Par Nicolas Nahmias et Emmanuelle Bénoit, avocats à la cour, AdDen avocats

PROTECTION DES DONNÉES

«Cloud computing» et marchés publics : garantir la confidentialité

- **L'«informatique en nuage» ou «cloud computing» permet à la personne publique de s'affranchir des contraintes liées à une infrastructure informatique complexe, et aux services publics de gagner en efficacité.**
- **Son utilisation pose cependant des questions sur la sécurité et sur la gestion des données transmises et stockées dans le cloud, qui est l'origine des normes mises en place depuis trois ans, fort utiles aux acheteurs publics.**

RÉFÉRENCES

- **Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**
- **Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel**
- **Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**
- **Normes ISO/CEI 27001, ISO/CEI 27002, ISO/IEC 17788, ISO/IEC 17789, ISO/CEI 27018**

Le «cloud computing» ou «informatique en nuage» désigne le stockage de données (telles que des fichiers de texte, des images et des vidéos) et de logiciels, auxquels les utilisateurs accèdent par internet en utilisant l'appareil de leur choix.

Selon la Commission nationale de l'informatique et des libertés (Cnil), il s'agit de la forme la plus évoluée d'externalisation, dans laquelle le client ou l'utilisateur dispose d'un service en ligne dont l'administration et la gestion opérationnelle sont effectuées par un sous-traitant (entendu comme celui qui traite les informations personnelles pour le compte du responsable de traitement, selon ses instructions). Ce type de services permet à la personne publique de s'affranchir des contraintes liées à une infrastructure informatique complexe (il suffit de disposer d'un ordinateur, d'une tablette ou d'un smartphone connecté à internet) et aux services publics de gagner en efficacité.

Le recours au cloud pose néanmoins d'assez nombreuses questions auxquelles les personnes publiques doivent impérativement être attentives : la sécurité des données transmises et stockées dans le cloud est-elle assurée ? Le choix du modèle économique de certains prestataires est-il compatible avec le fait que les personnes publiques gèrent des données sensibles, personnelles et d'intérêt général ? Ces problématiques et d'autres sont à l'origine d'une nouvelle norme qui peut s'avérer fort utile aux acheteurs publics.

I. La normalisation du cloud computing

● **Le cadre réglementaire.** La directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données constitue aujourd'hui le texte de référence, au niveau européen, en matière de protection des données à caractère personnel. Elle met en place un cadre réglementaire visant à établir un équilibre entre un niveau élevé de protection de la vie privée des personnes et la libre circulation des données à caractère personnel au sein de l'Union européenne (UE) (1). En France, c'est la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui constitue le fondement de la protection des données personnelles. Elle a notamment été modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui a transposé la directive de 1995.

Il existe également plusieurs normes internationales en matière de sécurité de l'information, et notamment la norme certifiante ISO/CEI 27001 Management de la sécurité de l'information et la norme ISO/CEI 27002 Technologies de l'information/Techniques de sécurité/Code de bonne pratique pour le management de la sécurité de l'information.

● **Les nouveaux textes.** Dans le prolongement de ces normes et dans le cadre de la stratégie de la Commission européenne visant à exploiter le potentiel du cloud computing en Europe (2), l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (IEC) ont très récemment élaboré trois textes spécifiques à ce domaine d'activité :

– la norme ISO/IEC 17788 Technologies de l'information/Informatique en nuage/Vue d'ensemble et vocabulaire ;

– la norme ISO/IEC 17789 Technologies de l'information/Informatique en nuage/Architecture de référence ;

– et la norme ISO/CEI 27018 Technologies de l'information/Techniques de sécurité/Code de bonnes pratiques pour la protection des informations personnelles identifiables dans l'informatique en nuage.

Cette dernière, publiée en juillet 2014, a pour but de protéger les données personnelles dans les services de cloud computing et d'améliorer la confiance dans les prestataires qui adhéreront à ces bonnes pratiques.

Plus précisément, le nouveau texte s'inscrit dans la perspective des objectifs et mesures de sécurité de la norme ISO/CEI 27002, ajoute des mesures supplémentaires pour

les prestataires de cloud computing (politique de sécurité de l'information, organisation de la sécurité de l'information, gestion des actifs, sécurité liée aux ressources humaines, cryptographie, gestion des incidents…) puis présente en annexe des mesures de sécurité additionnelles, spécifiques à la protection des données personnelles dans le cloud (consentement et choix, finalité et légitimité…).

Sont notamment consacrés par cette norme les principes suivants :

– la transparence : le lieu de stockage des données qui transitent sur le cloud doit être connu des utilisateurs, ainsi que le nom des éventuels sous-traitants appelés à intervenir ;

– la confidentialité : le prestataire de cloud doit conclure des engagements de confidentialité avec les membres du personnel qui ont accès aux données personnelles ;

– la conservation limitée des données : une politique de destruction des données personnelles à la fin du contrat doit être mise en œuvre par le prestataire ;

– la communication : le prestataire s'engage à informer son client ainsi que les autorités nationales en cas de faille de sécurité affectant les données ; en revanche, il ne doit pas divulguer d'informations aux autorités, sauf lorsqu'il y est tenu par la réglementation applicable. Dans ce cas, il s'engage à en informer le client, sauf interdiction légale ;

– la garantie d'un accès aux données : le prestataire doit permettre à ses clients de respecter les droits des personnes dont les données sont traitées, dont leur droit d'accès, de rectification ou de suppression de leurs données ;

– l'impossibilité pour le prestataire d'utiliser les données personnelles de ses clients à des fins publicitaires et de marketing, sauf avec le consentement exprès et préalable de ces derniers.

La soumission à cette norme devrait donc largement améliorer la sécurité et la confidentialité des données personnelles et ainsi rassurer les utilisateurs de cloud computing.

II. Le respect des normes relatives au cloud computing par les candidats à l'attribution de marchés publics

Ainsi que le relevait la Commission européenne dès 2012 (3), le secteur public dispose d'un pouvoir d'achat important dans le domaine informatique puisqu'il représente environ 20 % des dépenses en Europe. Comme le secteur privé, il a vocation à migrer vers le cloud, solution souple et évolutive, qui permet de s'affranchir de contraintes techniques fortes générées par une fonction support qu'il n'a donc pas nécessairement vocation à assurer directement.

Les principes que l'on vient d'énumérer, posés par la norme ISO/IEC 27018, répondent donc clairement aux préoccupations légitimes des personnes publiques en leur fournissant tout à la fois les clarifications et les garanties nécessaires.

Quel usage faire de cette norme ?

Compte tenu de la sensibilité du sujet et des données concernées, il serait souhaitable que la norme soit reprise en norme européenne et en norme française, puis que son respect soit imposé par le cahier des clauses administratives générales applicable aux techniques de l'information et de la communication (CCAG-TIC). A tout le moins, il conviendrait d'y intégrer les éléments essentiels (en reprenant les 6 items rappelés ci-dessus) de la norme, comme c'est le cas pour certaines normes dans le CCAG-Travaux, sans omettre pour autant de préciser explicitement son origine (les normes étant protégées par des droits de propriété intellectuelle). Compte tenu de l'intérêt de cette norme et de la relative nouveauté des offres cloud, il serait aussi souhaitable qu'une circulaire ou une fiche de la direction des affaires juridiques (DAJ) du ministère de l'Economie et des Finances y soit consacrée. Cela permettrait de donner rapidement de l'écho à cette norme ISO/IEC 27018 et aux principes qu'elle consacre, lesquels permettront sans aucun doute aux personnes publiques de mieux acheter, et en toute connaissance de cause, ce type de prestations. La norme pourra enfin être utilisée directement dans le cadre de la passation des marchés.

Définir ses besoins techniques

L'article 6 du Code des marchés publics impose que les prestations qui font l'objet d'un marché ou d'un accord-cadre soient définies, dans les documents de la consultation, par des spécifications techniques formulées, soit en termes de performances ou d'exigences fonctionnelles, soit par référence à des normes. L'acheteur public pourra donc, à terme, définir ses besoins et les spécifications techniques attendues, par référence à la norme ISO/IEC 27018. Il devra simplement admettre, comme le prévoit l'article 6-V, les candidats qui prouvent dans leur offre, par tout moyen approprié, que les solutions qu'ils proposent respectent de manière équivalente les spécifications techniques contenues dans la norme. Il peut également, dès à présent, demander aux candidats de satisfaire à des exigences fonctionnelles qui reprennent celles incluses dans la norme ISO/IEC 27018. Quant aux candidats, ils auront tout intérêt à mettre en valeur dans leurs réponses le fait qu'ils respectent la norme ISO et à mettre l'accent sur l'ensemble des garanties qu'elle apporte à l'acheteur. On peut surtout imaginer que la norme ISO/IEC 27018 et que le CCAG-TIC soient mis à jour pour intégrer les spécifications contenues dans la norme ISO, notamment dans son article 5 relatif à la confidentialité et les mesures de sécurité. Les acheteurs publics y gagneront sans aucun doute en sécurité et en efficacité. ■

(1) Ce cadre juridique est en cours d'évolution : en vue d'une plus grande harmonisation au sein de l'UE, la Commission a présenté le 25 janvier 2012 une proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données). Le texte a été adopté par le Parlement européen le 12 mars 2014, mais le Conseil européen ne s'est pas encore prononcé.

(2) Stratégie présentée dans son communiqué de presse du 27 septembre 2012.

(3) Communiqué de presse de la Commission du 27 septembre 2012 précité.