Consultation relative au Cloud computing

Consultation ouverte du 17 octobre au 17 novembre 2011

Fiche de présentation de la partie prenante à la consultation
(toutes les informations sont facultatives)

Nom de la société

Secteur d'activité :

Pays dans lequel se trouve l'établissement principal :

Pour le Cloud computing, vous êtes :

- ☐ **Un prestataire**

- ☐ **Un Client**

Merci de renvoyer ce document

- **par voie électronique** à consultationcloud@cnil.fr
- ou **par courrier papier à**

Commission Nationale Informatique et Libertés CNIL
Service des affaires européennes et internationales
8 Rue Vivienne
75002 PARIS.

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

A. Le Constat de la CNIL

Le terme Cloud computing étant à la fois récent et recouvrant de nombreuses notions, il n'y a pas encore de consensus pour en donner une définition précise.

B. Solution proposée

Une approchée fondée sur les éléments caractéristiques du Cloud computing nous semble ici plus appropriée.

La CNIL propose donc de retenir le faisceau d'indices suivant afin de caractériser l'existence d'une prestation de Cloud computing :

- **simplicité d'un service à la demande** : un utilisateur peut de manière unilatérale, immédiatement et généralement sans intervention humaine, avoir à disposition les ressources informatiques dont il a besoin (temps de calcul de serveurs, capacité de stockage, etc.).

- **extrême flexibilité** : les ressources mises à disposition ont une capacité d'adaptation forte et rapide à une demande d'évolution, généralement de manière transparente pour l'utilisateur.

- **accès « léger »** : l'accès aux ressources ne nécessite pas d'équipement ou de logiciel propriétaire. Il se fait au travers d'applications facilement disponibles (parfois libres[1]), généralement depuis un simple navigateur Internet.

- **virtualisation des ressources** : les ressources informatiques du prestataire sont configurées pour être utilisées par une multitude de machines et sont souvent réparties dans différents centres d'hébergements (éventuellement dans différents endroits de la planète).

- **paiement « à l'usage » :** le paiement de la prestation de Cloud computing peut s'effectuer proportionnellement à l'usage.

[1] Une application / logiciel libre est une application/logiciel dont la licence donne à chacun (et sans contrepartie) le droit d'utiliser, d'étudier, de modifier, de dupliquer, et de diffuser le dit logiciel. Il existe également des systèmes d'exploitation libres comme LINUX.

C. Question posée

Ce faisceau d'indices permet-il selon vous de caractériser une prestation de Cloud computing ? Selon vous, faut-il compléter ce faisceau d'indices ?

Réponse

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

A. Le principe

Aux termes de l'article 3 de la loi de 1978, 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.

B. Solution proposée

1. Le client

Le client 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.

2. Le prestataire

En principe, le prestataire 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 sera particulièrement effective lorsque le client aura recours à un Cloud privé[2] qui implique une grande maîtrise de la réalisation de la prestation du Cloud.

En revanche, lorsqu'un client a recours à un Cloud public[3], les rôles respectifs du client et du prestataire peuvent s'avérer difficiles à déterminer, et dépendront également du type de services souscrit par le client. La Commission propose 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.

---

[2] Dans le Cloud privé, les ressources informatiques (infrastructure, applications, etc.) sont mises à disposition d'une seule et même organisation. Ces ressources peuvent être détenues, gérées et administrées par l'organisation elle-même ou par un tiers. Dans tous les cas, l'organisation a généralement une maîtrise sur l'infrastructure associée et la localisation des données. Lorsque l'infrastructure est partagée entre plusieurs organisations supportant une communauté précise et ayant des préoccupations communes, on parle alors de « Clouds communautaires ».

[3] Dans le Cloud public, les ressources informatiques sont exploitées par des tiers et font coexister les tâches soumises par un grand nombre de clients sur les mêmes serveurs, systèmes de stockage et autres composants de l'infrastructure. L'utilisateur final n'a généralement aucun moyen de savoir quels autres usagers sont présents sur le serveur, le réseau ou le disque sur lequel ses tâches sont exécutées.

Critère	Signification
Niveau d'instruction	Evaluer dans quelle mesure le prestataire est tenu par les instructions du client.
Degré de contrôle de l'exécution de la prestation.	Evaluer le niveau de contraintes que le client peut imposer au prestataire.
Expertise du prestataire	Evaluer le niveau d'expertise du prestataire afin de savoir dans quelle mesure il maîtrise le traitement des données.
Degré de transparence du responsable de traitement au niveau de la prestation de services.	Savoir dans quelle mesure l'identité du prestataire est connue des personnes concernées. 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.

L'application de ce faisceau d'indices permettra 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.

La CNIL soumet donc à consultation l'analyse suivante :

- le client est nécessairement responsable de traitement
-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.

Dans le cadre de la réflexion menée sur la révision de la directive, il serait intéressant de réfléchir à la création d'un statut légal pour le sous-traitant afin de faire peser sur ce dernier un certain nombre d'obligations spécifiques.

C. Question posée

L'analyse présentée ci-dessus reflète-t-elle selon vous la spécificité du Cloud computing ? Pourquoi ?

Réponse

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

Réponse

III. Le droit applicable

Le Cloud computing étant basé sur l'utilisation de multiples serveurs situés en divers points de la planète, les difficultés quant à la détermination du droit applicable sont évidentes. En effet, la flexibilité et la fluidité des transferts de données rendent potentiellement applicables autant de lois que de pays dans lesquels se trouvent des serveurs traitant les données.

Il est pourtant particulièrement important d'identifier la loi applicable, afin notamment de déterminer quelles obligations pèsent sur le responsable de traitement.

A. Le principe

Aux termes de l'article 5 de la loi du 6 janvier 1978 modifiée, la loi s'applique si le responsable de traitement :

- ✓ a son établissement sur le territoire français
- ✓ a recours à des moyens de traitement situés sur le territoire français (sans être établi sur le territoire d'un autre Etat membre)

B. Pistes de réflexion

Alors que la CNIL est favorable à une extension de la notion de moyens de traitement, elle souhaite tout de même tempérer les conséquences excessives d'une interprétation particulièrement large des moyens de traitement et une éventuelle application systématique de la loi française.

Question posée :

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

Réponse

IV. Encadrement des transferts

A. Le principe

Aux termes de l'article 68 de la loi de 1978, les données à caractère personnel ne peuvent faire l'objet d'un transfert que si l'Etat dans lequel se situe le destinataire de données assure un niveau de protection adéquat. L'article 69 de ladite loi prévoit expressément les outils permettant d'encadrer ce type de transferts : clauses contractuelles types, règles internes d'entreprises (ou BCR), Safe Harbor ou exceptions.

Le recours à ces outils **implique de connaître le ou les pays dans lesquels les données vont être communiquées, élément essentiel pour procéder aux déclarations/autorisations auprès de la CNIL et pour informer les personnes concernées des transferts vers ces pays.**

Or, le Cloud computing est le plus souvent fondé sur une absence de localisation stable des données. Le Client est donc rarement en mesure de savoir en temps réel où se trouve les données et où elles sont transférées et stockées.

Dans ce contexte, les instruments juridiques permettent d'encadrer les transferts de données vers des pays tiers n'assurant pas un niveau de protection adéquat démontrent leurs limites.

Il existe par ailleurs des exceptions au principe d'interdiction de transferts

B. Solutions proposées

(i) Sur un plan juridique

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

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 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 bénéficie d'un niveau de protection adéquat.

(ii) Sur un plan technique

L'encadrement des transferts pourrait également dépendre des solutions techniques utilisées. Certains prestataires évoquent par exemple le recours à des « métadonnées »[4] pour définir ou décrire une autre donnée quel que soit son support (papier ou électronique), ou encore les solutions de chiffrement homomorphe[5].

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.

[4] Méthode permettant de lier des informations précises aux données et notamment permettrait de déterminer le périmètre géographique sur lequel les données pourront être transférées.

[5] Moyen de chiffrement permettant au prestataire d'agréger des messages bien qu'ils soient chiffrés et sans qu'il en est connaissance.

En pratique :

- **Le prestataire de Cloud,** qu'il soit responsable de traitement ou sous traitant, devra obtenir une approbation de ses BCR par les autorités européennes de protection des données, selon la procédure actuelle.
- **Le client** effectuera sa demande d'autorisation de transferts auprès des autorités de protection sur la base des BCR du prestataire approuvés.

C. Questions posées

1. Lequel des instruments existants vous semble le mieux adapté au Cloud computing ?

Réponse

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

Réponse

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

Réponse

4. 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 ?

Réponse

VI. Sécurité des données

Les problèmes de sécurité et de confidentialité des données externalisées vers le Cloud, couverts par l'article 34 de la loi « informatique et libertés », sont en général un des premiers sujets de préoccupation des utilisateurs[6].

Dans le cas d'un organisme ayant recours à une offre de Cloud computing, **la gestion de la sécurité de ces données se trouve largement déléguée au prestataire**, pour lequel il est

[6] Dans une étude effectuée par *IDC Enterprise Panel* (Etats-Unis), à la question « *Rate challenges/issues ascribed to the 'Cloud'/on-demand model* » la sécurité apparait en tête avec 74,6% (source : présentation du NIST sur le Cloud Computing et la sécurité, disponible à l'URL : http://csrc.nist.gov/groups/SNS/Cloud-computing/Cloud-computing-v26.ppt).

souvent difficile d'obtenir des garanties sur le niveau de sécurité réel. En application de l'article 35 de la loi, le sous-traitant doit « *présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées dans l'article 34 »*[7], le responsable de traitement ayant quant à lui « *une obligation de veiller au respect de ces mesures [de sécurité et de confidentialité] ».*

De plus, le même article prévoit que « *Le contrat liant le sous-traitant au responsable de traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable de traitement. »*

Il est donc nécessaire que ces exigences en termes de sécurité se trouvent matérialisées dans un contrat. Il est notamment essentiel que les responsabilités et rôles des parties soient clairement définis au préalable, afin de traiter efficacement les cas d'incident pouvant aboutir à une perte ou une divulgation de données.

Question posée

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 ?

Réponse

1. Des risques spécifiques au Cloud

Il est recommandé d'effectuer une analyse de risques[8] préalablement à la rédaction de toute politique de sécurité, en particulier pour les systèmes d'information de taille importante. Cette recommandation a déjà été formulée par l'ENISA[9] dans son rapport paru

[7] Article 35 de la loi « informatique et libertés ».

[8] La méthode d'analyse de risque la plus utilisé en France est celle développée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI, anciennement DCSSI), dénommée EBIOS (voir à l'url : http://www.ssi.gouv.fr/site_article45.html).

[9] *European Network and Information Security Agency*

en novembre 2009 et intitulé « Cloud computing: benefits, risks and recommendations for information security »[10] et par l'ANSSI dans son rapport plus général sur « L'externalisation des systèmes d'information – Maîtriser les risques » publié le 19 mars 2010[11].

Cette analyse de risques doit notamment prendre en compte la nature de l'organisme qui utilise le Cloud et le type de données traitées dans le Cloud.

La CNIL considère donc qu'adopter une démarche d'analyse de risques pour évaluer l'impact du passage au Cloud devrait être adopté par les responsables de traitement qui souhaitent utiliser le Cloud computing pour certains de leurs traitements de données personnelles.

Question posée :

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

Réponse

2. Constats et propositions en matière de sécurité

a) Les points de sécurité à renforcer

Lors de l'utilisation du Cloud computing, la CNIL recommande d'examiner particulièrement certains aspects de la sécurité :

- **la protection externe du réseau** (pare-feu, serveur proxy avec analyse de contenu, détection d'intrusion, etc.)
- **la protection du terminal** (PC portable, assistant personnel, téléphone portable) : antivirus, système d'exploitation et des logiciels mis à jour régulièrement, firewall[12].

[10] Ce rapport identifie notamment 35 risques spécifiques au Cloud computing. L'ENISA a précisé l'analyse à réaliser dans le cas de l'utilisation du Cloud par les services publics dans un second rapport, publié en janvier 2011 et intitulé « Security & Resilience in the Governmental Clouds ». Dans ce rapport, l'ENISA fournit un guide d'analyse à destination des services publics et recommande, globalement, l'utilisation de Clouds privés, dont le rapport bénéfice/risques en matière de sécurité semble positif

[11] Notamment les risques liés à la localisation et à l'hébergement mutualisé.

- **le chiffrement des liaisons** [13] de manière à garantir la confidentialité des échanges
- **la traçabilité :** conserver un historique des connexions et des opérations effectuées[14] sur les données (en effet, dans de nombreuses offres, y compris de grandes sociétés, les évènements de type « administration » qui permettent par exemple la création/suppression de compte ou les accès aux données ne sont pas enregistrés).

Pour les prestataires proposant des offres à destination d'organismes publics ou de sociétés, on peut rajouter :

- **la gestion des habilitations** par exemple le compte d'une personne ayant quitté l'organisme doit être immédiatement désactivé car le fait qu'elle n'a plus accès aux locaux ne l'empêche pas d'accéder aux systèmes d'information.
- **l'authentification** : de même, l'authentification doit être renforcée. Le recours à une authentification forte s'avèrera nécessaire dès lors que les données accédées sont sensibles et/ou volumineuses.

Questions posées:

Quels commentaires pouvez-vous formuler sur cette analyse ? Selon vous, sur quelles mesures de sécurité la CNIL devrait-elle attirer l'attention des responsables de traitement ?

Réponse

b) L'accès des administrateurs et le chiffrement

Lorsqu'aucun chiffrement n'est mis en œuvre au niveau du stockage des données, ce qui est très souvent le cas, les administrateurs informatiques[15] du prestataire ont un accès total aux données de leurs clients[16].

[12] Ou « pare-feu » servant à filtrer les connexions entrantes et sortantes. Ici, il se présentera sous forme d'un logiciel, ou à défaut de la fonctionnalité fournie par le système d'exploitation du terminal.

[13] Par exemple en ayant recours à https (HyperText Transfer Protocol Secure) pour sécuriser la navigation.

[14] Sil s'agit d'une offre de type *IaaS*, il sera important d'activer les journaux au niveau du système d'exploitation (sécurité, système, application), et au niveau des équipements contribuant à la sécurité du réseau (firewall, IDS). S'il y a en plus des prestations de type *SaaS*, il faudra journaliser les évènements (création de compte, exports, accès en écriture/lecture) au niveau de la base de données et/ou de l'applicatif associé. De plus, l'accès aux journaux devrait être protégé en écriture et limité au minimum de personnes. Bien que généralement gérés par la société offrant le service de Cloud computing, ils devraient être accessibles (éventuellement sur demande) au client.

[15] Réseau/ système d'exploitation, base de données et application ;

Une manière de se protéger partiellement de ces risques est de s'assurer que les administrateurs du prestataire ont une clause de confidentialité dans leur contrat de travail ou ont signé un engagement en ce sens. Une traçabilité des actions d'administration dans des journaux qui ne leur sont pas accessibles est par ailleurs recommandée.

Cependant, pour le client responsable de traitement, le chiffrement des données stockées dans le Cloud constitue le seul moyen d'empêcher que les administrateurs informatiques du prestataire[17] aient accès aux données qui lui sont confiées.

Question posée

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

Réponse

c) La destruction des données et la réversibilité

Lorsque la prestation offerte par le prestataire s'achève (fermeture d'un compte, rupture de contrat, etc.) il est important pour le client de s'assurer que les données qu'il a confiées au prestataire ne sont plus accessibles à ce dernier. En fonction de la sensibilité de ces données, les mesures suivantes peuvent être exigées :

- effacement classique des données
- effacement « sécurisé» [18] des données
- restitution des supports de stockage (disques durs, bandes de sauvegarde) ou destruction physique dans le cas de matériels dédiés au client (cas des Clouds privés par exemple) ;

[16] Ce qui peut représenter une quantité très importante de données quand on pense aux dizaines de milliers de clients d'ADP ou aux millions de clients de Google pour reprendre les exemples précédents.

[17] Et donc la société de « Cloud computing » elle-même.

[18] Les données effacées à l'aide de la fonction de suppression du système d'exploitation peuvent être facilement récupérables, même une fois la corbeille vidée ou après formatage du spport. Il existe en effet de nombreux logiciels, dont certains sont gratuits (Recuva par exemple), permettant de récupérer des données après effacement ou formatage. C'est la raison pour laquelle il existe des logiciels d'effacement sécurisé qui fonctionne par réécriture de bits aléatoires sur les données.

dans ce cas, il est important que ceci soit prévu dans des clauses contractuelles dès le départ[19].

Par ailleurs, la question de la réversibilité des données doit être prise en compte par le client avant la souscription à un service de Cloud computing. Le client peut souhaiter conserver les données qu'il a confiées au prestataire et dans ce cas, le prestataire devrait prévoir une restitution dans un format standardisé qui permette au client de réutiliser ces données avec un autre prestataire ou un logiciel classique.

Question posée :

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

Réponse

L'ensemble des problématiques citées ci-dessus pourrait être partiellement traité par un renforcement de la transparence des prestataires de Cloud sur leurs politiques de sécurité. Des mesures de certification des centres de données, tenant compte de la question de la protection des données personnelles pourraient renforcer la confiance des clients et des Autorités de protection des données, sans induire de risques supplémentaires[20]. Toutefois, il n'existe pas de normes de sécurité adaptées au Cloud, qui prennent pleinement en compte la problématique de la protection des données personnelles.

La CNIL recommande que des normes de sécurité incluant la question de la protection des données personnelles dans le Cloud soient définies par le secteur et promues pour renforcer la transparence vis-à-vis des clients.

Questions posées :

- **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 ?**

[19] Le rachat des supports a posteriori est parfois possible mais est en général facturé très cher.

[20] A l'inverse, si chaque client aurait la capacité de faire un audit sur le centre de données, ces audits permanents induisent de nouveaux risques sur la sécurité du centre.

Réponses