec tout sous-traitant.

7. Sécurité du Cloud computing

La question de la sécurité des données est centrale pour les clients recourant au Cloud computing et la consultation a confirmé la préoccupation centrale des clients sur ce sujet. En effet, en passant au Cloud computing, l'entreprise externalise les données personnelles qu'elle traite mais également d'autres données patrimoniales et stratégiques ainsi que les processus eux-mêmes. Dès lors, une panne du service de Cloud peut conduire à l'impossibilité pour l'entreprise d'avoir la moindre activité et une faille ou une fuite de données peut avoir des conséquences importantes sur son fonctionnement, vis-à-vis de ses clients et de ses concurrents.

a. Le renforcement du contrat de Cloud et les engagements de niveaux de service pour la protection des données

Si la contractualisation des conditions de sécurisation du traitement est vue comme une nécessité pour la plupart des acteurs, plusieurs acteurs en soulignent les limites dues au caractère standard des offres de Cloud computing et au constat que, de fait, le prestataire définit unilatéralement les mesures qui lui semblent pertinentes. Il semble donc nécessaire de considérer que des moyens additionnels doivent être définis pour encadrer la sécurité des traitements dans le Cloud, comme la certification du prestataire ou les audits par le client.

C'est pourquoi la CNIL a dressé la liste des dispositions minimales que le contrat doit inclure (responsabilité en cas de perte des données par exemple) et encourager la création de

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

SLAs/PLAs[7] associés au contrat et incluant des questions de protection des données. A terme, il est souhaitable que les contrats standards des prestataires incluent ces SLAs/PLAs.

b. L'analyse de risques

S'agissant de l'analyse de risques, le secteur reconnaît le caractère essentiel de cette démarche pour un client souhaitant passer au Cloud computing : les documents de l'ENISA et de la Cloud Security Alliance sont reconnus comme des outils pertinents pour une telle analyse mais devraient être complétés de la bonne prise en compte de la protection des données personnelles. C'est pourquoi la CNIL a fourni des recommandations, à destination notamment des petites entreprises qui n'ont pas nécessairement les moyens financiers et techniques de mener une analyse de risques complète. En particulier, la CNIL a identifié les risques relatifs à la protection des données qui s'appliquent généralement au Cloud computing.

c. Les mesures de sécurité

Concernant les mesures de sécurité, beaucoup de contributions ont souligné le recouvrement entre les mesures proposées par la CNIL et les mesures imposées par certaines normes de sécurité existantes, comme ISO 27001, SAS70 ou ISAE3402. Ces normes fournissent un cadre qui peut faciliter l'évaluation de la sécurité du prestataire, sans toutefois fournir de garanties absolues : il convient à chaque fois d'examiner les conditions exactes d'applications de la norme et notamment le périmètre d'activité concerné chez le prestataire. Par ailleurs, les réponses montrent que de nombreux professionnels identifient autant de facteurs de risques du côté du client que du prestataire.

d. Le recours au chiffrement

Sur le cas particulier du chiffrement qui était mis en avant par la CNIL dans sa consultation comme la façon la plus sûre pour le client de contrôler l'usage des données personnelles, les contributions des acteurs les plus impliqués dans la fourniture de services de Cloud (notamment les prestataires mais également quelques grands clients) montrent que cette solution n'est pas encore opérationnelle techniquement pour la plupart des services de Cloud computing. Seuls les services de stockage de données, type IaaS, semblent aujourd'hui éligibles à la mise en œuvre du chiffrement côté client. Pour les offres applicatives les plus répandues (SaaS), des progrès doivent encore être réalisés. En revanche, d'autres solutions, comme « l'obfuscation »[8] ou le morcellement des données sont avancées par certains acteurs mais devraient être approfondies pour déterminer leurs caractéristiques et leurs éventuels apports en termes de protection des données.

Le risque d'accès aux données par des autorités étrangères, par exemple dans le cadre du *Patriot Act* aux Etats-Unis, doit être pris en compte dans l'analyse de risques. En effet, même quand les données sont transférées sur des liens chiffrés (https ou VPN par exemple), elles restent le plus souvent traitées en clair par le prestataire de Cloud computing. Une solution pour limiter ce risque, lorsque le client a les moyens de mettre en place une gestion des clés

[7] SLA : *Service Level Agreement*, engagement de niveau de service pris par le prestataire. Les SLAs sont une pratique courante dans le cadre de prestations de service.
PLA : *Privacy Level Agreement*, déclinaison des SLA pour les questions de protection des données. Ce concept est en cours de développement, notamment au sein de la *Cloud Security Alliance* (CSA). La CNIL participe aux travaux de la CSA sur les PLAs.
[8] Anglicisme désignant une procédure destinée à rendre une information difficile à comprendre

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

adéquates et qu'il utilise un algorithme reconnu, est de chiffrer les données sur les terminaux du client avant de les transférer via un canal sécurisé[9]. Cette solution n'est cependant pas adaptée à de nombreux services SaaS, par exemple les services de gestion de documents en ligne, car dans ce cas le prestataire a besoin d'un accès en clair aux données pour fournir le service. En outre, l'impossibilité de réduire suffisamment le risque d'accès aux données par des autorités étrangères a déjà conduit certaines autorités de protection des données à limiter voire interdire l'utilisation de certains services SaaS[10].

e. La réversibilité (ou portabilité)

Enfin, tous les acteurs pratiquant le Cloud semblent avoir pris en compte la question de la réversibilité/portabilité, même si des progrès peuvent encore être réalisés (sur les formats et les éventuels logiciels nécessaires pour utiliser les données restituées, etc.), notamment pour les applications métier du client.

f. Les normes et certifications

En conclusion, de nombreux acteurs confirment l'analyse de la CNIL concernant le besoin de définir des références techniques sur la protection des données personnelles, notamment dans le Cloud computing. La norme ISO 27001 est régulièrement citée comme exemple pour les questions liées à la sécurité du système d'information. Il est cependant à noter qu'il s'agit d'une norme générique qui ne prend pas en compte toutes les spécificités des questions de Vie privée. Une certification ISO 27001 sur un périmètre englobant totalement la solution de Cloud est donc une référence en termes de bonnes pratiques de sécurité mais ne répond pas totalement aux besoins. Des travaux sont actuellement engagés à l'ISO pour mieux prendre en compte la problématique de protection des données, dès lors que le périmètre étudié est correctement établi. Par ailleurs, le travail de normalisation doit prendre en compte la maturité des services et, de ce point de vue, les services IaaS semblent les plus susceptibles d'être concernés par une telle démarche à court terme.

Le rôle de la CNIL sera de conseiller les responsables de traitement sur les bonnes pratiques à adopter, et de participer aux travaux de normalisation menés par le secteur. Les travaux de la CSA (Cloud Security Alliance), auxquels la CNIL participe, semblent fournir un cadre de travail reconnu par tous et pourraient inclure la question de la protection des données personnelles.

[9] Pour rappel, un canal sécurisé (https ou VPN par exemple) permet d'assurer la confidentialité des données pendant l'envoi afin de s'assurer que seul le serveur visé (ici, celui du prestataire de Cloud) puisse lire les données envoyées. Si les données sont envoyées sans avoir été préalablement chiffrées, elles seront donc lisibles par le prestataire.

[10] L'autorité norvégienne a ainsi interdit l'utilisation de Google Docs dans différents cas, notamment lorsque des données à caractère personnel sont concernées. L'autorité danoise a pour sa part interdit son utilisation lorsque des données sensibles sont concernées.

8 rue Vivienne - CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00