SECRET PROFESSIONNEL DE L'AVOCAT ET SOLUTIONS *CLOUD*

BENOÎT CHAPPUIS
Avocat, Professeur aux Universités de Genève et Fribourg

ADRIEN ALBERINI
Avocat, Docteur en droit, LL. M. (Stanford)

Mots-clés: informatique, secret professionnel, diligence, organisation d'étude, protection des données

Le développement de services informatiques en cloud a été spectaculaire ces dernières années et permet aujourd'hui le stockage d'informations et une accessibilité à distance pour des activités professionnelles. Les avocats sont évidemment concernés par cette évolution qui n'a pas manqué de susciter des craintes concernant la confidentialité des informations stockées. Contrairement à un certain nombre d'idées reçues, le recours à un cloud, s'il présente certes des risques spécifiques, apporte également un regain de sécurité par rapport aux moyens traditionnels, pour autant que l'on prenne un certain nombre de précautions techniques et juridiques. Enfin, la question du secret professionnel de l'avocat, qui a été décrite comme problématique par certains, ne constitue pas un obstacle lorsque l'on utilise l'hébergeur du cloud comme un auxiliaire de l'avocat dans l'accomplissement de tâches que ce dernier doit contractuellement accomplir envers son client.

I. Introduction

Les offres de solutions *cloud*[1] se sont multipliées ces dernières années à l'attention du grand public (Dropbox, pour citer un exemple connu). Il en va de même de solutions souvent plus sophistiquées développées pour des professionnels.[2] Cette évolution touche également la profession d'avocat, en particulier avec la disponibilité de solutions permettant de stocker les dossiers clients chez le fournisseur IT et d'y accéder en ligne.[3]

La question est d'autant plus importante qu'elle est appelée à se poser de façon accrue dans les années à venir; en effet, grâce aux progrès techniques, on assiste à la création d'études dites «virtuelles», en ce sens qu'elles ne disposent plus de locaux propres, mais organisent leur travail et le stockage des informations par le seul moyen de l'informatique à distance. La légalité et la faisabilité de telles solutions fait l'objet de débats dans nombre de systèmes juridiques, en particulier européens, débats qu'on n'analysera pas ici.[4] Il faut cependant garder à l'esprit l'existence de cette évolution, tant il est vrai qu'elle est inéluctable, comme elle l'est pour tous les autres domaines de l'activité économique.

Dans la perspective de l'avocat et du respect de son secret professionnel, le *cloud* est souvent perçu comme un

1 Pour une présentation générale du *cloud computing,* voir par exemple la page du Préposé fédéral à la protection des données dédiée à cette pratique: https://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=fr. Pour une approche commerciale et contractuelle du *cloud,* voir par exemple l'ouvrage de TOLLEN, The Tech Contracts Handbooks, Cloud Computing Agreements, Software Licenses, and Other IT Contracts for Lawyers and Businesspeople, ABA Section of Intellectual Property Law, Second Edition, 2016.

2 Sur la concurrence intense en matière d'offres *cloud,* voir par exemple Le Temps, Google veut se renforcer dans le cloud, 19. 3. 2017. Voir également Le Temps, Evernote gagne 75 000 usagers par jour, 3. 4. 2017.

3 Pour des contributions sur les questions à se poser en cas d'adoption d'une solution *cloud,* voir SURY/GOGNIAT, Umzug einer Kanzlei in die Cloud, Revue de l'Avocat 2015/5, p. 201, et FANTI, Cloud computing: opportunités et risques pour les avocats, Revue de l'Avocat 2013/2, p. 74. Pour la détermination d'une stratégie IT appropriée dans une étude d'avocats, voir les contributions de LAUX, The End of Lawyers? – Ableitungen aus Susskinds Thesen mit Blick auf IT in der Anwaltskanzlei, Revue de l'Avocat 2015/1, p. 5, et Planung von Kanzlei-IT, Revue de l'Avocat 2015/2, p. 69. Pour une contribution sur le choix du logiciel de gestion d'étude, voir FANTI/LOTTAZ, Die digitale Kanzlei, Revue de l'Avocat 2014/8, p. 311.

4 Sur cette question, CHAPPUIS, La profession d'avocat. Tome II: La pratique du métier: De la gestion d'une étude et la conduite des mandats à la responsabilité de l'avocat, 2e édition, Genève, Zurich, Bâle 2017 (cité «Tome II»), p. 17–21 et 31–33.

facteur de risque et ce, il est vrai, pas totalement à tort. En cas d'utilisation d'une solution *cloud,* les données clients ne sont plus, ou en tout état plus intégralement, stockées physiquement dans l'infrastructure IT de l'étude. La maîtrise de ces données est donc confiée à un tiers, ou à tout le moins partagée avec celui-ci.

D'un autre côté, le *cloud* constitue également une opportunité pour les avocats. Le recours à ce type de solutions permet d'éviter l'acquisition et le maintien d'une infrastructure IT souvent source de coûts importants. En outre, et bien que cela puisse paraître paradoxal, les solutions *cloud* peuvent garantir une sécurité accrue des données et de leur traitement.[5]

La discussion relative à l'utilisation de solutions *cloud* par les avocats n'est pas nouvelle. Selon notre expérience, elle reste toutefois souvent limitée à des postulats de principe, et voit s'opposer de manière dogmatique les «anti-*cloud*» et les «pro-*cloud*». En outre, la discussion peine généralement à progresser en raison d'une compréhension incomplète, voire d'une mauvaise compréhension, des éléments technologiques sous-jacents.

Après une brève présentation introductive de la notion de solutions *cloud* pour avocats (I), la présente contribution soutient que la discussion sur la légalité de l'utilisation de solutions *cloud* dans la perspective du respect du secret professionnel en tant que telle est dépassée (II) et qu'il convient plutôt de se focaliser sur celle de l'organisation appropriée d'un système *cloud* afin de se conformer aux règles professionnelles de l'avocat (III). Cette dernière partie permet par ailleurs de montrer qu'en pratique, *i. e.* en tenant compte de la réalité organisationnelle de la plupart des études, une solution *cloud* peut s'avérer plus sûre qu'une solution traditionnelle.

II. *Cloud:* quelques composantes

L'utilisation d'une solution *cloud* peut se définir, de manière générale, comme l'accès à distance à des composantes IT, soit une infrastructure IT *(hardware)* et/ou à des fonctionnalités IT *(software).* Ces composantes IT ne sont donc pas installées physiquement à l'étude, mais chez le fournisseur de services; il y a ainsi externalisation par l'étude de toute ou partie de son système informatique.[6]

En cas d'utilisation d'une solution *cloud,* l'infrastructure minimale qui doit être installée à l'étude est la suivante: des terminaux, comme un moniteur (écran) ou un téléphone mobile, et éventuellement des périphériques (clavier, souris), ainsi qu'un client léger *(thin client)* de type Wyse. Dans une telle situation, le recours au *cloud* est intégral: l'infrastructure de l'étude ne comprend aucun espace de stockage de données (absence de disque dur et de serveur) et, par conséquent, aucune donnée ne se trouve physiquement à l'étude.[7] Il est possible de disposer d'une combinaison de *cloud* et d'accès en local, par exemple en cas d'utilisation de logiciels installés sur un ordinateur portable (qui comprend par définition un espace de stockage) et, en parallèle, d'accès au moyen de l'ordinateur portable à des logiciels installés chez le fournisseur IT.

En outre, l'utilisation d'une solution *cloud* nécessite de disposer d'un accès internet, que ce soit via un réseau physique (avec cable ethernet qui relie l'infrastructure IT au réseau) ou mobile (en cas d'utilisation d'un téléphone portable ou d'une tablette). La liaison avec le fournisseur se fait généralement via un canal sécurisé VPN (*virtual private network,* avec fonction de cryptage des données).

S'agissant des fonctionnalités IT pour avocats accessibles par *cloud,* il y a typiquement la suite office de Microsoft lorsqu'elle hébergée chez le fournisseur IT, les services de messagerie (qui peuvent en partie reposer sur la suite office en cas d'utilisation de outlook), les solutions de gestion d'étude (organisation et classement des dossiers), les solutions de sécurité (*firewall* et antivirus) ainsi que les solutions de comptabilité et de facturation. En termes d'infrastructure IT, on mentionnera essentiellement les serveurs de stockage et les serveurs de réseau. Des solutions plus complexes peuvent également être accessibles par *cloud,* comme les logiciels de *e-discovery* utilisés dans les enquêtes internes.[8]

III. Légalité du *cloud:* une discussion dépassée

1. Observations liminaires

À notre connaissance, la question de la compatibilité de solutions *cloud* avec le secret professionnel de l'avocat est discutée, à tout le moins informellement, au sein de plusieurs commissions de surveillance et ordres d'avocats cantonaux. Aucune interdiction ou sanction n'a, semble-t-il, été prononcée en lien avec cette pratique. À noter encore que la FSA ne s'est pas encore prononcée sur ce sujet.

Il a récemment été soutenu par Wohlers que l'externalisation du traitement de données, y compris au moyen de solutions *cloud,* par les personnes soumises au secret constitue une violation de l'art. 321 CP, à moins que le consentement explicite ou par acte concluant du maître du secret n'ait été préalablement obtenu.[9] Le raisonne-

5 Nous reviendrons sur ce point – fondamental – à plusieurs reprises dans le cadre de la présente contribution.

6 Les composantes IT sont fournies en tant que services, raison pour laquelle on parle généralement, pour la partie logicielle, de software-as-a-service (SaaS) et, pour la partie infrastructure, d'infrastructure-as-a-service (IaaS); l'intégralité des services est souvent abrégée XaaS.

7 À noter que, contrairement à la conception erronée que l'on entend encore parfois, les données ne sont pas «perdues» quelque part dans un nuage, mais physiquement enregistrées sur les serveurs du fournisseur de services.

8 Les diverses composantes IT peuvent être fournies par un seul ou par plusieurs fournisseurs IT.

9 WOHLERS, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB)/Externalisation du traitement des données et secret professionnel (art. 321 CPS), Zurich 2016, p. 21 et 27 ss. Wohlers considère par ailleurs que l'art. 321 CPS ne s'applique pas en cas de cryptage des données empêchant le fournisseur IT d'avoir accès à leur contenu (p. 21). Un tel cryptage, empêchant totalement l'accès aux données par le fournisseur IT, est toutefois difficile à mettre en œuvre en pratique.

ment effectué par Wohlers est en substance le suivant: le fournisseur IT ne constitue pas un auxiliaire du mandataire car le fournisseur IT ne participe pas à l'exécution du mandat (la notion d'auxiliaire étant donc interprétée très restrictivement) et, en outre, le recours à un tel tiers n'est pas prévisible pour le client. Il est donc impératif, pour échapper à l'application de la norme pénale, que le maître du secret consente à la communication de l'information protégée par le secret audit fournisseur IT.[10]

2. But poursuivi par l'article 321 CP

On commencera par rappeler que la *ratio legis* de l'art. 321 CP consiste en la protection de plusieurs biens juridiques. Certes, cette disposition protège la sphère intime et privée du particulier, qui doit pouvoir se fier entièrement à la discrétion du professionnel. Mais elle protège également l'intérêt du professionnel à ce qu'un rapport de confiance existe avec son client et, plus généralement, l'intérêt de l'État à un exercice correct et sans entrave de professions particulièrement importantes pour le bon fonctionnement de la société (autrement dit, l'intérêt du public dans les institutions, en l'occurrence celle de l'avocat).[11]

Ces objectifs appellent la réflexion suivante: on ne voit pas en quoi la confiance du particulier et du public plus généralement pourrait être mise à mal si une solution *cloud* appropriée est mise en place par l'avocat. Une telle solution est, dans les faits, même souvent plus sûre, comme cela sera discuté ci-après, qu'une solution *in-house* ou qu'une externalisation plus classique consistant à remettre physiquement des supports de sauvegarde à un tiers. Partant, mettre l'accent, par le biais d'une interprétation restrictive de la notion d'auxiliaire, sur le consentement du mandant ne nous paraît pas conforme au but visé par l'article 321 CP.

En outre, mettre l'accent sur le consentement du client nous paraît constituer en réalité une position fortement sous-tendue par des considérations relevant de l'autodétermination informationnelle, c'est-à-dire par le droit fondamental de l'individu de déterminer l'utilisation faite de ses données personnelles.[12] Or, de telles considérations ont été développées dans le cadre du droit de la protection des données. Et dans ce domaine, c'est précisément le principe opposé qui s'applique en matière de sous-traitance, à savoir que le consentement de la personne concernée n'est pas requis en cas de sous-traitance (même en présence de données sensibles[13]), pour autant bien entendu que la sous-traitance réponde aux exigences fixées par l'art. 10*a* LPD.[14] La justification qui sous-tend ce régime est le fait que la responsabilité liée au traitement des données demeure auprès de la personne qui confie le traitement au tiers.[15] Par conséquent, si l'on entend suivre des considérations relevant de l'autodétermination informationnelle en droit pénal, il ne nous paraît pas justifié que le droit pénal s'écarte et vienne faire échec, par une interprétation restrictive de la notion d'auxiliaire, au principe applicable en droit de la protection des données au cas particulier de la sous-traitance à un tiers.[16]

3. Auxiliaire et devoir de diligence

Il est généralement considéré qu'est un auxiliaire, au sens de l'art. 321 CP, celui qui concourt à l'exécution du mandat dont est chargée la personne soumise au secret. Cela exclut, par exemple, le personnel de nettoyage qui n'est en aucune façon appelé à traiter des informations confidentielles ni à assister l'avocat dans l'exécution de sa mission.[17] Il n'en va en revanche pas de même du secrétariat, dont la fonction est d'accompagner l'avocat dans chacun des pas de son travail, y compris dans le traitement des informations concernant les clients.

Cela dit, cette notion toute générale de «concours à l'exécution du mandat» doit être définie plus précisément. La structure des études d'avocats, restée jusqu'à récemment très traditionnelle, n'a pas suscité de réflexions détaillées sur la question. En revanche, d'autres professions, par leur caractère technique, requièrent de nombreux intervenants aux côtés du mandataire. Il suffit de penser au chirurgien qui, le plus souvent, ne peut intervenir sans que plusieurs personnes ne l'assistent. De l'anesthésiste aux instrumentistes en passant par le personnel de la salle d'opération, nombreuses sont les personnes qui concourent à l'exécution de l'opération. La qualité d'auxiliaire du médecin reconnue à ce personnel n'a jamais été mise en cause.[18]

Le travail de l'avocat ne se limite pas à la stricte exécution de la mission dont il a été investi par le client, qu'il s'agisse de la conduite d'un procès, de la rédaction d'un contrat ou de l'établissement d'un avis de droit. Ses obligations contractuelles, en particulier son devoir de diligence, impliquent qu'il gère les informations reçues, qu'il les conserve – y compris à la fin du mandat –, qu'il détecte les conflits d'intérêts, qu'il respecte les nombreux

10 WOHLERS (n. 9), p. 21 ss.
11 ATF 142 II 307, consid. 2; 135 III 597, consid. 2c = SJ 2001 I 381; BOHNET/MARTENET, Droit de la profession d'avocat, Berne 2009, N 1804–1807; CHAPPUIS, La profession d'avocat, Tome I – Le cadre légal et les principes essentiels, 2e édition, Genève, Zurich, Bâle 2016 (cité «Tome I»), p. 163–166, CR LLCA-MAURER/GROSS, art. 13 N 66–73; DUPUIS ET AL., PC CP, Bâle 2017, art. 321 N 11 ss; FELLMANN, Anwaltsrecht, Berne 2010, N 466 ss; SCHILLER, Schweizerisches Anwaltsrecht, Zurich 2009, N 386–387.
12 Sur cette notion, voir par exemple FLÜCKIGER, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, PJA 2013/6, p. 837.
13 BK DSG-RAMPINI, art. 12 N 15.
14 Voir la page du Préposé fédéral à la protection des données consacrée au *cloud computing:* https://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=fr. La révision en cours de la LPD ne remet pas en question l'approche actuellement en vigueur; voir en particulier le Rapport explicatif du DFJP du 21. 12. 2016 concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales, para. 1.4.1.
15 BAERISWYL, in Baeriswyl/Pärli, Datenschutzgesetz, Berne 2015, art. 10a N 7 ss.
16 Contra, WOHLERS (n. 9), p. 46–47.
17 CHAPPUIS, Tome I (n. 11), p. 179 et références citées.
18 CHAPPUIS, Tome II (n. 4), p. 161. Nuancé, WOHLERS (n. 9), p. 55.

délais auxquels il est tenu, qu'il établisse une facturation régulière et précise, qu'il tienne la comptabilité du client, qu'il soit prêt à rendre compte de sa gestion en tout temps, et bien d'autres tâches encore.[19] Bon nombre de ces obligations contractuelles impliquent que l'avocat fasse appel à des tiers non-avocats (secrétaires, comptables, archivistes, etc.), qu'ils soient internes ou externes à l'étude.[20] Toutes ces personnes doivent être considérées comme pour des auxiliaires de l'avocat dans l'accomplissement de son mandat.

4. Fournisseur IT comme auxiliaire

Il se trouve que le traitement de l'information est aujourd'hui devenu très largement, sinon exclusivement, électronique. On ne peut que prendre comme un fait acquis que, dans la société actuelle, l'avocat ne peut plus travailler – et le pourra encore moins à l'avenir – sans un très large recours à l'informatique et à la digitalisation des informations. Cette évolution ne concerne évidemment pas la seule profession d'avocat, mais l'ensemble des professions et, plus largement, de la société.

Cela ne veut à l'évidence pas encore dire que toute évolution technique légitime en elle-même le recours à n'importe quels moyens nouveaux. Encore faut-il qu'ils ne soient pas expressément interdits par la loi (par exemple les art. 179bis ss CP réprimant les infractions contre le domaine secret ou le domaine privé) ou qu'ils ne représentent pas une mise en danger des intérêts du client. Il s'agit donc de s'interroger sur le but et le contenu des moyens techniques auquel on recourt.

Les données informatiques se caractérisent par leur vulnérabilité. Une grave panne de serveur ou un incendie (ou encore un cambriolage) sont susceptibles d'anéantir en quelques instants des années de collecte d'informations. Se pose alors la question du stockage, de la protection et de la conservation de ces dernières.

Il est simplement inconcevable que l'avocat se contente de les conserver sur son ordinateur personnel ou le serveur installé dans les locaux de son étude. Il ne satisferait pas à son devoir de diligence, puisqu'il serait à la merci des effets d'une panne ou d'un incendie et exposé au risque de ne pouvoir ni accomplir son mandat correctement, ni rendre compte de son travail, comme il le doit aux termes de l'art. 400 CO.

À cet égard, on doit se souvenir que la jurisprudence du Tribunal fédéral est sévère et que ce n'est que de manière très exceptionnelle qu'il reconnaît l'existence d'une force majeure. Cette dernière est interprétée strictement, notamment en droit civil.[21] Il doit s'agir de circonstances extraordinaires avec lesquelles on ne pouvait pas compter et d'une force irrésistible, ce qui, par exemple, selon le Tribunal fédéral, n'est pas le cas d'orages et de pluies importantes durant l'été en montagne.[22] On doit garder à l'esprit cette conception de la jurisprudence, compte tenu de la possible gravité des conséquences d'une panne électrique soudaine sur un système informatique, ce que les orages – qui ne sont pas non plus rares en ville – peuvent provoquer. Cette question joue un rôle tout particulier s'agissant du respect des délais, le Tribunal fédéral précisant que «le justiciable doit prendre les précautions nécessaires dans l'éventualité d'une panne informatique, technique ou électrique».[23] Sa conception se résume finalement en une phrase: «l'avocat doit s'organiser de manière à pouvoir respecter les délais même en cas d'empêchement».[24]

Face aux risques de pertes de données, nombre d'avocats ont mis au point des systèmes permettant de les dupliquer, le plus fréquent consistant à les sauvegarder sur des disques externes mis en sécurité dans un lieu tiers (par exemple un coffre bancaire). Outre le fait que ce système est contraignant sur le plan pratique, il mène à des transports réguliers de données confidentielles hors de l'étude, ce qui représente en soi un risque non négligeable: le simple vol physique de la serviette du transporteur aurait pour résultat de livrer l'entier des données conservées sur le disque à celui qui se l'est approprié. On ne parlera pas même ici du risque considérable que représente la conservation ou le transfert de données sur des clefs USB, façon de procéder pourtant extrêmement répandue en pratique. Aisément perdues, elles contiennent souvent moult fichiers anciens susceptibles d'être dévoilés à l'occasion de la remise de la clef à un tiers ou en cas de perte. Sauf à être gérées de façon extrêmement rigoureuse, ces solutions sont rapidement apparues comme comportant des risques importants et, partant, peu satisfaisantes.

C'est ainsi naturellement que le recours à un professionnel chargé de la conservation et la protection des données informatiques est devenu une nécessité puisqu'il constitue – dans l'état actuel de la technique – le seul qui soit efficace, sauf peut-être pour les études de très grandes dimensions susceptibles de disposer de moyens internes suffisants. Ce professionnel externe est dès lors chargé de l'une des missions contractuelles de l'avocat qui est celle de la gestion, de la conservation et de la protection des données confidentielles réunies dans l'exécution des mandats de l'avocat. Il assure ainsi la tâche qui, pendant des décennies, a été dévolue au secrétariat et à l'archiviste de l'étude.

En conséquence, il n'existe aucun motif théorique de ne pas le considérer comme un auxiliaire. Reste alors à déterminer à quelles conditions le recours à cet auxiliaire doit être soumis pour remplir les exigences du secret professionnel.

---

19 Pour une présentation de l'ensemble des obligations contractuelles de l'avocat, CHAPPUIS, Tome II (n. 4), p. 189 ss.

20 FELLMANN (n. 11), N 486; CORBOZ, Les infractions en droit suisse, vol. II, 3^{e} éd., Berne 2010, art. 321 CP N 16; TRECHSEL/VEST, in Trechsel/Pieth (éd.), StGB PK, 2^{e} éd., Zurich, St-Gall 2013, art. 321 N 13.

21 ATF 111 II 429, consid. 1b; CR CO I-WERRO, art. 41 N 46.

22 ATF 100 II 134, consid. 5; SCHWENZER, Schweizerisches Obligationenrecht Allgemeiner Teil, 7^{e} éd., Berne 2016, N 20.02. Pour d'autres exemples, CR CO I- WERRO, art. 41 N 46.

23 TF, 1B_222/2013, consid. 3.1.

24 ATF 119 II 82, consid. 2a = SJ 1993 237.

IV. Organisation du *cloud:* une discussion inachevée

1. Observations liminaires

La question des exigences minimales que l'avocat doit respecter en cas de recours à une solution *cloud* afin de garantir le respect du secret professionnel (et de se conformer à ses autres obligations professionnelles, en particulier l'obligation de diligence dans l'organisation de l'étude) n'a, à notre connaissance, été que relativement peu traitée à ce jour.[25]

Au niveau du principe, on peut se demander s'il faut exiger le respect d'une réglementation lourde. Par exemple, la question se pose de savoir si l'avocat doit se conformer à des exigences similaires à celles applicables aux banques (également tenues à une obligation de secret) et, partant, si l'on ne devrait pas appliquer la Circulaire Outsoucing de la FINMA *mutatis mutandis* aux avocats. À l'évidence, une telle approche risquerait de faire peser une charge réglementaire excessive sur les avocats, dont les structures et la manière de pratiquer diffèrent substantiellement de celles des banques. Cela étant, ce type de question permet de réfléchir au niveau de réglementation qu'il convient d'appliquer à l'avocat.

Traiter de manière exhaustive les obligations auxquelles l'avocat doit se conformer lorsqu'il procède à une externalisation dans un système *cloud* excèderait le cadre de la présente contribution. Dans les sections qui suivent, nous abordons les points qui nous paraissent essentiels à ce sujet; une distinction peut être opérée entre les obligations qui concernent l'organisation de la relation entre l'avocat et son fournisseur IT et les mesures qui doivent être prises au sein de l'étude lorsqu'une solution *cloud* est implémentée.

2. Organisation de la relation avec le fournisseur IT

Le fournisseur IT étant un auxiliaire de l'avocat, la discussion devrait se focaliser sur la thématique du respect – dans ce contexte particulier – des trois *curae* (choix, instruction et surveillance du fournisseur).[26] À notre sens, c'est surtout sur la question du choix du fournisseur qu'il convient de mettre l'accent. Le choix d'un fournisseur qui connaît bien les exigences de la profession réduit fortement le besoin de l'instruire. Quant à la surveillance, la plupart des avocats ne disposent pas des compétences pour la mettre en œuvre de manière appropriée. Ce qui précède conduit pratiquement à dire que l'avocat devrait se tourner presque exclusivement vers un fournisseur IT qui propose une solution *cloud* spécifiquement structurée pour les avocats (ou des professions similaires comme les médecins).[27]

Il faut éviter de faire preuve de trop de formalisme dans ce contexte. Le respect des trois *curae* exige bien plutôt que l'avocat choisisse le fournisseur qui a fait ses preuves sur le marché et s'assure auprès dudit fournisseur qu'il mette en œuvre les mesures techniques et organisationnelles adéquates. Ainsi, s'agissant du choix du fournisseur, on ne s'attachera pas uniquement aux certifications dont il dispose, même si de telles certifications constituent évidemment un point positif. Dans le même esprit, on ne saurait pas non plus exiger la conclusion d'un contrat écrit de fourniture de services IT régissant chaque paramètre de la relation entre le fournisseur et l'avocat. Cela étant, il faut au moins que le fournisseur IT s'engage à offrir une solution spécifiquement adaptée à la profession d'avocat.

Spécifiquement, une solution *cloud* destinée aux avocats devrait présenter essentiellement les caractéristiques suivantes:[28]

- Les données doivent être stockées en Suisse, avec un système de *back-up* (suffisamment distant) en Suisse. L'exigence d'une localisation en Suisse est importante, afin d'éviter que le secret de l'avocat ne soit mis en péril par des mesures judiciaires ordonnées par les autorités étatiques étrangères, dans le pays où le serveur est installé, obligeant son exploitant à leur donner accès aux informations qui y sont conservées.[29] Dans une telle hypothèse, il est peu probable que l'avocat soit en mesure d'opposer à cette mesure le secret dont il peut se prévaloir en Suisse selon les lois de procédure (art. 160 al. 1 let. b, 163 al. 1 let. b et 166 al. 1 let. b CPC; art. 171 et 264 CPP; art. 30 et 50 al. 2 DPA; art. 16 al. 2 et 17 PA).
- Les serveurs qui hébergent les données doivent se situer dans un *data center* qui offre une sécurité accrue (notamment avec une redondance sur les points-clés de l'infrastructure tels que les réseaux électriques et internet). On ne saurait en revanche exiger une séparation physique des données, une séparation logique étant suffisante.[30]
- Des mesures techniques et organisationnelles doivent être instaurées pour que l'accès aux données de l'avocat et de ses clients par les employés du fournisseur soit limité au nécessaire. Il faut également que le fournisseur IT soit organisé techniquement et opérationnellement pour réagir en cas ce cyberattaque contre le système.

---

25 Voir par exemple les Lignes directrices du CCBE sur l'usage des services d'informatique en nuage par les avocats, du 7. 9. 2012, disponibles à l'adresse http://www.ccbe.eu/NTCdocument/07092012_FR_CCBE_gui2_1347539443.pdf. Voir également FANTI (n. 3). S'agissant des obligations que l'avocat doit respecter de manière plus générale en lien avec les moyens informatiques qu'il utilise, voir CHAPPUIS, Tome II (n. 11), p. 28 ss, et JEANNERET, Le «risk management» dans un étude d'avocats, in: Jeanneret/Hari (éd.), Défis de l'avocat au XXIe siècle – Mélanges en l'honneur de Madame le Bâtonnier Dominique Burger, Genève 2008, p. 400 ss.

26 À noter que si l'avocat a reçu le pouvoir de se substituer quelqu'un, il ne répond que du soin avec lequel il a choisi le sous-mandataire et donné ses instructions (art. 399 al. 2 CO).

27 Dans le même esprit, Jeanneret (n. 25), p. 401 (trois premiers *bullet points* en fin de page).

28 Ces caractéristiques reflètent en bonne partie celles recommandées de manière générale pour tout système informatique par JEANNERET (n. 25), p. 401 ss.

29 CHAPPUIS, Tome II (n. 4), p. 24 et 31; FANTI (n. 3), p. 75.

30 La séparation physique implique que l'avocat se voie attribuer un serveur distinct par le fournisseur IT, alors que la séparation logique signifie que les données de plusieurs études peuvent être stockées sur le même serveur (mais distinguée de manière logicielle). La séparation physique engendre des coûts considérablement plus élevés que la séparation logique.

- La transmission de données par l'avocat dans le système *cloud* doit se faire au travers d'un canal sécurisé, type VPN (*virtual private network,* avec fonction de cryptage des données).
- Le fournisseur IT doit garantir la mise en place et la gestion continue de logiciels performants contre les intrusions (antivirus, *firewall,* etc.).
- Le fournisseur IT doit disposer d'un service de support et de maintenance offrant des temps de réponse rapides, en particulier en cas de requête de l'avocat de niveau de sévérité critique.
- Il est enfin important que l'avocat ne devienne pas captif du fournisseur IT dans la durée. Partant, le fournisseur IT doit garantir la portabilité des données de l'avocat et de ses clients (avec migration des données de manière structurée).

À noter encore que, si les grandes études disposent en principe des infrastructures et du personnel permettant d'atteindre un niveau de sécurité correspondant à celui offert par un fournisseur IT garantissant les paramètres énumérés ci-dessus, on peut douter que toutes les études moyennes et petites y parviennent. Dans ce type d'études, les serveurs ne sont pas toujours installés dans des pièces adéquates, et le *back-up* de données n'est pas effectué, dans tous les cas, de manière régulière et dans des centres de stockage offrant les garanties suffisantes. Il n'est pas non plus certain que les logiciels protégeant contre les intrusions soient toujours parfaitement conformes à l'état de la technique et régulièrement mis à jour (et ce, sur le poste de chaque employé). Dans ces circonstances, une solution *cloud* peut s'avérer plus sure qu'une solution traditionnelle.

3. Organisation au sein de l'étude

Le recours à une solution *cloud* a pour conséquence – par définition – de déplacer la gestion du système IT chez le fournisseur de services; dans ces circonstances et comme on l'a dit, les obligations de l'avocat se limitent au respect des trois *curae.* Cela dit, certaines mesures restent de la responsabilité de l'avocat. À défaut de les mettre en œuvre, l'avocat risque de ne pas être en conformité avec ses règles professionnelles.[31]

Dès lors que l'accès aux données de ses clients se fait à distance, l'avocat doit disposer d'une connexion internet de qualité. Cela signifie choisir une offre suffisamment rapide (si possible basée sur la fibre optique jusque dans les locaux – souvent abrégée *FTTH*) et, ce qui est souvent moins connu en pratique, un câblage suffisant dans l'étude (sans quoi le bénéfice d'une connexion rapide peut être perdu). Il faut également qu'un système de *switch* en cas de coupure de réseau soit installé. Un tel système permet de basculer du réseau physique au réseau mobile (4G ou 3G) en cas d'interruption de fonctionnement du réseau physique. À noter que la mise en place d'un *switch* efficace est indispensable pour les études qui ont opté pour un pur système *cloud, i. e.* un système ne comprenant que des terminaux, car aucune fonctionnalité n'est disponible en cas de coupure du réseau.[32]

En cas d'utilisation d'un terminal portable (*laptop,* tablette, *smartphone*) hors de l'étude permettant d'accéder aux dossiers clients, l'avocat doit mettre en place un système d'accès aux données clients comprenant un mot de passe spécifique et qui doit être modifié régulièrement. En revanche, il nous paraît excessif de requérir l'installation d'une signature digitale par le biais d'un élément de *hardware* supplémentaire type *token* ou d'autres solutions similaires offertes par les banques pour le e-banking, même s'il est vrai que ces solutions offrent une sécurité plus importante. S'agissant plus spécifiquement des téléphones portables, il est conseillé de limiter l'accès aux e-mails, compte tenu du risque accru de perte ou de vol; autrement dit, il est préférable de ne pas donner la possibilité d'accéder à l'intégralité des dossiers par le biais de téléphones portables.[33]

On soulignera encore que la majeure partie des failles de sécurité et des fuites de données sont le fruit d'inadvertances ou de malveillance de la part d'employés. Partant, que l'on opte pour une solution *cloud* ou un système plus traditionnel, c'est sur ce point qu'il convient de rester le plus attentif, par une sensibilisation continue de l'ensemble des membres de l'étude à propos de la diligence dont ils doivent faire preuve en lien avec l'utilisation de systèmes informatiques (mot de passe, non-utilisation d'espace de stockage externe type clé USB, disque dur externe, *Dropbox,* etc.).[34]

V. Conclusions

L'adoption par l'avocat d'une solution *cloud* est, sur le principe, conforme à son obligation de garder le secret professionnel et aux autres obligations professionnelles auxquelles il est soumis. Cela étant, il est essentiel, dans ce cadre, que l'avocat choisisse le bon fournisseur IT et s'assure que l'organisation de la solution *cloud* est adéquate. Dans cette perspective, certains paramètres nous paraissent essentiels, comme l'utilisation par le fournisseur IT de serveurs de stockage dans un *data center* en Suisse et offrant une sécurité accrue; on ne saurait toutefois fixer

31 Il est intéressant de consulter, à titre d'exemple, les recommandations publiées par l'American Bar Association, intitulées «Cloud Ethics Opinions Around the U. S.» (https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html); cf. également, CHAPPUIS, Tome II (n. 4), p. 17–21 et 32–33.

32 En lien avec la question de la qualité de la connexion, on relèvera les risques liés à l'utilisation d'un wifi au sein de l'étude, ainsi que le besoin de mettre en place une stratégie contre les cyber-risques.

33 On relèvera en outre les risques, en cas de voyage à l'étranger, découlant de la possibilité d'avoir un accès informatique à l'intégralité des dossiers clients. Voir à ce sujet Chappuis, Tome II (n. 4), p. 33.

34 Voir également Chappuis, Tome I (n. 11), p. 29 ss. Dans ce cadre, on gardera à l'esprit les difficultés qui peuvent se poser en cas de mise en œuvre d'une politique de *«bring your own device».* Voir à ce sujet la page du Préposé fédéral à la protection des données: https://www.edoeb.admin.ch/datenschutz/00763/01249/index.html?lang=fr.

des exigences trop importantes, sur le modèle de l'*outsourcing* bancaire par exemple, au risque sinon de faire peser une charge réglementaire excessive sur les études d'avocats.

Dans une perspective pratique, on soulignera que l'adoption d'une solution *cloud* peut même constituer, pour nombre d'études de petite et moyenne taille, l'approche offrant les meilleures garanties de sécurité, notamment dans les cas où les études ne disposent pas de l'infrastructure et des compétences suffisantes pour gérer leur système informatique.

Qu'il opte pour une solution traditionnelle ou *cloud,* l'élément essentiel pour l'avocat est, au final, à l'approche de 2020, de disposer d'une infrastructure et de solutions IT adaptées. En outre, à défaut d'en saisir toutes les subtilités techniques, l'avocat doit à tout le moins comprendre les composantes de son système informatique. Cet effort est d'autant plus important que la prochaine vague de technologies de l'information qui concernera la profession – comprenant notamment les *legal marketplaces,* la résolution des litiges en ligne, l'intelligence artificielle, la *blockchain,* ou encore le stockage de données sur ADN[35] – sera significativement plus complexe.[36]

35 Voir Le Temps, Le stockage de données sur ADN décolle, 10.1.2017.

36 Voir notamment GURTNER, L'innovation et l'avenir de la profession d'avocat, Revue de l'Avocat 2017/1, p. 15. Voir également la page de la Stanford Law School consacrée aux *legal tech:* https://techindex.law.stanford.edu/.