ORDRE DES AVOCATS
DE GENÈVE

De l'actuelle loi sur la protection des données (LPD) au projet de révision du 15 septembre 2017 (P-LPD) en passant par le nouveau règlement européen sur la protection des données du 27 avril 2016 (RGPD)

A. Préambule

1. Le 15 septembre 2017, le Conseil fédéral a publié son message **concernant la révision totale de la loi fédérale sur la protection des données (P-LPD)**[1].

   Le fil conducteur de cette modification est la responsabilisation des maîtres de fichier, avec pour eux l'augmentation d'un certain nombre d'obligations, corollairement au renforcement des droits des personnes concernées par la collecte de données.

   Cette révision tend également à opérer en droit suisse les adaptations nécessaires pour se conformer au droit européen et plus particulièrement au **Règlement général sur la protection des données européen (RGPD ; 2016/679)** et à la **Directive UE 2016/680 tous deux adoptés le 27 avril 2016** et entrés en vigueur conjointement le 25 mai 2018.

2. Le **P-LPD**) est en cours de traitement par **le Conseil national** lequel vient toutefois d'annoncer qu'il scindait en deux l'examen du projet[2].

3. Dans un premier temps, les débats législatifs se concentreront donc sur la seule entrée en vigueur de la Directive UE 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes dans le domaine du droit pénal, considérée comme un développement de l'acquis de Schengen. Ce premier point ne concerne donc pas le traitement de données par des privés.

4. Ce n'est que dans un second temps (et *« sans contrainte de temps »* [3]) que seront examinées par le Conseil national les questions relatives au traitement de données par des particuliers dans le cadre d'une refonte complète du droit suisse à la lumière du RGPD. Entre les lignes, cela signifie peut-être que les chambres souhaitent avoir un peu de recul sur les premières expériences générées par l'entrée en force du droit européen avant de lancer la réforme de droit suisse.

   Il est donc désormais peu vraisemblable que, s'agissant du traitement de données par des particuliers, le nouveau droit suisse de la protection des données entre en vigueur en 2018, voir même début 2019, comme cela était annoncé dans un premier temps.

5. La décision que vient de prendre le Conseil national apparaît d'ores et déjà regrettable, à la lumière des débats entourant l'entrée en force prochaine de la réglementation européenne.

   D'une part, comme le souligne le Message du Conseil fédéral du 15 septembre 2017 (ci-après « le Message »), la compatibilité du droit suisse au droit réglementaire européen est indispensable, pour que la Suisse soit considérée par l'Union européenne comme un Etat tiers ayant un niveau de protection des données suffisant et que la possibilité d'échanger des données avec elle soit préservée. Tel est certes déjà le cas en l'état, puisqu'une décision d'adéquation a été rendue en 2000 concernant la Suisse, sur la base de la LPD actuelle

[1] FF 2017 6565.
[2] Communiqué de presse de la Commission des institutions politiques (CIP-N) du 12 janvier 2018.
[3] *Idem.*

considérée comme répondant aux impératifs de sécurité tels que définis par le droit de l'Union européenne. Dans la mesure où cette décision est relativement ancienne, on ne peut toutefois complètement exclure qu'elle ne soit remise en question après l'entrée en force du RGPD[4].

D'autre part et surtout, le **RGPD**, même s'il ne fait pas partie des acquis de Schengen, comporte d'importants effets extra-territoriaux[5].

Ce règlement européen, d'application immédiate, prévoit en effet à son article 3 al. 2, son application à toutes entreprises (cas échéant étrangères) offrant des biens et des services à des personnes sur le territoire de l'UE (qu'un paiement soit ou non exigé).

Ces dernières sont en outre obligées de désigner un « représentant » dans l'un des Etats membres de l'Union Européenne dans lesquels elles agissent (art. 27 RGPD[6]), représentant coresponsable – avec le responsable du traitement et le sous-traitant – en cas d'*« actions en justice »* (art. 27 al. 5 RGPD)[7].

La portée de l'art. 3 al. 2 RGPD prête évidemment à interprétation[8]. Selon certains, ce n'est par exemple pas en soi l'existence d'une clientèle française qui crée l'assujettissement, mais bien l'offre faite à cette clientèle.

En tout état, à ce stade, faute d'éléments suffisants pour déterminer quelle sera l'étendue en pratique du champ d'application du RGPD, il n'est pas invraisemblable de considérer qu'une étude d'avocats genevoise, disposant d'un site internet offrant explicitement les services de l'étude à une clientèle locale et internationale, dont une partie de la clientèle est effectivement européenne, pourrait être susceptible de tomber sous le coup de la réglementation européenne et partant d'une série de devoirs accrus en matière de protection des données, ce avant-même l'entrée en force de la nouvelle LPD. Ce constat est encore accru par la situation géographique particulière du canton par rapport à la France et le nombre important de personnes frontalières susceptibles de recourir aux services d'avocats genevois dans le cadre de difficultés rencontrées au quotidien, par exemple en matière de droit du travail ou d'assurances sociales.

D'emblée il apparaît que l'application directe du RGPD aux entreprises suisses crée une regrettable insécurité juridique que le législateur suisse ne semble pas avoir anticipée. De son côté, dans une notice récemment parue, le Préposé suisse à la protection des données laisse pour l'essentiel aux entreprises suisses le soin de prendre connaissance de leurs droits et obligations directement auprès des autorités européennes[9].

6. En l'espèce, il nous a initialement été demandé de mettre en exergue les éventuelles conséquences des modifications législatives **du droit suisse** prévues dans le projet du Conseil fédéral du 15 septembre 2017 pour les études d'avocat et leur fonctionnement en matière de données.

   Dans la mesure toutefois où le RGPD est susceptible d'une application directe, il nous a semblé nécessaire de l'inclure dans notre analyse.

   La présente note identifie donc une série de sujets qui nous ont semblé pertinents, puis compare pour chacun de ces sujets : (1) les règles applicables aujourd'hui selon la LPD, (2) la teneur du P-LPD - qui, pour une grande part, reprend les principes de la LPD actuelle tout en les adaptant au RGPD 2016/679 – et enfin (3) la teneur de ce dernier règlement.

[4] Dans ce sens, FANTI Sébastien, Le nouveau Règlement général sur la protection des données et la Suisse in EF 11/2017 p. 861 (ci-après « Le nouveau Règlement »).
[5] FANTI, Le nouveau Règlement, *op cit.*, p. 856 et ss, notamment p. 858 et ss.
[6] Cette disposition prévoit certes une exemption à son article 27 al. 2 let. a. Il est toutefois loin d'être certain qu'une étude d'avocats puisse remplir les conditions de cette exemption.
[7] Au vu des sanctions potentielles prévues par le RGPD (cf. *infra*), le coût d'une telle représentation peut s'avérer potentiellement important.
[8] La doctrine allemande propose de se référer aux critères identifiés par la jurisprudence en matière de contrat de consommation telle que développée dans le cadre de l'article. 6 du Règlement (CE) n° 593/2008 du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I) ; cf. FANTi, Le nouveau Règlement, *op. cit.*, p. 859 et références citées.
[9] *Cf.* la fiche du Préposé suisse à la protection des données du mois de janvier 2018 intitulée « Le RGPD et ses conséquences sur la Suisse ».

B. Champ d'application matériel

7. La loi fédérale du 19 juin 1992 sur la protection des données (ci-après : « LPD »)[10] vise à protéger la personnalité des personnes physiques ou morales qui font l'objet d'un traitement de données (art. 1 et 2 LPD) et donc à garantir le droit fondamental à la sphère privée (art. 13 al. 2 Cst). Elle s'applique notamment au traitement des données personnelles concernant des personnes physiques ou morales effectué par des personnes privées (art. 2 al. 1 let. a LPD), avocats inclus, à l'exclusion du traitement de données effectués pour un usage exclusivement personnel.

   L'usage des données dans un cadre professionnel (par ex. fichier de patientèle d'un médecin, fichier de clientèle et de parties adverses d'un avocat) est en principe soumis à la LPD[11].

   Tout au plus, l'article 2 LPD exclut-il du champ d'application de la loi le traitement de données personnelles dans le cadre de procédures civiles, pénales ou administratives, à l'exception des procédures administratives de première instance. L'application de cette exclusion est restrictive puisqu'elle ne vise que la période durant laquelle la procédure est pendante et est régie par les dispositions spéciales de procédure.

   La LPD s'applique en revanche *avant* la litispendance, notamment pour la phase qui voit l'auteur du traitement récolter des données qui lui serviront dans la procédure à venir, et *après* la clôture de la procédure[12].

8. **Sous l'angle du P-LPD**, il n'en ira pas différemment, de sorte qu'il appartiendra aux avocats, maîtres de fichiers de données (désormais désignés comme « responsables du traitement » dans la nouvelle terminologie de la loi), de continuer à veiller dans leur pratique au respect des dispositions la nouvelle LPD.

   Le champ d'application de la loi reste pour l'essentiel identique, sous réserve du fait que le P-LPD propose de renoncer à la protection des données des personnes morales (ce qui est également le cas du RGPD).

   Par ailleurs, le Message rappelle que si des traitements de données personnelles sont régis par des dispositions de protection des données prévues dans d'autres lois fédérales, celles-ci sont en principe applicables en vertu du principe de la priorité des dispositions spéciales sur les dispositions générales[13].

9. Le champ d'application matériel du **RGPD** est décrit à son article 2. Il s'applique à tout traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

   Sont exclues uniquement les activités ne relevant pas du champ d'application du droit de l'Union, les activités menées par les Etats membres dans des domaines visés par le chapitre 2 du titre V du traité sur l'UE (par exemple les activités militaires), les activités des personnes physiques dans un cadre strictement personnel ou domestique, ainsi que les activités soumises à la Directive UE 2016/680 (art. 2 al. 2 RGPD).

   Le champ d'application du RGPD est donc large et s'applique notamment aux avocats, comme le souligne le Conseil des barreaux européens (CCBE)[14] qui a publié sur son site des recommandations et lignes directrices afin d'aider les barreaux des différents Etats membres à préparer l'entrée en force du règlement.

[10] RS 231.1.
[11] MEIER Philippe, Protection des données, Fondements, principes généraux et droit privé, Stämpfli (Berne), 2011, p. 187, N° 382.
[12] MEIER, *op. cit.*, p 190 N° 392 et 394.
[13] FF 2017 6631.
[14] *Cf.* www.ccbe.eu, «<lignes directrices du CCBE sur les principales nouvelles mesures de conformité des avocats au règlement général sur la protection des données » et « recommandations du CCBE pour la mise en œuvre du règlement général sur la protection des données ».

C. Des principes généraux applicables et de l'introduction d'une nouvelle règle : le droit à l'oubli

10. Aujourd'hui, l'article 4 **LPD** énonce les principes fondamentaux que tout traitement de données doit respecter, soit notamment la licéité, la proportionnalité et la conformité à la bonne foi.

    Ces principes sont complétés par ceux figurant aux articles 5 à 7 LPD, à savoir le principe d'exactitude (art. 5 al. 1 LPD), le droit de rectification (art. 5 al. 2 LPD) ainsi que le principe de sécurité (art. 7 al. 1 LPD).

11. Ces principes sont repris dans le **P-LPD** aux articles 5 et 7 P-LPD, lesquels ajoutent, par rapport au texte actuel, un devoir du responsable du traitement de détruire ou d'anonymiser les données dès qu'elles ne sont plus nécessaires au regard des finalités du traitement.

    A notre sens, cette règle - nouvelle - doit être gardée à l'esprit en matière d'archivage des dossiers. Une fois le dossier terminé, les données devraient être archivées dans une base spécifique distincte de la base active, afin notamment de devenir inaccessibles aux personnes n'ayant plus d'intérêt à les traiter. Les documents introduits dans des bases de données (exemples, modèles) devraient en toute hypothèse être anonymisés d'emblée même s'ils sont uniquement à la disposition des avocats de l'étude.

12. Les principes énoncés dans le P-LPD correspondent dans les grandes lignes aux principes édictés par le **RGPD.**

    A noter toutefois que, s'agissant du principe même de la licéité du traitement, le CCBE[15] adopte une approche formaliste et recommande aux barreaux de prendre des mesures afin de s'assurer que leur système national de réglementation offre une base juridique explicite pour le traitement général de données à caractère personnel réalisé par les avocats, ce en référence à l'article 6 al. 1 let. e RGPD qui prévoit que le traitement est licite notamment s'il est *« nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement »* (cf. également l'art. 6 al. 2 RGPD). A cet égard, le CCBE distingue les activités judiciaires des activités « hors litige », lesquelles pourraient ne pas automatiquement entrer dans l'exception d'intérêt public, conseillant dès lors aux barreaux d'informer leurs membres sur la nécessité de demander le consentement exprès du client pour le traitement des données à caractère personnel dans le cadre d'activités juridiques hors litiges.

    À noter par ailleurs l'article 17 RGPD qui consacre une disposition entière au droit à l'oubli, soit à l'effacement des données à caractère personnel à l'issue du traitement pour lequel elles étaient nécessaires. L'alinéa 3 de cette disposition réserve la nécessité, pour le responsable du traitement, de respecter une obligation légale d'intérêt public (let. b) ainsi que celle de permettre la constatation, l'exercice ou la défense de droits en justice (let. e). A ce stade, (1) des doutes subsistent quant à l'étendue de la protection des activités de l'avocat « hors litige » et (2) les remarques émises ci-dessus en matière d'archivage sont pertinentes dans le cadre de l'application du règlement européen.

D. L'autorité en charge d'assurer le respect de la loi

13. L'article 26 LPD prévoit la nomination d'un préposé fédéral à la protection des données et à la transparence. En ce qui concerne le traitement de données par des privés, le rôle du préposé consiste à l'heure actuelle à donner des conseils (art. 28 LPD) et émettre des recommandations (art. 29 LPD).

14. **Le P-LPD** élargit et renforce les pouvoirs du préposé en prévoyant désormais que celui-ci puisse ouvrir, d'office ou sur dénonciation, une enquête contre un organe fédéral ou contre une personne privée (art. 43 P-LPD).

[15] *Cf.* www.ccbe.eu, recommandations du CCBE pour la mise en œuvre du règlement général sur la protection des données.

À teneur du projet, le préposé peut également rendre des décisions, que ce soit dans le cadre de l'enquête qu'il mène, au titre de mesures d'instruction – cas échéants sur mesures provisionnelles – (art. 43 et 44 P-LPD), ou en présence de violations des dispositions du P-LPD, au titre de mesures administratives (art. 45 LPD). La violation d'une décision du préposé, assortie des menaces des peines de l'art. 57 P-LPD, est par ailleurs sanctionnée[16]. Les sanctions pénales seront en revanche prononcées par les juridictions pénales des cantons (art. 59 P-LPD).

La loi fédérale sur la procédure administrative[17] (laquelle réserve le secret professionnel dans certaines de ses dispositions) s'applique dans le contexte des enquêtes et décisions du préposé (art. art 46 LPD) dans le cadre desquelles seul l'organe fédéral ou la personne privée contre qui une enquête a été ouverte a la qualité de partie.

A notre sens, s'agissant de la protection des données au sein d'une étude d'avocats et de la possibilité prévue par le P-LPD de recourir à des mesures coercitives permettant l'accès aux locaux ou aux documents (art. 44 P-LPD), le P-LPD dans sa teneur actuelle n'est pas satisfaisant. Se pose notamment la question du caractère opportun de la compétence du seul Préposé fédéral (sans à tout le moins une collaboration avec l'autorité de surveillance de l'avocat concerné) pour traiter de tels dossiers et en tout état de l'étendue des pouvoirs du préposé compte tenu par ailleurs des nécessités de préserver le secret professionnel.

15. C'est le lieu de noter qu'en cas d'application directe du **RGPD** à des entreprises suisses, et nonobstant une controverse initiale sur ce sujet entre la doctrine et les autorités fédérales[18], les entreprises suisses sont très manifestement[19] soumises à la supervision – et cas échéant aux décisions – des autorités de contrôle[20] désignées par l'UE, lesquelles disposent elles aussi de pouvoir très étendus (y compris, en dernier recours, celui de prononcer des amendes pour des montants pouvant aller jusqu'à plusieurs millions d'euros)[21].

    L'article 58 RGPD décrit par ailleurs les pouvoirs – étendus – des autorités de contrôle lesquelles doivent, dans le cadre de leur enquête concernant des responsables de traitement localisés à l'étranger, solliciter l'entraide administrative des Etats concernés (cf. sur ce point le nouvel art. 49 P-LPD qui règlemente l'assistance administrative avec les autorités étrangères, et en particulier son al. 3 qui traite (à notre sens de manière **très** insatisfaisante[22]) de la question des données susceptibles de contenir des informations couvertes par le secret professionnel). Là encore, il conviendrait de prévoir une norme particulière pour les procédures concernant les avocats et la participation de l'autorité de surveillance de l'avocat concerné à la procédure d'entraide aux fins de préserver le secret professionnel.

    À noter que l'article 90 RGPD (« obligations de secret ») prévoit la possibilité pour les Etats membres d'adopter des règles spécifiques afin de définir l'étendue des pouvoirs des autorités de contrôle à l'égard des responsables de traitement ou de leurs sous-traitants, lorsque ceux-ci sont soumis à une obligation de secret professionnel ou à d'autres obligations de secret équivalentes en vertu du droit de l'Union ou de celui de l'Etat membre. L'article 90 al. 1 in fine RGPD précise encore expressément : *« Ces règles ne sont applicables qu'en ce qui concerne les données à caractère personnel que le responsable du traitement ou le sous-traitant a reçues ou obtenues dans le cadre d'une activité couverte par ladite obligation de secret ».*

    De son côté, la CCBE[23] propose l'introduction, dans les droits nationaux des Etats membres, d'une norme précisément applicable aux avocats, limitant les pouvoirs des autorités de contrôle tels qu'énoncés à l'article 58 al. 1 let. e et f (ordres de production et perquisitions) en

[16] *Cf. Infra*.
[17] RS 172.021.
[18] Sur ce débat, cf. FANTI, le nouveau Règlement., *op. cit*., p. 859.
[19] *Cf.* L'article 27 RGPD lequel requiert des entreprises étrangères tombant sous le coup de l'article 3 al. 2 RGPD de désigner formellement un représentant sur sol européen ; *cf.* également la fiche du Préposé suisse à la protection des données du mois de janvier 2018 intitulée « Le RGPD et ses conséquences sur la Suisse » laquelle, après avoir souligné que les autorités de protection européenne disposeront selon le nouveau droit de la compétence pour prononcer elles-mêmes des amendes *« effectives, proportionnées et dissuasives »* renvoie pour toute question additionnelle les entreprises suisses concernées à consulter une autorité de protection européenne comme la CNIL (France), la CPVP (Belgique) ou la CNDP (Luxembourg).
[20] *Cf.* Articles 51 et ss RGPD.
[21] *Cf. Infra*.
[22] Selon cette disposition : *« Avant de transmettre à une autorité étrangère des informations susceptibles de contenir des secrets professionnels, de fabrication ou d'affaires, il informe les personnes physiques ou morales détentrices de ces secrets et les invite à prendre position, à moins que cela ne s'avère impossible ou ne nécessite des efforts disproportionnés. ».*
[23] *Cf.* www.ccbe.eu, « recommandations du CCBE pour la mise en œuvre du règlement général sur la protection des données ».

les soumettant à un certain nombre de conditions, dont notamment l'autorisation du barreau de l'avocat concerné[24].

E. Du devoir d'information du maitre de fichier/responsable de traitement et du consentement de la personne dont les données sont traitées

16. A l'heure actuelle, l'article 4 al. 4 LPD requiert une simple « *reconnaissabilité* » de la collecte des données personnelles, en particulier les finalités du traitement, par la personne concernée. L'article 4 al. 5 LPD prévoit que « lorsque son consentement est requis pour justifier le traitement de données personnelles la concernant, la personne concernée ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée. Lorsqu'il s'agit de données sensibles et de profils de la personnalité, son consentement doit être au surplus explicite. ».

    L'article 11a LPD dispose que le préposé tient un registre des fichiers accessible en ligne. Ce registre a notamment pour but d'assurer la transparence de certains traitements de données et de faciliter l'exercice du droit d'accès. Toutefois, en vertu de l'article 11a al. 5 let. a LPD, lequel réserve le traitement de données traitées en vertu d'une obligation légale, les avocats ne sont d'ordinaire pas soumis à une obligation de déclaration de leurs fichiers. Cette exception découle selon la doctrine de l'obligation imposée aux avocats à teneur de la LLCA de tenir des dossiers corrects, complets et cohérents[25], découlant elle-même de leur obligation de soin et de diligence telle qu'énoncée à l'article 12 let. a LLCA.

    L'article 14 LDP impose quant à lui un véritable devoir d'information spontané et actif au maître du fichier en cas de « *collecte de données sensibles ou de profils de la personnalité* » destinée à entrer dans un fichier (art. 3 let. g LPD), lorsque celui-ci se trouve en Suisse ou que le tiers chargé de la collecte a son siège dans notre pays. Là encore, toutefois, par le renvoi de l'article 14 al. 5 LDP à l'article 9 al. 1 LDP[26], l'avocat maître du fichier en question peut refuser, restreindre ou différer l'information puisqu'il est soumis au secret professionnel en vertu des articles 321 CP et 13 LLCA.

17. **Le P-LPD** maintient le principe de la reconnaissabilité (art. 5 al. 3 P-LPD) de même que la notion de consentement prévu par l'actuelle LPD (art. 5 al. 6 P-LPD). En revanche, le devoir d'information spontané est étendu désormais à toute collecte de *« données personnelles »* et non plus seulement à la collecte de données sensibles. Est toutefois prévue, pour ce qui concerne les personnes privées, comme les avocats par exemple, une exception au devoir d'informer en raison d'une *« obligation légale de garder le secret »* (art. 18 al. 1 let. c P-LPD).

    Par ailleurs, la tenue d'un registre des fichiers par le préposé, de même que le devoir d'annonce de l'existence du fichier qui en découle, tels que prévus à l'art. 11a LPD, sont abandonnés dans le P-LPD.

18. De son côté, le **RGPD** prévoit une longue liste d'informations à donner à la personne concernée lors d'une collecte d'informations à son sujet. Il distingue toutefois les informations spontanées à fournir, lors de la collecte de données, selon si les données ont été collectées auprès de la personne concernée (art. 13 RGPD) ou non (art. 14 RGPD). Dans le second cas seulement, l'article 14 al. 5 let. d RGPD réserve le secret professionnel (tel que *« réglementé par le droit de l'Union ou le droit des Etats membres »*) lequel dispense de fournir la moindre information.

    La notion de consentement est par ailleurs décrite à l'article 7 RGPD, en imposant au responsable de traitement d'être en mesure de démontrer son existence. Lorsque ce consentement est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement doit être présentée « *sous une forme compréhensible et aisément accessible, et formulée en des termes claires et simple* » et distinguée des autres questions.

[24] *Cf.* Annexe.
[25] Sébastien FANTI, Cloud Computing : opportunités et risques pour les avocats, *in* Revue de l'Avocat, 2013, p. 74 à 77, p. 77.
[26] *Cf. Infra*.

F. Du droit d'accès à ses données personnelles par la personne sujet du traitement

19. L'article 8 **LPD**, complété par les articles 1 et 2 de l'Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (« OLPD »)[27], consacre le droit d'accès aux données personnelles pour la personne concernée, et ce indépendamment de toute atteinte à la personnalité. Le droit d'accès est en principe inconditionnel.

    Cependant, il peut être restreint par une loi au sens formel (art. 9 al. 1 let. a LPD) ou entrer en conflit avec des intérêts prépondérants, qu'ils soient publics, de tiers ou du maître du fichier lui-même (art. 9 al. 1 let. b et 9 al. 4 LPD).

    A l'heure actuelle, un avocat, maître de fichier, peut se fonder sur les articles 9 al. 1 let. a LPD en liaison avec les articles 321 CP et 13 LLCA pour refuser ou restreindre la communication de renseignements à autrui, étant entendu que ni ces dispositions, ni l'article 9 al. 1 let. a LPD ne peuvent être invoqués pour refuser de communiquer à son propre client des données personnelles le concernant[28]. En d'autres termes, ce dernier dispose notamment (en sus donc des règles applicables au mandat) de la faculté de se prévaloir de l'article 8 LPD vis-à-vis de son avocat. De son côté, le client d'un avocat est en droit de communiquer à ce dernier les données lui permettant d'analyser une question juridique, d'établir un contrat ou de rédiger un mémoire[29].

20. **A la lumière du P-LPD**, il en irait de même à l'avenir, les articles 23 et 24 P-LPD prévoyant à la fois :

    - le droit de toute personne de demander au responsable du traitement si des données personnelles la concernant sont traitées ainsi qu'un droit d'accès auxdites données (art. 23 P-LPD)

    - et des restrictions à ce droit d'accès lorsqu'une loi au sens formel le prévoit (art. 24 P-LPD).

    La question du droit d'accès par des tiers aux données de personnes décédées est pour le surplus réservée et traitée dans une norme séparée[30].

21. Le **RGPD** prévoit également le droit d'accès (et ses corollaires, à savoir un droit de rectification et un droit à l'effacement) à son article 15, sans – étonnamment – prévoir de réserve pour les cas couverts par un secret professionnel. La question se pose donc, dans ce contexte, de l'application par analogie de l'article 14 let. 5 RGPD[31].

G. Données de personnes décédées

22. A l'heure actuelle, la gestion des données de personnes décédées est régie par une seule disposition d'une ordonnance et non d'une loi (art. 1 al. 7 **OLPD**). Cette disposition a pour effet d'étendre un droit d'accès à des tiers (proches parents ou époux) pour les données d'un autre tiers (défunt) ce en contradiction avec le texte clair de la loi qui ne prévoit qu'un droit d'accès pour les données concernant personnellement la personne sollicitant l'accès (art. 8 LPD)[32].

23. **L'article 16 al. 1 P-LPD** institue désormais dans une norme idoine un droit d'accès aux données d'une personne décédée moyennant l'examen préalable d'un certain nombre de conditions (intérêt légitime ou proche parenté, mariage ou partenariat enregistré, concubinage ou exécuteur testamentaire ; absence d'interdiction par le défunt de son vivant ; absence d'intérêt prépondérant du responsable du traitement ou d'un tiers à la consultation).

---

[27] RS 235.11.
[28] BOHNET François/MARTENET Vincent, Droit de la profession d'avocat, Stämpfli (Berne) 2009, p. 160, N° 375 et références citées. Cf. par ailleurs, BENHAMOU Yaniv, BRAIDI Guillaume et NUSSBAUMER Arnaud, la restitution d'informations : quelques outils à la disposition du praticien, PJA 2017 pp. 1302 à 1317.
[29] BOHNET / MARTENET, *op. cit.* p. 160 N° 375 et références citées.
[30] *Cf. Infra*.
[31] *Cf. Supra*.
[32] Sur ces questions à la lumière du droit actuel, *cf.* EIGENMANN Antoine et FANTI Sébastien, Successions, données personnelles, numériques et renseignements, in SJ 2017 II p. 193 et ss, notamment p. 206 et ss.

A cet égard, quand bien même l'article 321 CP protège le secret professionnel au-delà du décès du maître du secret, l'article 16 al. 1 P-LPD s'appliquera aussi lorsque la demande de consultation portera sur des données protégées par le secret professionnel au sens de l'article 321 CP. L'article 16 P-LPD crée ainsi un nouveau motif justificatif pour le détenteur du secret, au sens de l'article 14 CP. Dans le cas où le responsable du traitement est un avocat et qu'il refuse l'accès en raison de son secret professionnel, les personnes légitimées selon l'article 16 al. 1 let. a P-LPD peuvent demander, à Genève, à la Commission du barreau de délier l'avocat en question de son secret. Notons que si l'avocat détenteur du secret a des doutes par rapport à la pesée des intérêts, il aura également la possibilité de se faire formellement délier de l'obligation de garder le secret professionnel par la Commission du barreau, à Genève[33].

L'article 16 al. 3 P-LPD institue également un droit, pour les héritiers ou l'exécuteur testamentaire, de faire détruire les données du défunt (droit à l'oubli). Cette disposition prévoit toutefois des exceptions, dont l'intérêt prépondérant du responsable du traitement, lequel inclut ses obligations légales de conservation s'opposant à un effacement[34].

24. Le **RGPD** ne prévoit pas de normes particulières s'agissant des personnes décédées.

H. La communication transfrontière de données

25. Selon l'article 6 al. 1 LPD, « *aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquat*».

L'article 6 LPD s'applique à tous les cas de délégation volontaire de traitement à l'étranger, que les données soient transférées à un tiers ou à un autre service ou collaborateur, sis à l'étranger, de la même entreprise[35]. Une série d'exceptions restrictives à ce principe – parmi lesquelles le consentement de la personne concernée – est par ailleurs prévue à l'alinéa 2 de l'article 6 LPD. Par ailleurs, le préposé publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat (art. 7 OLPD).

A noter que la simple détention de données sur sol étranger (au travers par exemple du *cloud computing*) peut équivaloir à une communication transfrontière. La problématique est accrue dans la mesure où par exemple les Etats-Unis ne sont pas reconnus comme un Etat assurant un niveau de protection adéquat, alors que les données sauvegardées dans le *cloud* sont le plus souvent hébergées aux USA ou par des sociétés américaines[36]. La problématique découle avant tout de droits d'accès ou de consultation par des autorités publiques nationales en vertu de leurs pouvoirs d'enquête ou de contrôle[37]. Il apparaît dès lors essentiel pour une étude d'avocats de veiller à n'utiliser des méthodes de *cloud computing* qu'après avoir vérifié avec attention l'ensemble des modalités applicables à ce type de services[38].

Peut également s'avérer problématique l'utilisation des e-mails dans les communications avec les clients et les tiers (confrères ou autres) lorsqu'ils se trouvent à l'étranger. Ce type de communication tombe en effet sous le coup de l'article 6 LPD via l'article 3 let. e LPD. En revanche, les données qui ne font que transiter dans un Etat étranger, sans y être traitées, alors que l'expéditeur et le récipiendaire sont en Suisse ne tombent pas sous le coup de l'article 6 LPD[39].

26. **Sous l'angle du P-LPD**, les principes applicables sont intégrés aux articles 13 et 14 LPD. La situation sera très pour une grande part semblable à la situation actuelle. Tout au plus, appartiendra-t-il au Conseil fédéral (et non plus au préposé ; art. 7 ODLP) d'établir une liste

[33] Article 321 al. 2 CP ; FF 2017 p. 6665.
[34] FF 2017 p. 6667.
[35] MEIER, *op. cit.*, p. 423-424, N° 1204.
[36] METILLE Sylvain, Confier ses données à une société étrangère n'est pas sans risque, *in* Medialex 2013 p. 63.
[37] FANTI Sébastien, Cloud computing, *op.cit.*, p. 74 et ss, p. 75.
[38] *Cf.* Sur ces questions CHAPPUIS Benoît, ALBERINI Adrien, Secret professionnel de l'avocat et solutions cloud, *in* Revue de l'Avocat 2017 p. 337 et ss.
[39] MEIER, *op. cit.*, p. 444, N° 1280.

des Etats considérés comme *« assurant un niveau de protection adéquat »*, dans laquelle en pratique tous les Etats membres de l'UE figureront. Le transfert de données personnelles vers ces Etats ne déclenchera pas d'exigences supplémentaires. Par ailleurs, un certain nombre de situations additionnelles, où la transmission de données sera autorisée, est précisé à aux articles 13 al. 2 et 14 al. 1 P-LPD. A noter, en cas de communication de données vers un Etat « *non adéquat* » mais couverte par une dérogation, qu'il existe un devoir d'information du préposé – sur demande de ce dernier – et partant la nécessité pour le responsable du traitement de documenter le transfert de données (art. 14 al. 2 P-LPD). Une sanction pénale en cas de violations des articles 13 et 14 P-LPD est par ailleurs prévue[40].

27. Le **RGPD** prévoit à ses articles 44 ss les modalités relatives au transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, en distinguant là aussi les pays avec ou sans niveau de protection adéquat.

I. Sécurité des données personnelles, « outsourcing » et obligation (nouvelle) d'annonce d'une faille de sécurité

28. Selon l'article 7 **LPD**, la sécurité des données doit être assurée. Le Conseil fédéral a édicté la liste des objectifs à atteindre à l'article 9 OLPD. Selon l'article 10a LPD, le traitement de données peut être confié à un tiers, à condition que celui-ci garantisse la sécurité des données.

Une partie de la doctrine[41] souligne à cet égard s'agissant des données numériques des avocats : *« 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'article 400 CO. »* pour conclure : *« C'est ainsi naturellement que le recours à un professionnel chargé de la conservation et de 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 grandes dimensions susceptibles de disposer de moyens internes suffisants. »*

Le traitement de données par un tiers selon l'article 10a LPD suppose la délégation par le mandant en charge de données personnelles d'opérations de traitement (art. 3 let. e LPD), sur tout ou partie de ces données, à une personne tierce[42]. La délégation n'est licite qu'aux conditions de l'article 10a LPD, soit en particulier pour autant qu'« *aucune obligation légale ou contractuelle de garder le secret de l'interdise* ». La violation par le mandant de ces règles légales ou contractuelles engage sa responsabilité contractuelle, pénale et/ou administrative[43]. Ainsi, le secret professionnel peut s'opposer à ce que le traitement de données personnelles soit confié par un avocat à un tiers (art. 10a al. 1 let. b LPD). S'agissant de l'article 321 CP, celui-ci ne s'oppose pas à la délégation du traitement à des auxiliaires, également soumis au secret professionnel. Dès lors qu'il n'y pas de violation du secret professionnel lorsque l'avocat délègue une partie de ses tâches à un auxiliaire (collaborateur, secrétaire, comptable)[44], il doit en aller de même, selon la doctrine majoritaire[45] (mais non unanime...)[46], en cas de recours à un professionnel externe à l'étude chargé de la conservation et de la protection des données informatiques de l'étude.

Dans les autres cas, la délégation du traitement ne sera en principe autorisée qu'en présence d'un motif justificatif, en particulier un fait justificatif pénal ou le consentement de la personne concernée. Lorsque la délégation est conforme à la loi, elle ne nécessite ni information, ni consentement de la personne concernée[47]. Pour le reste, la délégation ne dispense pas le mandant de l'ensemble de ses devoirs généraux en matière de protection des données,

[40] *Cf. Infra*.
[41] CHAPPUIS / ALBERINI, *op. cit.*, p. 340.
[42] MEIER, *op. cit.*, p. 421-422, N° 1196.
[43] MEIER, *op. cit.*, p. 431, N° 1232.
[44] CHAPPUIS / ALBERINI , p. 337 et ss, p. 340.
[45] CHAPPUIS / ALBERINI, *op. cit.*, p. 340 et ss.
[46] FF 2017 p. 6651.
[47] RSJ 2006 522 N° 35.

notamment le respect du principe de sécurité (art. 10a al. 2 LPD) ou de proportionnalité (art. 4 al. 2 LPD).

Comme le souligne la doctrine[48], c'est donc avec le plus grand soin qu'il y a lieu de procéder au choix du tiers chargé de la protection des données et aux instructions données à celui-ci. Il est notamment important – pour ne pas dire indispensable - que celui-ci soit familier des exigences de la profession et bien entendu des règles applicables en matière de protection des données.

A noter que la problématique de la sécurité des données, en particulier informatiques, est une problématique dont les contours sont encore parfois mal appréhendés compte tenu des développements technologiques sans cesse améliorés et de l'utilisation professionnelle de plus ou plus importante de divers moyens fonctionnant en tout ou en partie en *cloud computing*[49]. Si accéder à ses données en tout temps et en tout lieu est devenu la norme, cela induit néanmoins une perte de maîtrise dont il y a lieu de connaître les contours très précisément pour en limiter les risques[50]. A cet égard, le Message rappelle que lorsque des données sont stockées en « nuage », il s'agit en principe de sous-traitance qui doit satisfaire aux conditions y afférentes. Si les données sont dans ce contexte stockées à l'étranger, les articles 13 et 14 P-LPD (actuellement 6 LPD) sont applicables[51].

A ce jour, l'article 11 LPD et l'Ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données[52] incitent à l'autoréglementation, en disposant que les fournisseurs de logiciels et de traitement de données ou les personnes privées qui traitent des données personnelles peuvent soumettre leurs systèmes, procédures et organisation à une évaluation effectuée par des organismes de certification agréés et indépendants.

29. **Le P-LPD** traite de la sécurité des données et des questions de sous-traitance aux articles 7 et 8 P-LPD.

L'article. 7 P-LPD correspond dans les grandes lignes à l'article 7 LPD. Les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. La compétence d'édicter les mesures organisationnelles minimales est ici également déléguée au Conseil fédéral.

La sous-traitance requiert une base légale ou l'existence d'un contrat en bonne et due forme (art. 8 al. 1 P-LPD). Pour l'essentiel, les principes précités applicables de *lege lata* sont repris. Le responsable du traitement doit s'assurer de manière active que le sous-traitant respecte la loi dans la même mesure que lui. Cela concerne principalement le respect des principes généraux de protection des données. Les règles relatives à la sécurité ainsi que les règles sur la communication transfrontière[53]. Le sous-traitant ne pourra lui-même déléguer le traitement à un tiers sans l'accord préalable du responsable du traitement (art. 8 al. 3 LPD). Il pourra par ailleurs faire valoir les mêmes motifs justificatifs que le responsable du traitement (art. 8 al. 4 P-LPD).

L'article 12 P-LPD reprend pour le reste la teneur de l'article 11 LPD.

Disposition inconnue jusqu'alors, l'article 22 P-LPD instaure par ailleurs une obligation d'annonce d'une violation de la sécurité des données personnelles :

- du sous-traitant au responsable du traitement, pour *« tout cas de violation de la sécurité des données »* (art. 22 al. 3 P-LPD) ;
- du responsable du traitement au préposé, lorsque la violation en question *« entraine vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée »* (art. 22 al. 1 P-LPD) ;

[48] CHAPPUIS / ALBERINI, p. 337 et ss, p. 341.
[49] *Cf. Supra*.
[50] *Cf. Supra*, ainsi également que METILLE Sylvain, Confier ses données, *op. cit.*, p. 63 ; FANTI Sébastien, Cloud computing,, *op.cit.*, p. 74 et ss ; CHAPPUIS / ALBERINI, *op. cit.*, p. 337 et ss .
[51] FF 2017 p. 6652.
[52] RS 235.13.
[53] FF 2017 p. 6651.

- du responsable du traitement à la personne concernée, *« lorsque cela est nécessaire à sa protection ou que le préposé l'exige »* (art. 22 al. 4 LPD).

La notion de *« violation de la sécurité »* est désormais définie à l'article 4 let. g P-LPD. Est visée par là toute violation de la sécurité, qu'elle soit ou non intentionnelle ou illicite, entrainant la perte, la modification ou la divulgation non autorisée de ces données.

En cas de devoir légal de garder le secret, l'article 22 al. 5 let. a P-LPD prévoit la possibilité de restreindre, différer ou renoncer à l'information de la personne concernée. En l'état du texte légal, il n'existe toutefois pas de dérogation à l'obligation d'annonce au préposé. Il en découle à notre sens une obligation pour l'avocat d'informer le préposé (ce tout en veillant au strict respect du secret professionnel dont l'avocat n'est nullement libéré dans ce contexte), ainsi que le client concerné par la violation de la sécurité des données, puisque le secret professionnel ne peut en toute hypothèse pas être opposé à ce dernier. Le cas où une telle communication apparaîtrait disproportionnée au vu des circonstances est par ailleurs réservé à l'article. 22 al. 5 let. b P-LPD.

L'alinéa 6 de l'article 22 P-LPD prévoit par ailleurs que l'annonce effectuée au sens de cette disposition ne peut être utilisée – sans le consentement de la personne soumise à l'obligation d'annonce – dans le cadre d'une procédure pénale contre lui (respect du droit à la non-incrimination).

Les dispositions pénales incluent désormais une norme additionnelle qui réprime les violations intentionnelles du devoir de diligence sous l'angle des articles 7, 8, 13 et 14 P-LPD[54]. En revanche, le non-respect du devoir d'annonce de l'article 22 P-LPD n'est pas pénalement réprimé en l'état du projet.

30. Etonnamment, le **RGPD** ne prévoit que peu de dispositions en matière de sécurité des données et laisse une large part à l'appréciation des mesures à prendre au cas par cas *« compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité varie, pour les droits et libertés des personnes physiques »* (art. 32 RGPD).

En revanche, le RGPD prévoit lui-également un devoir d'annonce en cas de violations de données à caractère personnel, ce par quoi il faut entendre toute violation de la sécurité entrainant – de manière accidentelle ou illicite – la destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel (art. 4 ch. 12 RGPD). Ce devoir doit être accompli dans les 72 heures auprès de l'autorité de contrôle (art. 33 RGPD) et *« dans les meilleurs délais »* à la personne concernée lorsque la violation *«est susceptible d'engendrer un risque élevé »* pour ses *« droits et libertés »* (art. 34 RGPD). Les articles 33 et 34 RGPD ne prévoient pour le reste aucune modalité particulière ni exemption en présence de données couvertes par le secret professionnel.

Comme le souligne la doctrine[55], le respect de ces obligations suppose une préparation préalable au sein de l'entreprise (désignation d'un responsable interne et mise sur pied d'une procédure d'urgence).

J. Du traitement illicite de données par des personnes privées et des droits qui en découlent pour la personne concernée

31. La **LPD** concrétise les principes généraux du droit de la personnalité et les systèmes mis en place sont par conséquent calqués sur les articles 28 ss CC.

L'article 12 LPD énonce le principe général de l'interdiction de l'atteinte illicite à la personnalité des personnes concernées et l'article 13 LPD, les motifs justificatifs rendant une telle atteinte licite, à savoir le consentement de la victime, un intérêt privé ou public prépondérant ou la loi. Les moyens de droit sont prévus à l'article 15 LPD lequel renvoie aux articles 28 ss CCS,

[54] *Cf. Infra*.
[55] METILLE Sylvain, Annoncer les failles de sécurité n'est plus une option, *in* EF 11/17 p. 863.

auxquels s'ajoutent les moyens prévus aux articles 5 al. 2 LPD (Droit de rectification) et 8 LPD (droit d'accès).

32. Sous l'angle du nouveau droit, le **P-LPD** reprend dans une large mesure le droit actuel, tout en y apportant quelques adaptations rédactionnelles destinées à le rendre plus clair. C'est ainsi les articles 26 et 27 P-LPD qui traitent désormais des problématiques visées à l'heure actuelle aux articles 12 et 13 LPD.

33. Le contenu du **RGPD** correspond dans les grandes lignes à celui du droit suisse (cf. notamment l'article 82 RGPD *« Droit à réparation et responsabilité »*).

K. De l'obligation (nouvelle) de tenir un registre de traitement

34. L'article 11 **P-LPD**[56] - dont la teneur est nouvelle - prévoit l'obligation pour le responsable du traitement et les sous-traitants de tenir un registre des activités de traitement. La liste des informations qui devront figurer dans ce registre est énoncée à l'article 11 al. 2 P-LPD.

    Cette obligation s'applique à tous les responsables de traitement et, partant, également aux avocats.

    A teneur de l'article 11 al. 5 P-LPD, le Conseil fédéral sera libre de prévoir des exemptions pour les entreprises de moins de 50 collaborateurs et dont les traitements présentent un risque limité d'atteinte à la personnalité des personnes concernées. Ces conditions étant cumulatives[57], il apparaît douteux que les études d'avocat puissent prétendre bénéficier d'exemptions en la matière.

35. A noter que de son côté, l'article 30 **RGPD** prévoit lui aussi une obligation de tenir un tel registre à disposition cas échéant des autorités de contrôle des Etats européens.

    Si une dispense est possible pour des entreprises de moins de 250 collaborateurs, les autres conditions – également cumulatives et semblables à celles prévues à l'article 11 al. 5 P-LPD – conduisent ici aussi à douter qu'une étude d'avocats puisse bénéficier d'une exemption.

L. Des dispositions pénales

36. Les articles 34 et 35 LPD répriment pénalement la violation intentionnelle de certains devoirs du maître de fichier privé.

    En vertu de l'article 34 LPD, le maître de fichier privé qui viole ses obligations de renseigner, de déclarer et de collaborer est puni d'une amende pouvant s'élever jusqu'à CHF 10'000.-.

    La violation du secret professionnel par l'avocat est sanctionnée tant par l'article 321 CP (délit) que par l'article 35 LPD (contravention). Ces deux normes se trouvent toutefois en concours imparfait, l'article 35 LPD étant subsidiaire à l'article 321 CP.

    Actuellement, seule la personne physique auteur de l'infraction peut être poursuivie (art. 29 CP). La punissabilité de l'entreprise, lorsque l'infraction incombe à une personne morale, est exclue, l'article 102 al. 1 CP ne visant que les crimes et délits.

37. Sous **l'angle du nouveau droit**, les dispositions pénales sont régies par les articles 54 à 60 P-LPD. De manière générale, le seuil maximum des amendes est augmenté à CHF 250'000. Seules les infractions intentionnelles sont poursuivies.

    Le P-LPD contient **une nouvelle norme pénale** (article 55 P-LPD) sanctionnant les violations des devoirs de diligence en cas de communication de données à l'étranger en violation de la loi, de « *outsourcing* » dans le traitement des données sans que les conditions prévues par la loi ne soient remplies ou de non-respect des exigences minimales fixées par le Conseil fédéral en matière de sécurité des données.

[56] Lequel correspond sur ce point à l'article 30 RGPD.
[57] FF 2017 p. 6656.

Le concours imparfait entre la teneur des articles 56 P-LPD et 321 CP subsiste[58].

L'article 45 al. 3 P-LPD permettant au préposé de prononcer une décision ordonnant le respect des obligations inscrites dans cette loi, une contravention pour insoumission à cette décision du préposé est instaurée (article 57 P-LPD). Est également passible d'une amende l'insoumission à une décision d'une autorité de recours.

En outre, en cas d'infraction commise au sein d'une entreprise, l'article 58 al. 1 p-LPD renvoie désormais aux articles 6 et 7 DPA. Ainsi, les dirigeants de l'entreprise pourront être tenus responsables en cas de non-respect des obligations de la LPD, conformément à l'article 6 al. 2 DPA. De plus, les autorités de poursuite pénale peuvent, à certaines conditions, renoncer à rechercher les personnes punissables selon l'article 6 DPA et condamner directement l'entreprise au paiement de l'amende, conformément à l'article 7 DPA (article 58 al. 2 P-LPD).

Enfin, le délai de prescription de l'action pénale est prolongé à cinq ans (article 60 P-LPD).

En ce qui concerne le **RGPD**, il est renvoyé à la lecture de son article 83, lequel requiert des autorités de contrôle qu'elles prononcent (elles-mêmes) des amendes *« effectives, proportionnées et dissuasives »* pour des montants pouvant aller, en fonction des violations commises, jusqu'à 4% du chiffre d'affaire annuel (mondial) de l'exercice précédent ou 20 millions d'euros (soit le montant le plus élevé des deux).

M. Conclusion

38. La récente entrée en force du RGPD ainsi que son applicabilité potentielle aux avocats suisses et en particulier genevois suppose la plus grande attention et une information aux acteurs concernés qui, pour la plus grande part, ignorent aujourd'hui encore cette problématique qui n'a en définitive été anticipée que par peu de monde en Suisse. La récente décision du Conseil national de reporter les discussions relatives au P-LPD n'est par ailleurs pas de nature à aider à une prise de conscience globale et rapide. Elle a pour effet – très regrettable - de laisser aux acteurs privés la tâche de s'adapter seuls à l'entrée en force de la réglementation européenne.

39. Manifestement, le législateur suisse ou genevois n'a pas anticipé les éventuelles conséquences de l'entrée en force du RGPD et il n'est pas certain que le droit suisse actuel soit suffisamment précis pour protéger le secret professionnel des avocats suisses face à une nouvelle réglementation européenne complète, exigeante et relativement formaliste, dont les effets extra-territoriaux - indéniables - sont encore difficiles à percevoir complètement. La situation est d'autant plus délicate que la protection du secret professionnel, telle que reconnue en droit suisse, peut s'avérer plus complexe à assurer dans le cadre de l'application d'une réglementation qui ne fait pas partie de l'acquis de Schengen. En d'autres termes, les références contenues dans le RGPD au droit des Etats membres, lequel peut sur certains sujets spécifiques en atténuer la portée, ne s'appliquent pas forcément aux avocats étrangers pour lesquels le RGPD est néanmoins susceptible d'application. Par ailleurs, même protégé par le droit national de son client, l'avocat suisse est susceptible d'être traité à l'aune de normes différentes en fonction du domicile (français, belge etc.) de son client… La problématique est donc complexe et l'insécurité juridique relativement importante en l'état.

* * *

[58] FF 2017 p. 6717.