L'informatique en nuage au sein d'une étude d'avocats


DR

Sylvain Métille,
Dr en droit, avocat*.

Les PME peuvent, en recourant aux services d'informatique en nuage, acquérir à bon marché des technologies de haut niveau. Le lieu de traitement des données, leur cryptage ou leur répartition chez différents sous-traitants doivent être envisagés dans un but de précaution, en particulier s'il s'agit d'une étude d'avocats.

Toute utilisation d'un outil informatique, y compris d'un simple smartphone, nécessite et génère un certain volume de données qui doivent être enregistrées soit sur un support local (l'appareil lui-même), soit ailleurs (cet ailleurs étant atteint au travers d'un réseau, le plus souvent internet). A titre privé, le choix dépend souvent d'une question de confort et les réglages par défaut sont conservés. A titre professionnel, des obligations légales imposent de savoir ce qu'il advient de ces données et de faire, ensuite, les choix qui s'imposent.

Cet article présentera la notion d'informatique en nuage et les fausses croyances qui l'entourent, puis les obligations professionnelles de l'avocat. Les conséquences seront analysées selon que les données sont hébergées en Suisse ou à l'étranger, pour conclure, ensuite, avec quelques recommandations dépassant les exigences légales.

Informatique en nuage

L'informatique en nuage (infonuagique[1] ou *cloud computing*) réunit un ensemble de technologies et de modèles de services dans lesquels l'utilisation et la livraison d'applications informatiques, la capacité de traitement, le stockage et l'espace mémoire reposent tous sur internet[2].

Les fournisseurs d'informatique en nuage offrent toute une gamme de services, allant des systèmes de traitement de données à mémoire virtuelle (qui remplacent et/ou fonctionnent conjointement avec les serveurs classiques) aux services à l'appui du développement d'applications et aux services d'hébergement avancés, en passant par des solutions de logiciels en ligne qui peuvent remplacer les applications traditionnellement installées sur les ordinateurs des utilisateurs finals (notamment des applications de traitement de texte, d'agendas et de calendriers, de systèmes de classement pour le stockage de documents en ligne ainsi que de solutions de messagerie externalisée)[3].

Comme le relève à juste titre le Groupe de travail «article 29» sur la protection des données, l'informatique en nuage n'est pas négative par définition. Elle peut générer des avantages économiques considérables, sachant que les ressources à la demande sont faciles à configurer et à développer sur internet, où elles sont par ailleurs aisément accessibles. En outre, l'informatique en nuage peut également présenter des avantages du point de vue de la sécurité; les entreprises, notamment les petites et moyennes entreprises, peuvent ainsi acquérir, à un coût marginal, des technologies de haut niveau qui, normalement, dépasseraient leur budget.

Quatre mythes

Si le recours à l'informatique en nuage devrait simplifier le travail de l'utilisateur, il a aussi pour effet de le pousser hors de sa zone de confort[4]. Cette nouvelle configuration diffère de celle utilisée depuis des années et sur laquelle il avait une certaine maîtrise[5]. Pire encore, il perd le support physique qu'il pouvait voir dans son bureau et qui avait un côté rassurant. L'utilisateur doit donc apprendre à évaluer et à gérer des risques nouveaux.

La dématérialisation de ces services engendre beaucoup de mythes et de croyances fausses.

*Chargé de cours (Université de Lausanne et IIMT Fribourg), bloggeur (ntdroit.wordpress.com).

[1]Le substantif et l'adjectif «infonuagique »ont été proposés en novembre 2009 par l'Office québécois de la langue.

[2]Avis 05/2012 du Groupe de travail «article 29» sur la protection des données au sujet de l'informatique en nuage, adopté le 1er juillet 2012, p. 5, disponible sur http://bit.ly/1djRkN9. Voir également Préposé fédéral à la protection des données et à la transparence, Explications concernant l'informatique en nuage *(cloud computing)*, octobre 2011 disponible sur http://bit.ly/1djRpQQ.

[3]Avis 05/2012, op. cit., p. 5.

[4]ADKINS, Andrew Z., Law Firm Management in the Cloud: Leveling the Playing Field for Law Firms, disponible sur http://bit.ly/16NLNt4.

[5]Ou seulement une apparence de maîtrise.

Il n'y a premièrement pas de solution standard qui corresponde à toutes les situations. La taille de l'étude, les services recherchés, le type de données traitées (données confidentielles, jurisprudence librement accessible, etc.) doivent être pris en compte et permettent de définir des solutions très variables. Le service finalement retenu ne sera pourtant pas la solution miracle à tous les problèmes.

Deuxièmement, l'informatique en nuage ne présente pas, en elle-même un plus grand risque qu'une solution locale en termes de sécurité des données. Une solution en nuage représente indéniablement des risques, mais ils sont parfois moins importants que ceux liés à une infrastructure locale désuète, mal gérée ou facilement accessible par des tiers non autorisés. Un bon fournisseur de services informatiques, contrairement à l'avocat, dispose des ressources et des connaissances techniques adéquates.

Troisièmement, le prix: le principal avantage de l'informatique en nuage n'est pas toujours son prix. La solution la moins chère n'est souvent pas celle qui offre les meilleures garanties et prestations si l'on regarde bien les détails de l'offre et que l'on prend en compte tous les paramètres.

Quatrièmement, le *cloud* public n'est pas moins sûr qu'une infrastructure privée. On parle généralement de *cloud* privé lorsque l'infrastructure est réservée à un utilisateur, alors qu'il est public lorsqu'il est partagé entre plusieurs. C'est plutôt la manière dont il est géré, sa localisation, la sécurité des accès, les services proposés et les garanties données, qui sont déterminants, plutôt que le nom sous lequel il est vendu. Les mêmes remarques s'ajoutent à la distinction entre les services d'informatique en nuage proposés par une collectivité publique ou une entreprise privée.

Ainsi, c'est bien plus la prestation proposée et les conditions auxquelles elle est proposée qui font ses qualités et ses défauts, que la simple présence d'informatique en nuage.

Obligations professionnelles de l'avocat

L'avocat exerce sa profession avec soin et diligence[6]. La tenue de dossiers corrects, complets et cohérents concernant chaque cas fait partie intégrante de cette obligation. Elle découle notamment de l'obligation de rendre compte[7]. L'avocat est soumis au secret professionnel pour toutes les affaires qui lui sont confiées par ses clients dans l'exercice de sa profession et il veille à ce que ses auxiliaires respectent le secret professionnel[8]. Il est néanmoins courant que les avocats délèguent une partie de leurs tâches techniques, en particulier informatiques, à des spécialistes externes. Il n'existe cependant aucune réglementation spécifique que les avocats devraient obligatoirement respecter[9].

Lignes directrices du CCBE

Les lignes directrices du CCBE – conseil des barreaux européens – rappellent que l'avocat doit faire preuve de la diligence nécessaire quant au choix du fournisseur et aux conditions de l'accord de niveau de service[10] et que, avant de signer tout contrat, l'avocat doit vérifier l'expérience, la réputation, la spécialisation, le siège social et l'emplacement du fournisseur de services ainsi que l'adéquation de la solvabilité, la

Il n'y a premièrement pas de solution standard qui corresponde à toutes les situations.

fiabilité, la propriété et le capital du fournisseur; les conflits d'intérêts potentiels; les risques d'abus des données conservées; l'emplacement exact des serveurs de sauvegarde des données; dans la mesure du possible, la sécurité physique et électronique des serveurs et du centre de données où ils sont hébergés ainsi que les droits civil, pénal et public et réglementations applicables[11].

Le CCBE conclut de manière avisée que l'avocat devrait également évaluer la fiabilité de ses propres normes de sécurité internes en établissant des règles en matière de technologies de l'information, en fournissant des informations à son personnel et en le formant[12]. Cette remarque s'applique bien évidemment aussi à l'avocat qui n'utilise que des services informatiques hébergés et gérés localement[13].

La loi sur la protection des données

L'essentiel des données traitées par un avocat sont des données soumises à la loi fédérale sur la protection des données (LPD), soit des informations qui se rapportent à une personne identifiée ou identifiable[14]. Cela concerne les personnes tant morales que physiques.

Le traitement de données par l'avocat repose sur une obligation légale et le maître du fichier est libéré de l'obligation de déclarer le fichier tant qu'il est exploité dans un but couvert par l'activité classique de l'avocat. Le moyen technique utilisé pour gérer les dossiers (par exemple l'informatique en nuage) est sans influence sur l'exception à l'obligation de déclarer[15].

Du point de vue de la LPD, l'informatique en nuage sera considérée comme un traitement de données par un tiers[16] et, selon les cas, également comme une communication transfrontière de données[17]. L'utilisateur du service (en l'espèce l'avocat) restera débiteur du droit d'accès[18] et du droit d'effacer ou de rectifier les données[19]. Il doit s'assurer que le fournisseur de services garantit la sécurité des données[20].

Le traitement de données personnelles peut être confié à un tiers s'il se base sur la loi ou sur une convention (en l'occurrence, ce sera un contrat entre l'avocat et le fournisseur de services) et qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

L'existence d'une obligation de garder le secret n'exclut pas par principe, la possibilité de déléguer le traitement de données, mais il faut vérifier les conditions prévues par cette obligation spécifique[21], en l'espèce les normes applicables au secret professionnel de l'avocat[22].

L'art. 321 CP ne s'oppose pas à la délégation du traitement à des auxiliaires soumis au droit suisse, ceux-ci étant également tenus au respect du secret professionnel, pour les tâches de nature tant juridique que technique ou administrative[23]. Il est néanmoins de la responsabilité de l'avocat de s'assurer que ses auxiliaires respectent le secret professionnel[24].

Dans un cas de délégation de traitement, l'avocat serait bienvenu de conclure un accord de confidentialité avec son prestataire de services[25]. L'enregistrement de données de clients dans le nuage est donc permis pour l'avocat, y compris sans l'accord du client[26].

Il ne faut pas rejeter la délégation de traitement, parce qu'elle est liée à une infrastructure ou à un service informatique. Le risque d'utilisation d'un accès indu de l'hébergeur aux données

[6]Art. 12 lit. a LLCA.

[7]Art. 400 CO. Voir également BOHNET, François, MARTENET, Vincent, Droit de la profession d'avocat, Berne, 2009, pp. 1123-1128, et CHAPPUIS, Benoît, La profession d'avocat, Genève, 2013, pp. 34-36.

[8]Art. 13 LLCA et art. 15 CSD. Voir également BOHNET, / MARTENET, op. cit., pp. 764-766, et CHAPPUIS, op. cit., pp. 114-183.

[9]Voir également CHAPPUIS, op. cit., p. 135.

[10]Service Level Agreement. Ce contrat complète le contrat principal et définit la qualité du service fourni, notamment la performance minimale garantie du service et les conséquences si cette performance n'est pas atteinte.

[11]Conseil des barreaux européens, Lignes directrices du CCBE sur l'usage des services informatiques en nuage par les avocats, septembre 2012, p. 7, disponible sur http://bit.ly/TOFmkI.

[12]*Ibid.*

[13]Voir par exemple le Code de bonne pratique pour la gestion de la protection des données édicté par le Préposé fédéral à la protection des données et à la transparence (basé sur le Code de bonne pratique pour la gestion de la sécurité de l'information ISO 27002) disponible sur http://bit.ly/14Z9GLg.

[14]Art. 3 LPD. Les données anonymes ne sont pas concernées. Les données pseudonymisées, soit celles dont l'«anonymat» n'est que temporaire, sont soumises à la LPD. Nombre de données sont considérées à tort comme anonymes, alors que cet anonymat est réversible ou qu'il subsiste suffisamment d'informations pour identifier la personne. Sur la base du recensement américain de 1990, 87,1% des résidents US pouvaient être identifiés de manière unique avec la seule combinaison de leur numéro postal, leur date de naissance et leur sexe (Sweeney, Latanya, Uniqueness of Simple Demographics in the U.S. Population, Working Paper LIDAP-WP4, 2000).

[15]Art. 11a al. 5, lit. a LPD; ROSENTHAL, David, JÖHRI, Yvonne, Handkommentar zum Datenschutzgesetz, n. 64 *ad* art. 11a; Préposé fédéral à la protection des données et à la transparence, Exceptions pour les avocats, les médecins et les responsables des affaires du personnel, mai 2009, disponible sur http://bit.ly/15enRSv. Pour un avis contraire FANTI, Sébastien, Cloud computing: opportunités et risques pour les avocats, *in* Revue de l'avocat 2/2013, p. 77.

[16]Art. 10a LPD.

[17]Art. 6 LPD. Explications du Préposé fédéral à la protection des données et à la transparence concernant l'informatique en nuage *(cloud computing)*, octobre 2011, disponible sur http://bit.ly/16NOw5G.

[18]Art. 8 LPD.

[19]Art. 5 LPD.

[20]Art. 7 et 10a al. 2 LPD ainsi que 8 ss OPD. Avis 05/2012, op. cit., pp 17-20.

[21]MEIER, Philippe, Protection des données: fondements, principes généraux et droit privé, Berne 2011, pp. 429-431.

[22]Art. 13 LLCA, 15 CSD et 321 CP.

[23]MEIER, op. cit., pp. 430 ss; ROSENTHAL/JÖHRI, op.cit., N 106 *ad* art. 10a.

[24]Art. 13 al. 2 LLCA.

[25]Ainsi qu'une garantie d'indemnisation en cas de violation et /ou de dommage.

[26]SCHWANINGER, David, et LATTMANN, Stephanie S., Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, ch. 10, *in* Jusletter 11 mars 2013, disponible à http://bit.ly/1fgqYIw.

sera souvent bien moindre que les possibilités d'accès dont jouit le service de nettoyage de l'étude, l'étudiant qui vient classer des documents durant l'été ou encore le coursier qui livre un mémoire au tribunal ou au client.

Le fournisseur de prestations ne pourra évidemment pas effectuer un traitement de données plus étendu que celui que l'avocat lui-même est en droit d'effectuer[27].

Règles applicables si les données sont à l'étranger

La situation est plus compliquée si les données sont traitées à l'étranger, ce qui sera très souvent le cas[28]. Il faudra d'abord tenir compte des exigences de la LPD en matière de communication transfrontière[29]. Le principe est que celui qui traite des données dans un autre pays doit assurer une protection légale au moins équivalente à celle qui est garantie en Suisse. Celui qui exporte des données dans un pays n'offrant pas le même niveau légal de protection[30] doit soit apporter des garanties particulières (par le biais d'un contrat notamment), soit avoir l'accord de la personne dont les données sont traitées (ce qui implique qu'elle en soit clairement informée).

Le traitement des données à l'étranger joue ensuite un rôle s'agissant des obligations liées au secret professionnel. L'avocat restera soumis au droit suisse même si les données sont hébergées dans le nuage par une société étrangère. Il ne pourra toutefois pas s'assurer du respect du secret professionnel par ses sous-traitants étrangers, car ils ne seront pas soumis au CP suisse (en particulier l'art. 321 CP)[31]. Une obligation contractuelle pourrait ne pas être exécutable et, comme nous allons le voir, le droit impératif étranger peut aussi conduire à la violation du secret.

L'enregistrement de données couvertes par le secret professionnel de l'avocat dans le nuage à l'étranger (que les serveurs soient situés hors de Suisse ou gérés par une société étrangère) est donc interdit, sauf accord du client[32]. Si le maître du secret (en l'espèce le client) donne son accord à la délégation de traitement, la question du secret professionnel en tant que limitation à la délégation du traitement ne se pose évidemment plus[33].

En rendant accessible des secrets de fabrication ou des secrets d'affaires à une administration ou à une entreprise étrangère, l'avocat pourrait se rendre coupable de l'infraction de service de renseignements économiques à un organisme privé étranger[34]. L'information qui est chiffrée n'est pas à considérer comme accessible.

Cette disposition pénale ayant pour but de protéger l'Etat, l'accord du client ne serait pas suffisant à rendre le comportement licite[35]. Certains considèrent que l'accord du client à la transmission de l'information exclut la volonté de la garder secrète ou connue seulement d'un cercle très restreint. Ainsi, et pour autant qu'aucun intérêt public particulier ne s'y oppose, l'information n'est plus à considérer comme un secret protégé au sens de l'art. 273 CP[36]. Cette solution n'est pas très heureuse car une information devrait pouvoir être hébergée par un fournisseur de services étranger sans que son propriétaire doive renoncer à la protection offerte aux secrets commerciaux, mais cela semble bien être la seule solution actuellement. Cela peut néanmoins se comprendre en ce sens que celui qui accepte de confier une information sans avoir les moyens de s'assurer du maintien de sa confidentialité peut difficilement prétendre simultanément à la protection de cette confidentialité par le droit pénal, l'infraction de l'art. 273 CP étant une infraction intentionnelle. De manière pragmatique, on peut aussi retenir que le comportement de l'avocat relèvera plus de la négligence que d'une intention de rendre les données accessibles à un organisme officiel ou privé étranger (y compris sous l'angle du dol éventuel). Si l'on admet que l'intention doit porter également sur une exploitation (au moins théorique) des données dans un but de renseignement économique, on évite alors au Ministère public de la Confédération de devoir ouvrir une procédure pour chaque cas où des données sont accessibles depuis l'étranger.

Les données exportées depuis la Suisse vers un pays tiers seront finalement soumises au droit suisse (pour les protections qu'il apporte) et au droit du pays tiers (pour les possibilités d'accès à ces données en particulier des lois de procédure, de lois fiscales ou de lois sur les services de renseignement).

Le Foreign Intelligence Surveillance Act (FISA) permet par exemple au Gouvernement américain d'obtenir directement d'une entreprise américaine ou présente sur sol américain des informations qu'elle héberge et qui concernent des personnes qui ne sont pas des résidents US[37]. Les «non U.S. residents» sont exclus de la protection offerte par le 4e amendement et ne bénéficient en outre pas de la possibilité de saisir une autorité judiciaire. Si les USA sont souvent cités en exemple, presque tous les pays prévoient des dispositions simi-

laires et peuvent obtenir la remise d'informations auxquelles l'entreprise nationale a accès. Les conditions auxquelles ces données peuvent être obtenues varient et certains pays exigent par exemple un lien avec la commission d'une infraction pénale[38].

En transmettant ces informations, l'entreprise locale ne fera qu'appliquer la loi. Cet argument ne sera pourtant pas d'un grand secours pour l'avocat suisse[39].

Au-delà des exigences légales

Une société ne sera guère heureuse de voir une autorité étrangère ou une société concurrente accéder à ses données, et cela même si la loi est respectée. De plus, une fois que les données ont été transmises ou enregistrées, la suppression des données originales ne supprimera pas les copies.

Personne n'aurait l'idée d'aller mettre une liasse de documents confidentiels dans le coffre-fort d'une société en faillite ou dont la gestion des affaires est sujette à caution, dans l'armoire sans clé d'un local ouvert au public et où le risque d'inondation est important ou encore dans un pays politiquement et économiquement instable.

Pourtant, lorsqu'il s'agit d'héberger des données informatiques, le choix se porte souvent sur la solution la moins chère, sans se poser la question de savoir où, comment et par qui les données seront traitées. Il n'est guère moins inquiétant d'avoir des données sur une feuille imprimée dans un local ouvert que des données dans un serveur facilement accessible dans un pays inconnu. L'importance de la solidité financière du prestataire et la possibilité de retrouver ses données en cas de défaillance de ce dernier sont des aspects souvent négligés[40].

Conclusions

Avant d'utiliser l'informatique en nuage, il est essentiel de définir les services actuellement utilisés et ceux qui sont souhaités. Si l'informatique en nuage est préféré, il faut alors bien choisir son fournisseur et vérifier les prestations qu'il propose (y compris le niveau de services, les prestations proposées en cas de résiliation ou de faillite). On prendra ensuite garde au lieu de traitement des données, aux possibilités pour le sous-traitant de sous-déléguer le traitement, aux devoirs d'information du sous-traitant (en cas de faille de sécurité, de transmission de données, etc.), aux garanties apportées et aux possibilités d'indemnisation. Le choix d'un sous-traitant (y compris un simple hébergeur de données ou un fournisseur de messagerie électronique) dépendra donc d'abord du type de données traitées.

Des moyens techniques sont également judicieux comme le cryptage des données ou la répartition segmentée des données chez différents sous-traitants, de sorte que les données présentes chez un fournisseur ne puissent pas être lues sans la partie détenue par un autre fournisseur.

Dans certains cas, la seule solution sera un hébergement dans le même pays (voire pour l'Etat sur ses propres serveurs) ou limité à quelques pays. La limitation s'applique tant à la «nationalité» de la société qui gère les données qu'au lieu où sont les données.

Et, une fois que le service est prêt à être déployé, il ne reste plus qu'à informer ses clients et à obtenir les consentements requis. ▮

[27]Art. 10a al. 1 lit a. LPD. Cela exclut aussi un traitement dans un autre but que celui dans lequel les données ont été récoltées.

[28]La majorité des fournisseurs de services d'hébergement sont américains (comme Amazon, Apple, Google, Microsoft, etc.).

[29]Préposé fédéral à la protection des données et à la transparence, La communication de données à l'étranger en 24 questions, avril 2011, disponible sur http://bit.ly/17jvBP6; MEIER, op. cit., pp 436-476; MÉTILLE, Sylvain, Swiss Information Privacy Law and the Transborder Flow of Personal Data, Journal of International Commercial Law and Technology, Vol. 8, N° 1 (2013), disponible à http://bit.ly/XEHjnP; ROSENTHAL/JÖHRI, op.cit, N 1-103 ad art. 6; WALTER, Jean-Philippe, La communication de données personnelles à l'étranger, in Die Revision des Datenschutzgesetzes, EPINEY, Astrid, HOBI, Patrick (Eds.), Zurich 2009, pp. 99-137.

[30]Les Etats membres de l'Union européenne ou parties à Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) sont réputés offrir un niveau de protection équivalent pour les données des personnes physiques. Le Préposé fédéral à la protection des données et à la transparence tient une liste des pays adéquats disponible sur http://bit.ly/oBTRNn.

[31]SCHWANINGER, op. cit., ch. 31 ss.

[32]ROSENTHAL / JÖHRI, op. cit., N. 108 *ad* art. 10a.

[33]ROSENTHAL / JÖHRI, op. cit., N 109 *ad* art. 10a.

[34]Art. 273 CP.

[35]Le véritable maître du secret au sens de cette disposition, soit celui en faveur de qui la protection est souhaitée, est l'Etat et non le client: Petit Commentaire du Code pénal, DUPUIS, Michel et alii, N. 31 *ad* Art. 273 CP; CORBOZ, Bernard, Les infractions en droit suisse, vol. II, Berne 2010, N. 18 *ad* art. 273 CP.

[36]DONATSCH, Andreas, WOHLERS, Wolfgang, Strafrecht IV, Zurich, 2011, p. 349.

[37]Van HOBOKEN, Joris, ARNBAK, van EIJK, Nico, Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act, Amsterdam, novembre 2012, disponible sur http://bit.ly/1dLDTEt.

[38]Pour des exemples concernant l'Allemagne, l'Australie, le Canada, le Danemark, l'Espagne, la France, l'Ireland, le Japon et le Royaume-Uni: MAXWELL, Winston, WOLF, Christopher, A Global Reality: Governmental Access to Data in the Cloud, mai 2012, disponible sur http://bit.ly/12FRjjb.

[39]A moins que le client n'ait donné son accord au traitement de ses données à l'étranger.

[40]En cas de faillite, les données ne seront pas considérées comme des objets corporels dont la restitution peut être revendiquée: SCHWANINGER / LATTMANN, op. cit., ch. 51 ss.