TECHNICIEN PRINCIPAL TERRITORIAL DE 1ère CLASSE

Examen professionnel d'avancement de grade

SESSION 2015

EPREUVE DE RAPPORT AVEC PROPOSITIONS

ÉPREUVE ÉCRITE :

Rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : Ingénierie, Informatique et Systèmes d'Information

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni votre numéro de convocation, ni signature ou paraphe.
- Aucune référence (nom de collectivité, nom de personne, …) **autre que celles figurant le cas échéant sur le sujet ou dans le dossier** ne doit apparaître dans votre copie.
- Seul l'usage d'un stylo à encre soit noire, soit bleue est autorisé (bille non effaçable, plume ou feutre). L'utilisation d'une autre couleur, pour écrire ou pour souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 29 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

Vous êtes recruté(e) comme technicien principal territorial de 1ère classe à la Direction des systèmes d'information (DSI) de la ville de TECHNIVILLE, (2 000 agents), rattaché(e) au chef du service études en tant que référent technologies innovantes.
Les services associés à l'informatique en nuage (ou cloud computing) se généralisent de plus en plus.
Votre collectivité souhaite bénéficier des avantages liés à cette technologie mais reste vigilante sur les aspects relatifs à la sécurité.

Dans un premier temps, le chef du service études vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur le cloud computing.

10 points

Dans un second temps et en vue d'une mise en œuvre rapide, il vous demande d'effectuer des propositions opérationnelles destinées à la mise en place sécurisée du cloud computing au sein de la collectivité.

10 points

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances.

Liste des documents :

Document 1 : « Cloud computing : la sécurité en question » - *cad-magazine* - Mai-Juin 2012 - 3 pages

Document 2 : « Cloud computing : les 7 étapes clés pour garantir la confidentialité des données » - *fiche pratique, CNIL* - 1er juillet 2013 - 2 pages

Document 3 : « Le nuage est-il adapté aux collectivités territoriales ? » - *colloque Syctiam* - 21 septembre 2012 - 9 pages

Document 4 : « 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 » - *CNIL* - Janvier 2012 - 10 pages

Document 5 : « Quand les collectivités s'emparent du Cloud Computing » - *Solutions et logiciels N°28* - Mars 2012 – 1 page

Document 6 : « L'Etat appelé à montrer l'exemple par le plan cloud computing » - *usinedigitale.fr* - 6 juin 2014 - 2 pages

avis d'expert

REPÈRE

Cloud computing : la sécurité en question

Au moment où le cloud computing gagne du terrain, Christophe Auberger, Responsable technique chez Fortinet, s'explique sur les erreurs à ne pas commettre en matière de sécurité informatique.

« *Toutes les entreprises ont été ou seront attaquées informatiquement un jour ou l'autre, par hasard ou volontairement. Il faut savoir que l'argent généré par la cybercriminalité est plus important que celui du trafic de drogue !* » C'est l'avertissement de Christophe Auberger, Responsable technique chez Fortinet, société créée il y plus de dix ans, dont l'activité est la sécurité des réseaux informatiques. Celle-ci intervient aussi bien auprès des grands groupes que des PME et ceci dans pratiquement tous les domaines d'activité. D'ailleurs, pour le spécialiste, la sécurité doit être abordée de la même manière, quelle que soit la taille de la structure.

En réalité, il n'existe pas de chiffres fiables qualifiant la cybercriminalité. Les données disponibles varient du simple au triple et les évaluations sont sujettes à caution. Ne serait-ce que parce que les entreprises qui ont subi des attaques informatiques ne le crient pas sur les toits et ne peuvent déterminer précisément le préjudice financier d'un vol ou d'une perte de données. Et puis parce que nombre d'entre elles sont fournies par les prestataires

Christophe Auberger, responsable technique chez Fortinet.

de services comme Fortinet, ou des éditeurs d'anti-virus... Reste que le risque est là et, qu'à l'échelle mondiale, le coût de la cybercriminalité est sans doute de plusieurs centaines de milliards de dollars chaque année !

Les cinq erreurs à éviter

Alors, y a-t-il plus de risque de perdre ses données, ou d'être piraté si l'on adopte les services de cloud computing proposés désormais aux industriels et notamment bureaux d'études ? Des services qui logiquement améliorent la flexibilité et la productivité de l'entreprise tout en réduisant les coûts d'infrastructure. « *Pas plus que dans toute démarche d'externalisation. Vous devez évaluer les capacités de votre prestataire à assurer la sécurité de vos données. Mais c'est loin d'être simple, car il n'existe pas de références communes sur ce critère technique. Les bonnes*

pratiques se standardisent dans certains domaines d'activité comme la finance, mais l'industrie reste encore pauvre en la matière. Le passage au cloud est l'occasion pour l'entreprise qui se lance de se poser les bonnes questions sur la sécurité de la chaîne informatique mise en place. Et dans tous les cas, le niveau de celle-ci dépend de son maillon le plus faible. Il faut donc porter attention à cinq points majeurs... »

1. Ne pas opter pour le bon modèle de cloud

Les entreprises migrant vers le cloud peuvent choisir parmi les clouds publics, clouds privés, clouds communautaires ou clouds hybrides.

• Le cloud public : Il appartient à un fournisseur cloud et est accessible à un large public. Le principe est de payer à l'utilisation et la plateforme est partagée avec d'autres utilisateurs.

• Le cloud privé : Il appartient à une organisation et est déployé pour sa propre utilisation puisqu'elle en est la seule et unique propriétaire.

• Le cloud communautaire : Il est partagé en coopération par plusieurs organisations, souvent de la même industrie.

• Le cloud hybride : Il mixe les modèles de déploiement cloud énumérés ci-dessus, permettant aux applications et données de passer facilement d'un cloud à l'autre.

Chaque type de déploiement en matière de cloud a ses avantages. Les facteurs à considérer avant l'adoption sont : le niveau de criticité des applications que l'entreprise veut basculer dans le cloud ; les questions de réglementation et de conformité ; les niveaux de services (SLA) nécessaires ; les modes d'utilisation selon les charges de travail ; et la manière dont les applications doivent être intégrées aux autres fonctions de l'entreprise.

2. Ne pas intégrer la sécurité cloud dans sa politique de sécurité d'entreprise

Vos politiques de sécurité cloud et sécurité d'entreprise doivent être intégrées. Au lieu de créer une nouvelle politique de sécurité pour le cloud, renforcez plutôt celles qui existent en considérant cette plateforme supplémentaire. Pour modifier vos politiques cloud, vous devez tenir compte des facteurs suivants : où sont stockées les données ? Comment sont-elles protégées ? Qui y a accès ? Mais aussi la conformité avec les règlementations, et les niveaux de services SLA.

Lorsqu'elle est correctement effectuée, l'adoption du cloud computing peut être une occasion d'améliorer vos politiques de sécurité et votre position globale de sécurité.

3. Compter sur la sécurité de son fournisseur de services cloud

Ne pensez pas que vos données soient automatiquement sécurisées parce que vous utilisez un fournisseur

« Toutes les entreprises ont été ou seront attaquées informatiquement un jour ou l'autre, par hasard ou volontairement. »

de services. Vous devez faire un examen complet de la technologie et des processus de sécurité du fournisseur, et vérifier la manière dont ils sécurisent vos données et leurs infrastructures. Plus précisément, vous devez examiner :

• La transportabilité des données et applications : votre fournisseur vous permet-il d'exporter les applications, données et processus existants dans le cloud ? Pouvez-vous les importer de nouveau aussi facilement ?

• La sécurité physique des centres de données : comment les fournisseurs de services protègent-ils leurs centres de données physiques ? Utilisent-ils des centres de données certifiés aux normes SAS 70 Type II ? Comment leurs opérateurs de centres de données sont-ils formés et qualifiés ?

• La sécurité des accès et des opérations : comment votre fournisseur contrôle-t-il l'accès aux machines physiques? Qui peut accéder à ces machines, et comment sont-elles gérées ?

• La sécurité du centre de données virtuel : l'architecture cloud est la clé de l'efficacité. Sachez comment les parties individuelles telles que les nœuds de traitement, nœuds du réseau et nœuds de stockage sont-elles architecturées, et comment sont-elles intégrées et sécurisées.

• La sécurité des données et des applications : Pour mettre vos politiques en application, la solution cloud doit vous permettre de définir des groupes et rôles avec un contrôle d'accès basé sur le rôle précis, des règles de mots de passe et un cryptage des données appropriées (en transit et à l'arrêt).

Y a-t-il plus de risque de perdre ses données ou d'être piratés si l'on adopte les services de cloud computing ?

4. Supposer que vous n'êtes plus responsable de la sécurisation des données

Ne pensez jamais que l'externalisation de vos applications ou systèmes signifie que vous n'êtes plus responsable en cas de violation de données. Certaines PME ont cette fausse idée, mais sachez que votre entreprise est toujours au bout du compte responsable vis-à-vis de ses clients et de tout autre partie prenante lorsqu'il s'agit d'inviolabilité des données. Autrement dit, c'est votre CEO qui risque d'aller en prison, et non le fournisseur cloud...

5. Ne pas savoir quelles lois locales s'appliquent

Les données qui sont en sécurité dans un pays peuvent ne pas l'être dans un autre. Cependant, dans de nombreux cas, les utilisateurs des services cloud ne savent pas où sont stockées leurs informations. Actuellement, dans le processus d'harmonisation des lois sur les données de ses états membres, l'Union Européenne favorise la protection très stricte de la vie privée, tandis que les lois américaines, telles que l'US Patriot Act, permettent au gouvernement et autres organismes d'avoir un accès quasi illimité aux informations appartenant aux entreprises.

Sachez toujours où sont vos données. Si nécessaire, stockez-les dans plusieurs endroits. Il est conseillé de choisir une juridiction qui vous permette d'accéder à vos données même si votre contrat avec votre fournisseur cloud se termine de manière inattendue. Le fournisseur de services devrait également vous donner l'option de choisir l'endroit où vos données seront stockées.

Pour conclure, l'adoption du cloud passe par des démarches de réductions des risques, et il est important que les entreprises se chargent de bien planifier et de veiller au respect de ces mesures dès le début, de sorte que les retours sur investissements en matière de cloud soient maximisés. ▮

CNIL Fiche pratique

Cloud computing : les 7 étapes clés pour garantir la confidentialité des données

01 juillet 2013

En juin 2012, la CNIL a publié des recommandations pratiques à destination des entreprises françaises, et notamment des PME, qui souhaitent avoir recours à des prestations de Cloud. Elle a aussi mis à leur disposition des modèles de clauses contractuelles qui peuvent être insérés dans les contrats de services de Cloud computing. Un an après, la CNIL rappelle aux entreprises les étapes clés pour garantir la confidentialité des données personnelles dans le Cloud.

Des recommandations pratiques permettant de définir le partage des responsabilités
Avant tout engagement commercial, l'organisme souhaitant recourir à une prestation d'externalisation devra mener une réflexion spécifique afin :

1. D'identifier clairement les données et les traitements qui passeront dans le cloud ;
2. De définir ses propres exigences de sécurité technique et juridique ;
3. De conduire une analyse de risques afin d'identifier les mesures de sécurité essentielles pour l'entreprise ;
4. D'identifier le type de cloud pertinent pour le traitement envisagé ;
5. De choisir un prestataire présentant des garanties suffisantes ;
6. De revoir la politique de sécurité interne ;
7. De surveiller les évolutions dans le temps.

Ces 7 étapes préalables permettent :

- De déterminer la qualification juridique du prestataire : s'agit-il d'un simple sous-traitant au sens de l'article 35 de la loi Informatique et libertés ou bien d'un responsable conjoint de traitement au sens de l'article 2 de la Directive 95/46/CE ?
- La CNIL recommande que les obligations et le périmètre des responsabilités de chacun, notamment en matière de sécurité, soient clairement établis. Cette distribution des responsabilités doit être actée en amont, par exemple dans le contrat de prestation de services, et cela de la manière la plus précise possible.
- La CNIL retient la responsabilité conjointe du client et du prestataire lorsque le client ne peut pas réellement donner d'instructions à son prestataire et ne peut pas contrôler l'effectivité des garanties de sécurité apportées par ce dernier. Ceci peut être dû notamment à des offres standardisées, non modifiables par les clients, et à des contrats d'adhésion qui ne laissent aucune possibilité de négociation. Cette absence d'instruction et de moyens de contrôle étant constatée pour certains services de PaaS et de SaaS publics, le prestataire pourrait donc dans ces cas être a priori considéré comme responsable conjoint de traitement.
- D'évaluer le niveau de protection assuré par le prestataire aux données traitées : le niveau de sécurité offert par le prestataire est-il supérieur ou égal à celui qui était préalablement assuré ?

Le cloud ne doit pas aboutir à une diminution du niveau de protection des données, particulièrement s'agissant de donnés sensibles, au sens de l'article 8 de la loi Informatique et libertés.
Des modèles de clauses pour définir clairement les responsabilités dans un contrat
Que la responsabilité du traitement soit conjointe ou bien à la charge unique du client, les responsabilités du client et du prestataire doivent être expressément définies et comporter :

1. Une information transparente sur les modalités de traitement :

Il s'agit pour le prestataire :

- De s'engager à respecter les principes essentiels en matière de protection des données personnelles (par exemple, obligation d'informer les personnes, soit en fournissant au client toutes les informations nécessaires pour remplir cette obligation, soit en informant directement les personnes concernées lorsque le prestataire est responsable conjoint du traitement),
- De mettre à disposition un système de remontée des plaintes et des failles de sécurité,
- De décrire les moyens de traitement à mettre en œuvre, d'informer le client de tout recours à des sous-contractants (et d'obtenir son accord préalable lorsque le prestataire est sous-traitant),
- De proposer des procédures simples pour respecter les droits des personnes concernées vis-à-vis de leurs données (notamment le droit d'accès aux données) ;

2. Une information transparente sur les lieux de stockage des données et sur les transferts indiquant, de manière claire et exhaustive :

- Les pays hébergeant les serveurs du prestataire (et de ses sous-contractants éventuels),
- L'existence d'une protection suffisante des données lorsqu'elles sont hébergées en-dehors de l'Union européenne (notamment grâce à des Clauses contractuelles types ou à des règles contraignantes d'entreprise " BCR "),
- La possibilité de limiter les transferts de données uniquement vers des pays assurant un niveau de protection suffisant,
- Et portant à la connaissance du client toute requête provenant d'une autorité administrative ou judiciaire étrangère ;

3. Les garanties mises en œuvre par le prestataire :

- Respect de durées de conservation des données limitées et raisonnables au regard des finalités pour lesquelles elles sont collectées,
- Destruction ou restitution de ces données,
- Devoir de coopération avec les autorités de protection des données compétences,
- Possibilité pour le client de diligenter des audits ;

4. Les formalités auprès de la CNIL

Elles peuvent être effectuées au nom du client (par lui ou un sous-traitant mandaté à cet effet), ou du prestataire s'il est responsable conjoint du traitement ;

5. La sécurité et la confidentialité des données hébergées

- Indication des obligations du prestataire en matière de sécurité des données (et, lorsque celui-ci est sous-traitant, précision qu'il ne peut agir que sur instruction du client),
- Politique de sécurité et mesures de sécurité retenues,
- Procédure de certification éventuelle (soumise à libre négociation),
- Procédure permettant l'audit (notamment lorsque le prestataire est sous-traitant),
- Réversibilité/portabilité des données, traçabilité, continuité de service, sauvegardes et engagements de niveau de service.

Des modèles de clauses, portant uniquement sur la protection des données personnelles et n'ayant donc pas vocation à constituer un contrat de prestation de services complet, sont présentés à titre d'illustration. Elles peuvent faire l'objet d'aménagements formels, dès lors que les droits, les obligations et le partage des responsabilités du client et du prestataire sont clairement définis dans le contrat.

Le nuage est-il adapté aux collectivités territoriales ?

« Le nuage, c'est quoi finalement ? »

Le terme apparait fin 2008 et depuis, on n'arrête plus d'en entendre parler. Mais de quoi s'agit-il ? En deux mots, adopter le *cloud* consiste à abandonner nos serveurs informatiques locaux au profit de serveurs distants, partagés avec d'autres usagers. Qui dit « partage des ressources » dit « partage des coûts » : le nuage nous promet des économies sur le stockage d'informations, la location de puissance de calcul et la fourniture de services numériques de toute sorte : mails, calendriers, gestion des ressources humaines ou financières, progiciels métiers, etc.

Cette définition somme toute simpliste, qui nous rappelle énormément l'infogérance des années 90, appelle quelques précisions. Et c'est là que le bât blesse. La multiplicité des définitions du cloud donne à chacun l'impression d'avoir fait appel au nuage, voire d'opérer un nuage, à un moment ou à un autre de sa vie professionnelle. Des caractéristiques communes émergent cependant :

1. **Self-service :** ces ressources numériques externes peuvent être commandées en ligne, à partir d'un catalogue, sans interaction humaine.
2. **Accès universel** : les ressources numériques sont accessibles, quelle que soit l'heure, l'endroit ou le terminal de l'usager.
3. **Mutualisation :** on l'a dit, le partage de la ressource est au cœur du principe du nuage, mais également une certaine opacité vis-à-vis de la localisation de ces ressources communes. Si elles changent d'emplacement, les usagers ne sont pas impactés.
4. **Élasticité :** les ressources mises à votre disposition peuvent augmenter ou diminuer en fonction de vos besoins, de manière très réactive, voire complètement automatisée. En la matière, la capacité à diminuer est presque plus importante que celle d'augmenter, car votre facture mensuelle elle-aussi suit cette même variation.
5. **Mesure :** les ressources consommées, leur disponibilité et leur performance sont observées en temps réel. Ces mesures sont consultables par les usagers. Elles constituent la base de la facturation des services.

Est-ce à dire qu'un service n'ayant pas exactement ces cinq caractéristiques ne soit pas « dans le nuage » ? C'est sans compter le génie marketing des éditeurs qui n'hésitent pas à accoler cette étiquette sur toute forme d'externalisation de service. Mais au-delà de cette tendance, il faut savoir être pragmatique et faire la part des choses entre d'une part une vision idéale et maximaliste du nuage et d'autre part ses racines. Celles-ci sont les valeurs qui sous-tendent cette nouvelle manière de fournir un service informatique : le partage, la souplesse d'utilisation et la relation directe avec l'usager. Les collectivités locales, et en matière de numérique, les syndicats informatiques, portent ces valeurs depuis bien longtemps.

« C'est bien beau ce nuage, mais le contexte de nos collectivités est vraiment particulier. »

Les systèmes informatiques des collectivités territoriales ont des spécificités liées à leurs compétences en tant qu'autorités administratives, à leur territoire, ainsi qu'au mode de fonctionnement du service public.

Nos villes, nos agglomérations, nos départements et nos régions sont amenés à exercer des dizaines voire des centaines de métiers différents. Tous ne sont pas informatisés, mais cela suffit pour qu'une ville de taille moyenne compte 75 logiciels dans son parc applicatif. À ce nombre s'ajoute une difficulté de taille, car les éditeurs œuvrant dans les métiers des collectivités se partagent un marché de niche. En conséquence, la diversité de l'offre proposée est limitée techniquement. Les critères fonctionnels étant rois en matière de choix de logiciel, la direction des systèmes d'information doit se résoudre à faire coexister des solutions techniques radicalement différentes. Dans ces conditions, la rationalisation des environnements techniques devient difficile.

S'il est évident que régions et départements doivent gérer un territoire important, c'est également le cas à plus petite échelle pour les agglomérations et même les villes. Les directions centrales sont assistées dans leurs missions par des services de proximité disséminés sur l'ensemble du territoire. Cette territorialisation a des conséquences sur l'infrastructure du réseau informatique qui doit permettre à l'ensemble des agents, voire aux administrés, de travailler ensemble quelle que soit leur localisation. Dans les

locaux de l'administration centrale, où sont en général hébergés les services numériques, la situation est confortable car les échanges de données s'appuient sur un réseau local performant. Dans les bureaux des services de proximité, la situation est plus précaire. Toutes n'ont pas la chance de bénéficier d'une ligne dédiée les reliant aux serveurs centraux. Beaucoup se contentent d'une ligne SDSL, voire ADSL, sur laquelle doivent transiter l'ensemble des données et la voix dans le cas des installations incorporant la téléphonie sur IP. Il en résulte une iniquité de traitement entre les agents et, par suite, les administrés, en fonction de leur implantation géographique.

Enfin, conjoncture impose aux collectivités une recherche d'économies, notamment sur les frais de fonctionnement. S'il est encore possible de dégager des fonds en vue d'investissement, il est bien plus difficile d'augmenter les coûts de fonctionnement, que ce soit en masse salariale ou en abonnements récurrents à des services.

« Dans ce contexte, que peut-on tirer du nuage ? »

Les ressources proposées dans le nuage sont de trois natures :

- **Du logiciel métier.** On parle de *software as a service* (SAAS). Il s'agit de louer des applications web capables de gérer plusieurs organisations en même temps. Toutes les organisations partagent la même version du logiciel.
- **Du logiciel technique.** On parle de *platform as a service* (PAAS). Il s'agit de louer des logiciels intermédiaires : des bases de données, des serveurs d'application, des systèmes d'exploitation.
- **Du matériel**. On parle d'*infrastructure as a service* (IAAS). Il s'agit de louer des machines, de l'espace disque ou du temps de calcul.

Nos collectivités peuvent-elles bénéficier du SAAS ? La réponse est – quasiment – non ! Très peu d'éditeurs sont aujourd'hui capables de fournir des applications web multi-tenant et partageant la même version pour nos logiciels métiers. Les collectivités adaptent les progiciels, plutôt que les adopter. Les seuls candidats réalistes sont la messagerie, l'agenda et la bureautique. Quant à héberger nos sites internet, intranet ou extranet sur le nuage, n'oublions pas que la dématérialisation est passée par là et que ces guichets du web sont étroitement connectés à nos applications métiers, hébergées localement.

Nos collectivités peuvent-elles bénéficier du PAAS ? La réponse est mitigée. On se heurte ici au nombre de plateformes techniques hébergées dans nos murs. Les offres du nuage sont standardisées pour conserver une certaine simplicité de gestion. Trouver des prestataires capables de fournir nos configurations, dans la durée, relève de la gageure. À cela s'ajoute une difficulté : si pour de jeunes start-up du secteur privé il est plus facile de dépenser quelques centaines d'euros par mois plutôt que d'investir des dizaines de milliers d'euros, la situation est plutôt inverse dans notre contexte.

Nos collectivités peuvent-elles bénéficier de l'IAAS ? Cette fois la réponse est positive. La logique de la virtualisation et de la mutualisation est critique pour nos systèmes, où la complexité technique nous oblige à aligner autant de machines que de logiciels, et les multiplier par environnement (recette, formation, production). Par ailleurs, les besoins en stockage ne font qu'augmenter, comme les exigences portant sur la conservation et la restauration des données avec la prise de conscience des directions de la nécessité de mettre en place des plans de continuité et de reprise d'activité (PCA/PRA).

Qui a peur du grand méchant *cloud* ?

« Mais attendez, il est hors de question que nos données sortent de chez nous ! »

Qui dit infrastructure dans les nuages dit stockage des données des collectivités à l'extérieur de leurs murs.

Tordons d'abord le cou à une idée reçue : on peut tout à fait savoir où sont stockées nos données, même sur le nuage. En la matière, seul Google entretient un flou réel sur la localisation des données. Les autres fournissent une carte de leurs *datacenters*, ces centrales numériques à dimension industrielle, et il est possible de choisir dans quelle(s) zone(s) géographique(s) les données sont stockées.

Le problème n'est donc pas de savoir où sont localisées nos données, mais qu'elles soient entreposées hors de notre territoire qui pose problème.

Disons-le tout de go, il y a dans nos collectivités un attachement fort à la donnée, qu'il soit rationnel ou pas. Les usagers n'aiment pas l'idée que leurs données ne soient pas physiquement près d'eux. Cet éloignement est assimilé à une perte de contrôle. Hors nos murs, comment savoir qui lit nos données ? Comment savoir si elles n'ont pas été modifiées par un tiers ? La peur de voir des informations confidentielles filtrer est bien réelle. Le fait que les données soient stockées outre-Atlantique n'est pas en soi le problème. L'obstacle est qu'elles sortent des limites du territoire de la collectivité, qu'il soit limité à une ville ou qu'il s'étende sur toute une région.

À cet aspect culturel s'ajoute une contrainte juridique tangible. Aujourd'hui, une collectivité n'a tout simplement pas le droit d'envoyer des données en dehors de l'Europe. Héberger ses mails chez Google, c'est se mettre en infraction vis-à-vis du droit national et européen. L'ignorance étant une bien maigre protection pour les directions informatiques qui s'y risquent, nous disons clairement ici qu'il n'est pas envisageable de recourir à ces services pour quelque autorité administrative que ce soit. Dans le même ordre d'idée, rappelons également que la réglementation interdit aux collectivités de confier l'archivage définitif de leurs documents à un prestataire externe. Ceux-ci doivent rester dans les locaux même de l'administration qui en a la charge.

« Notre problème de confidentialité des données est bien réel. »

Dans leurs missions, nos collectivités sont attachées à garantir la confidentialité et l'intégrité de l'ensemble de leurs données. Si beaucoup de données traitées finissent par être publiques, un certain nombre restent confidentielles, et même sensibles.

Nos systèmes hébergent les données personnelles d'administrés. On trouve classiquement les coordonnées postales et téléphoniques, la composition de la famille, la capacité à exercer ou non le droit de vote, mais aussi des données sociales sensibles dans le cadre des compétences des départements, où on trouve en particulier le droit au RSA ou le dossier handicap.

N'oublions pas non plus les informations sur les agents que recèlent les systèmes d'information des ressources humaines, notamment les évaluations annuelles et bilans personnels.

Le risque sécuritaire est-il tellement plus grand hors de nos murs ?

Si l'externalisation des données semble plus risquée que de les conserver dans nos bureaux, qu'en est-il réellement ? Le stockage interne donne-t-il une garantie de confidentialité, ou n'est-ce qu'une confortable illusion ?

Une bonne partie de nos informations est encore sur papier. Sont-elles aussi sécurisées que nos salles informatiques ? Pourtant, c'est souvent dans les armoires que les informations les plus sensibles se trouvent.

Quant à nos données informatisées, nous n'hésitons pas à les faire transiter par mail, donc par le réseau Internet, sans pour autant les chiffrer. Que penser du fichier des paies qui part à la Banque de France par mail tous les mois ? Qu'il soit hébergé à l'intérieur ou à l'extérieur n'a finalement que peu de conséquences quand on est prêt par ailleurs à le transmettre sur un canal non sécurisé.

Enfin, donnons un chiffre : 80 % des délits sont commis à l'intérieur même des structures. C'est à se demander si on ne réduirait pas les délits en externalisant la donnée et en contrôlant précisément qui y accède de l'intérieur.

En matière de sécurité, il est très simple de jouer à se faire peur. L'industrie informatique a acquis un peu de maturité sur la question et a abandonné la recherche de la sécurité absolue au profit de la maîtrise des risques. L'essentiel est de comprendre et de bien évaluer quels sont les risques réels encourus. Pour reprendre une métaphore bien connue, il est inutile d'installer une porte blindée si les murs sont en cartons et si ceux qui détiennent les clés les cachent sous le paillasson. La sécurité réelle des données est loin d'être un problème uniquement technique. Elle tient à la solidité du maillon le plus faible de la chaîne, celle-ci impliquant bien des hommes et des femmes qui n'ont pas idée des impacts en cas de perte ou de fuite des données. Ce n'est pas pour rien que cette évaluation est la première tâche réclamée par le référentiel général de sécurité (RGS), à l'aune d'un contenu essentiellement composé d'annexes rappelant les normes et textes réglementaires applicables.

Le référentiel général de sécurité

Le RGS définit les règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information et plus particulièrement s'agissant des téléservices mis en œuvre. Il entre en application en mai 2013.
http://references.modernisation.gouv.fr/rgs-securite

Les fournisseurs du nuage ont à cœur de rassurer leur clientèle potentielle sur l'importance qu'ils accordent à la sécurité de leurs données. Certains choisissent de subir des audits de sécurité et d'en publier les résultats. D'autres affichent des certifications ISO 27001 mais, malheureusement, la culture française ne fait pas grand cas de ces certifications, qui ne sont pas souvent considérés comme de réels gages de qualité malgré les investissements réel de ces sociétés.

Reste que toutes les certifications du monde ne lèveront pas les contraintes juridiques. Chaque pays d'Europe a adapté la directive européenne sur la protection des données, la France y compris, au travers de la CNIL. Une réglementation est en préparation pour harmoniser ces dispositifs locaux, mais il n'est pas question d'ouvrir la possibilité d'externaliser les données en dehors de nos territoires.

Comment déployer le nuage dans nos collectivités territoriales ?

Il est entendu que les contraintes juridiques nous empêchent de faire appel au nuage mondial. Quelles sont les alternatives ?

Nous attendons toujours le nuage public national

L'État a lancé un projet de nuage hébergé sur le territoire national. Ce projet se nomme Andromède. Cette figure mythologique semble vouloir nous protéger des « monstres » venus de l'océan, à savoir Google, Amazon et autres grands opérateurs du nuage nés outre-Atlantique...

Les motivations du projet sont multiples. On peut citer l'enjeu de la souveraineté, la nécessité de conserver une compétence technique pointue sur les infrastructures informatiques et également la création d'emplois.

Après quelques péripéties, le projet s'est scindé en deux initiatives pesant chacune 250 millions d'euros, financées pour un tiers par le grand emprunt : Numergy avec SFR Business Team et Bull et Cloudwatt avec Orange et Thalès.

Pour le moment, les sites web de ces projets nous informent sur ce qu'est le cloud à destination du grand public. Quant à connaître leur date de disponibilité, le contenu du catalogue des services, la tarification et leur cible, on nage dans le brouillard ! Ces projets doivent donc encore se concrétiser et démontrer qu'ils répondent à nos attentes. C'est la raison pour laquelle il serait prématuré de les intégrer d'ores et déjà dans nos stratégies d'évolution des systèmes d'information.

Par ailleurs, alors que la contrainte juridique serait levée par un tel cloud national, la contrainte culturelle demeure. Pour beaucoup d'acteurs locaux, il n'est pas envisageable que leurs données franchissent les limites de leur ville. Même en restant dans nos frontières, le cloud national parait extrêmement éloigné de nos collectivités territoriales.

Le nuage privé est possible mais nécessite un investissement élevé

À défaut de pouvoir bénéficier des services d'un opérateur de nuage, des collectivités ambitieuses se sont lancé dans des projets d'infrastructure pour devenir elles-mêmes leur propre fournisseur !

Citons les exemples des deux collectivités nous ayant fait l'amitié de bien vouloir intervenir pendant cette conférence.

Commençons par le projet initié conjointement par l'agglomération du Grand Lyon et le SITIV, un syndicat informatique composé de plusieurs villes de l'agglomération lyonnaise. Cette association est complémentaire. Le syndicat informatique offre déjà des services numériques, mais n'a pas les moyens de mettre en place des infrastructures suffisamment puissantes pour les ouvrir à un large public. De son côté, le Grand Lyon monte fortement en compétence sur l'infrastructure.

Ce projet est motivé par plusieurs facteurs :

- Les capacités numériques de la région lyonnaise sont insuffisantes pour répondre aux besoins des entreprises et des administrations déjà installées, ou qui souhaiteraient s'installer ;
- Les audits de sécurité informatique des villes montrent de nombreuses failles de sécurité ;
- Des projets ambitieux de gestion de la relation avec les citoyens (GRC) et d'ouverture des données (OpenData) nécessitent un besoin important en stockage de données et une sécurité renforcé.

Les services principalement attendus de cette centrale numérique commune sont la capacité de stockage et de sauvegarde, ainsi que la capacité à servir d'hébergement de secours ou complémentaire dans le cadre des plans de continuité et de reprise des activités (PCA/PRA).

Poursuivons avec l'exemple du département des Côtes d'Or. En 2007, l'actuel directeur des systèmes d'information fait un état des lieux préoccupant de sa salle serveur. Il lance alors un schéma directeur visant à transformer son infrastructure pour assurer la performance et la sécurité tout en maîtrisant les coûts. En six ans, la salle informatique encombrée de 150 serveurs physiques s'est transformée en utilisant les mêmes technologies que celles utilisées dans le nuage. Le département dispose aujourd'hui d'un espace redondé où tous les serveurs ont été virtualisés.

Les disques durs ont quitté les serveurs pour rejoindre une baie de stockage de plusieurs dizaines de téraoctets. Ceci a permis la virtualisation des postes de travail. Près de 900 postes sont ainsi à tout moment exécuté dans la salle machine plutôt que sur les ordinateurs individuels des agents. Ce *desktop as a service* a permis de prolonger la durée de vie du matériel pendant deux ans, portant leur longévité à sept années, permettant ainsi des économies substantielles, et servant à justifier le coût total du projet. L'exploitation du parc informatique disséminé sur l'ensemble du territoire est optimisée. En cas d'incident matériel, les agents prennent d'eux-mêmes l'ordinateur de secours rangé dans leurs armoires. Il leur suffit de le brancher sur l'électricité et le réseau et de s'identifier pour retrouver leur environnement de travail dans l'état où ils l'avaient laissé sur la précédente machine. Les techniciens n'ont pas besoin de se déplacer pour intervenir dans l'urgence.

Ces projets démontrent la capacité des collectivités à mener des projets innovants et ambitieux dans ce domaine. Malheureusement, en avance sur leur temps, ils restent l'exception. Un datacenter comme celui du Grand Lyon coûte 2 millions d'Euros. Alors que les budgets se resserrent, chaque ville, chaque syndicat ne pourra pas se payer sa centrale numérique.

Il faut donc que ce nuage soit communautaire et local.

Comme on l'a vu dans l'exemple du SITIV et du Grand Lyon, les syndicats informatiques ont une position privilégiée vis-à-vis des collectivités locales. Ces structures font de la coopération intercommunale leur métier. Elles disposent de la confiance de leurs adhérents. Étant eux-mêmes des établissements publics, émanant d'autres communes, leur implication permet également de contourner les freins culturels sur l'exploitation non souhaitées des données des villes.

Seuls, les syndicats n'ont pas les moyens de construire des centrales numériques. La masse critique nécessaire pour avoir la capacité de créer une centrale numérique locale nécessite l'association des moyens et des compétences de plusieurs collectivités territoriales. Une mutualisation au niveau des territoires, que ce soit dans les grandes agglomérations ou dans les régions prend tout son sens.

Un tel *cloud* communautaire s'inscrit dans un cercle de confiance qui respecte les conditions réglementaires et juridiques, et limite ainsi les conditions de réversibilité des marchés publics.

Les formes juridiques de l'entité exploitant ces centrales numériques locales restent à choisir. Société publique locale, délégation de service public, groupement d'intérêt public ou partenariat public-privé ? Les options sont nombreuses et seule une étude pourra déterminer la forme juridique la plus adaptée dans chaque contexte. La question de la gouvernance du dispositif devra également être clarifiée.

Par ailleurs, si la demande de proximité des données est d'abord culturelle, elle rejoint une problématique technique cruciale en matière de nuage, qui est celle de la bande passante. L'externalisation des ressources matérielles entraîne la dépendance à la connexion au réseau Internet, et la performance de ces ressources est limitée par celle du réseau. Or, on l'a vu, sur un territoire étendu, la qualité du réseau est souvent en deçà des besoins. Pour assurer un débit suffisant avec les bureaux centraux, il est essentiel que l'accès au réseau soit performant. La proximité géographique est encore le moyen le plus simple de le permettre, à court ou moyen terme.

Ces deux raisons, culturelle et technique, expliquent pourquoi on voit ainsi fleurir de nombreux projets de création de *datacenters* dans nos territoires, malgré les promesses du nuage public national.

Une centrale numérique ?

Le terme de centrale numérique est construit par analogie avec la centrale électrique. Là où la centrale électrique est un site industriel produisant de l'électricité, la centrale numérique est une usine informatique, qui produit de l'information et du service numérique.

Qu'est-ce que le nuage va apporter à nos collectivités ?

Les territoires physiques peuvent être valorisés en les enrichissant d'un territoire numérique.

Le tabou est tombé : on a désormais le droit de parler de compétitivité des territoires. Ceux-ci sont en concurrence les uns avec les autres. Les acteurs économiques choisissent le lieu d'implantation en fonction de plusieurs critères. L'accès aux infrastructures numériques en fait pleinement partie. Dans le cas du Grand Lyon, c'est l'aménagement et la promotion du territoire par le projet de centrale numérique qui ont emporté l'adhésion des instances politiques.

Le numérique au sens large est maintenant bien identifié comme un vecteur d'évolution pour améliorer l'attractivité de nos territoires auprès des entreprises et des citoyens. Au même titre que le collectif a financé la construction d'autoroutes pour faciliter la mobilité des tous, puis le fibrage du territoire pour faire circuler les informations, il reste à disposer de centrales numériques pour compléter le dispositif.

Les centrales numériques locales, construites pour répondre aux besoins des administrations, peuvent jouer un rôle d'accélérateur et aider au démarrage d'une entreprise en lui vendant du stockage et un hébergement local et sécurisé. C'est la même logique qui préside à celle des pépinières d'entreprise : créer un contexte favorable à l'innovation et à la croissance. Une fois qu'elles ont atteint une taille critique leur permettant d'être auto-suffisante, ces entreprises peuvent alors se tourner vers le marché des fournisseurs privés.

Ces territoires numériques favorisent nos populations de travailleurs nomades.

Le besoin en mobilité des agents territoriaux se développe.

De par leur attachement à un territoire, certains sont appelés à le parcourir, et ils ont besoin d'emporter leur poste de travail avec eux.

Moins développé, le télétravail nécessite également que les agents disposent de leur poste de travail à l'extérieur des locaux. Cela suppose un accès à distance au système d'information, et qu'un technicien puisse intervenir sur ce poste déporté ou installé au domicile de l'agent, parfois loin de l'administration centrale. Ce mode d'organisation du travail à distance est appelé à se développer. Un accord cadre fixant les modalités juridiques du télétravail dans la fonction publique est en cours d'élaboration. Parmi les bénéfices recherchés, on peut citer la capacité de la collectivité à fonctionner même en cas de crise. La grippe aviaire a rappelé à tous les difficultés que rencontreraient nos organisations si les agents devaient rester à demeure à leur domicile.

Le développement de centrales numériques locales apporte une réponse technique à ce besoin de mobilité. Cette réponse n'est pas complète mais elle va dans la bonne direction, celle d'un accès au système d'information de la collectivité où qu'on se situe, dans des conditions satisfaisantes de sécurité. L'initiative des Côtes d'Or en matière de *desktop as a service* est une illustration parfaite des bénéfices qu'on peut attendre d'un tel dispositif.

À ces valeurs ajoutées stratégiques s'ajoute une simplicité de gestion pour les directions informatiques.

Les bénéfices du nuage dans l'exploitation de l'infrastructure sont bien connus des directions informatiques.

La virtualisation systématisée des serveurs permet de ne plus réserver des machines physiques distinctes pour chaque progiciel. Désormais, ces programmes évoluent dans des environnements virtualisés et s'exécutent indifféremment sur l'une ou l'autre des machines physiques dans leur centrale numérique, au gré des besoins. La mise à disposition d'un environnement de recette ou de formation, distincts de la production, ne nécessite plus d'arbitrage sur l'utilisation optimale des ressources. Ils sont fournis sans délai. Par ailleurs, la consolidation des serveurs permet un meilleur usage des ressources, et potentiellement des économies d'énergie.

La mutualisation du stockage permet d'atteindre des niveaux d'espace disponible et de fiabilité élevés. Combinée à la virtualisation, elle simplifie considérablement la sauvegarde des données et des programmes et, par suite, leur restauration rapide. Le dimensionnement de ces espaces dédiés au stockage doit être bien évalué. La quantité de données à sauvegarder double tous les ans. Une baie de disque dont la taille était confortable il y a cinq ans est aujourd'hui très remplie.

Comme on l'a vu avec le retour d'expérience de la Côte d'Or, la virtualisation des postes de travail facilite l'exploitation du parc. Les techniciens ont moins besoin d'intervenir directement sur les machines, ce qui diminue les déplacements dans les bureaux et dans le territoire. La durée de vie du poste est augmentée mais on gagne également en sécurité. Les données n'étant plus stockées sur les machines des agents, leur vol n'est plus une menace en matière de confidentialité. En cas de panne ou de sinistre, ils sont remplacés sans que l'agent perde le fruit de son travail.

Pour revenir au SAAS écarté au début de ce document, il peut rendre service en matière d'outils collaboratifs dont la standardisation est plus simple à imposer que pour un progiciel métier. On a évoqué la messagerie électronique et les agendas, mais également la bureautique en ligne. Les versions de Microsoft Office, OpenOffice et autre LibreOffice se multiplient dans nos collectivités. La compatibilité des documents soulève régulièrement des questions, en interne ou avec les partenaires. Dans ce contexte, la standardisation du SAAS est ici une force.

Mettons le nuage au service de nos collectivités pour mieux servir les usagers

Nous avons le sentiment d'être à un moment charnière. Les attentes en matière de service numérique sont de plus en plus fortes. La dématérialisation s'est installée dans nos modes de travail. Cette transformation est maintenant irréversible.

Le territoire numérique « augmente » le territoire physique

Pour soutenir cette transformation, nos collectivités ont besoin de mutualiser leur infrastructure pour répondre aux nouveaux projets de services numériques aux usagers (gestion de la relation citoyen, dématérialisation, OpenData, etc.). Les technologies du nuage nous apportent une souplesse de gestion ainsi qu'une disponibilité des services et des données inégalées. Pour en bénéficier, nous devons lancer des projets de centrales numériques communautaires, portés par nos collectivités, et implantés localement. Les syndicats informatiques sont les partenaires naturels de ces projets collectifs. La gouvernance de ces projets doit permettre d'impliquer tous les partenaires dans l'animation de ces services.

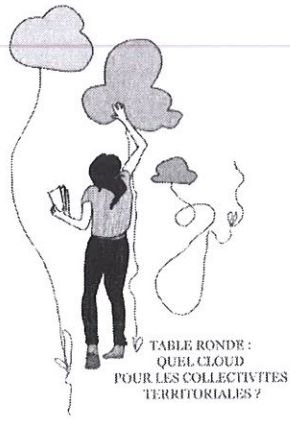
Dans nos organisations, ces centrales donneront un poste de travail aux télétravailleurs, que ce soit en contexte de crise ou en mode de fonctionnement quotidien, dans des conditions d'exploitation efficientes. Ces centrales pourront également s'ouvrir aux entreprises, pour aider à leur démarrage et renforcer l'attractivité de nos territoires.

Nous sommes en train de gagner en maturité

Ce contexte évolue très rapidement : tant les éditeurs que les utilisateurs comprennent les bénéfices qu'ils peuvent tirer de ces technologies. Les cahiers des charges prennent en compte la possibilité de travailler dans le nuage, mais bien souvent en imposant des contraintes techniques, de sécurité, et de fonctionnalités relativement complexes. Nous nous attendons à que les usages et l'expérience clarifient et simplifient nos exigences, tout en apaisant nos craintes quant à la protection des données, à leur pérennité quand elles sont dans le nuage et à la réversibilité des systèmes choisis.

Départements, régions et gouvernement sont sensibles à la nécessité d'aménager le territoire pour rendre la donnée disponible partout. Nos collectivités doivent être dans le mouvement, et dépasser les peurs et les difficultés budgétaires. À nous de nous donner collectivement les moyens de répondre aux attentes de nos usagers, qui sont tout autant administrés que citoyens, pour qu'ils aient accès aux collectivités territoriales et leurs services.

Le numérique doit devenir un service public de proximité !



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

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

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.

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.

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.

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 :

- 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.

[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.

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

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

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

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.

DOCUMENT 5

Quand les collectivités s'emparent du Cloud Computing

L'informatique en nuage apporte aux collectivités une nouvelle façon de concevoir et de consommer l'IT. Les migrations démarrent et transforment déjà certains métiers.

CHELLES : une meilleure qualité de service grâce au cloud

Le cloud computing figure au coeur des projets informatiques de Chelles et de la communauté d'agglomération Marne & Chantereine. Issu du contrôle de gestion, René-Yves Labranche, le DSI de Chelles, dresse un bilan positif sur la productivité des équipes, les services délivrés de façon économique et environnementale.

➜ Solutions IT & Logiciels : La ville de Chelles et sa Communauté d'Agglomération sont-elles engagées dans l'informatique en nuage ?

• René-Yves Labranche : Le Cloud computing fait partie de notre stratégie à court et moyen terme. Nous utilisons de plus en plus d'applications hébergées comme la plateforme des marchés publics, le portail des familles et le nouveau portail des citoyens qui sera mis en production courant 2012. Internet est devenu un vecteur majeur de communication dans les collectivités. En mutualisant nos infrastructures, nous pouvons héberger une dizaine de structures municipales et para-municipales, avec des équipements redondants sur deux sites, offrant quatre pivots : les télécoms avec des liens différenciés vers Internet, les serveurs, le stockage et un dispositif différencié pour les écoles du territoire.

➜ Vous imposez-vous ou vous impose-t-on des contraintes environnementales ?

• R-Y. L. : Nous sommes dans une démarche « green it » depuis 2005, date de la création de la communauté d'agglomération Marne & Chantereine. Nous avons réduit notre facture énergétique de plus de 40% avec le remplacement des écrans cathodiques, la virtualisation des serveurs (quasiment 100% aujourd'hui) et la mise en place de clients légers. Nous veillons, notamment au travers du code des marchés publics, à choisir des partenaires qui respectent les critères sociaux et environnementaux.

➜Quels sont les autres avantages du cloud les plus sensibles pour votre collectivité ?

• R-Y. L. : L'externalisation des datacenters améliore la disponibilité des services et réduit les coûts d'infrastructures. La virtualisation des serveurs et du stockage nous a permis de réduire aussi nos coûts de maintenance. Dès lors que l'on met moins les mains dans le cambouis, toute la productivité de l'infrastructure évolue, la qualité de services s'améliore et le reporting également. De plus, nous avons mis en place un plan de reprise d'activités, en créant un deuxième datacenter avec l'agglomération ; le datacenter de l'hôtel de ville est secouru par celui de l'agglomération, et inversement. Le fonctionnement en mode actif-actif est devenu possible grâce à la virtualisation massive de nos serveurs via VMware, avec la mise en place d'un stockage virtualisé avec Datacore et une sauvegarde à trois niveaux (deux niveaux sur disques et un niveau sur bandes).

➜ Rencontrez-vous des réticences internes au sujet du cloud computing ?

• R-Y. L. : Il faut accompagner cette réflexion car il y a toujours la crainte de perdre son emploi. Nous sommes lancés dans une démarche cloud hybride, ce qui suppose de redéployer certaines équipes techniques vers l'accompagnement des métiers. C'est la stratégie que je proposerai dans les mois à venir aux élus et aux directions générales de Chelles et de la communauté d'agglomération Marne & Chantereine.

DOCUMENT 6

L'Etat appelé à montrer l'exemple par le plan cloud computing

Parmi les dix propositions d'actions du plan industriel sur le cloud computing, l'Etat est invité à donner l'exemple en adoptant massivement l'informatique en nuage. Une manière de générer des économies, de créer un climat de confiance sur le marché et d'entraîner dans son sillage les entreprises.

"*C'est sans doute l'un des plans les plus stratégiques de 34 plans de la Nouvelle France industrielle*". C'est ce qu'Arnaud Montebourg, ministre de l'Economie, du Redressement productif et du Numérique a déclaré à l'issue de la présentation, le 4 juin 2014, par Octave Klaba, le directeur général d'OVH, du plan industriel sur le cloud computing élaboré avec Thierry Breton, PDG d'Atos. La feuille de route du plan a été immédiatement validée par le gouvernement.

Dix propositions d'actions sont sur la table. Pour Alban Schmutz, Vice-président sénior chez OVH, en charge du dossier pour le compte d'Octave Klaba, la plus importante concerne le rôle des pouvoirs publics en tant que prescripteurs. L'Etat est invité à donner l'exemple en adoptant massivement l'informatique en nuage, non seulement dans les administrations centrales mais aussi dans les agences gouvernementales. *"C'est un gage de confiance, indispensable au développement de la demande,* martèle Alban Schmutz. *L'engagement de l'Etat aura un effet d'entraînement important non seulement sur les collectivités locales, mais aussi sur les PME qui hésitent beaucoup à franchir le pas."*

Opter cloud systématiquement, sauf bonne raison

Les finances publiques ont à tout à y gagner. L'adoption du cloud pourrait générer une économie de 800 millions d'euros par an, rien qu'au titre de la rationalisation des datacenters de l'Etat. Auxquels s'ajoutent des gains non négligeables sur les frais de personnel. *"Au total, l'Etat pourrait économiser plus de 1 milliard d'euros par an sur ses dépenses informatiques* ", estime Alban Schmutz. Un gain potentiel de même ordre existe dans les collectivités locales. Ces économies se doubleraient de recettes fiscales supplémentaires de 1 à 1,5 milliard d'euros par an dues à l'implantation de nouveaux datacenters en France. Au total, le gain dépasserait les 3 milliards d'euros par an pour les finances publiques, selon le dirigeant d'OVH.

Le rapport propose d'instaurer l'obligation dans les achats publics de privilégier systématiquement les services de cloud computing, sinon de justifier le choix de solutions informatiques traditionnelles, comme cela se fait en Italie, au Royaume-Uni, aux Etats-Unis ou en Inde. Ceci impose d'introduire de la souplesse dans les budgets publics où aujourd'hui les dépenses d'investissement et les dépenses de fonctionnement sont rigoureusement compartimentés. Or si l'informatique

traditionnelle relève de l'investissement, le cloud computing s'inscrit dans des dépenses de fonctionnement.

Pour une plate-forme d'apps administratives

L'une des mesures recommandées est la création d'un directeur informatique dont le rôle est de piloter les budgets informatiques des administrations et de mettre en ligne une boutique d'applications à la disposition des collectivités locales qu'elles pourront utiliser à la demande. Il est également suggéré de modifier la politique de TVA à l'égard des services de cloud computing en l'alignant sur celle touchant les investissements. Aujourd'hui, les collectivités locales récupèrent la TVA sur les investissements informatiques, mais pas sur les achats de services cloud. Selon Alban Schmutz, le décret de modification serait prêt à Bercy. Il devrait être publié dans les semaines à venir.

Les autres mesures proposées sont : la mise en place d'un label de confiance pour les services de cloud en France, la création d'un dispositif d'aide aux entreprises dans leur migration vers le nuage, l'accompagnement des éditeurs de logiciels dans leur transition vers le modèle de service en ligne, le développement du cloud à usage personnel, le soutien à l'innovation, la construction d'un espace de confiance à l'échelle européenne, et l'amélioration de l'attractivité de la France pour l'implantation de datacenters de fournisseurs étrangers.

Les dix propositions vont être détaillées au sein de groupes de travail. Quatre groupes ont déjà démarré leurs travaux : celui sur la création de label sous l'égide de l'Anssi, l'agence française de cyber défense, celui sur la mise en place d'un espace de confiance au niveau européen sous la houlette de SAP et Atos, celui sur le cloud à usage personnel sous l'égide de JoliCloud, et celui sur l'accompagnement des éditeurs de logiciels sous l'égide d'OVH. Les autres groupes devraient être mis en place d'ici fin juin 2014. Le prochain bilan d'étape du plan est prévu pour septembre 2014.