GESTION DES ACCÈS INTERNES AUX DOSSIERS DES CLIENTS ET PROTECTION DES DONNÉES

PIERRE BYDZOVSKY
LL. M. (Turin), CAS pour la magistrature pénale, avocat à Genève

Mots-clés: protection des données, Privacy by Design, contrôle des accès aux dossiers des clients, durée de conservation des dossiers

Dans le cadre de son activité, l'avocat traite de nombreuses données personnelles dont celles de ses clients. Qui, au sein d'une étude d'avocats, doit avoir accès à ces données parfois sensibles, toujours confidentielles? Et pour combien de temps? La présente contribution cherche à répondre à ces questions sur la base du droit suisse actuel, avec des références au droit réglementaire européen et au projet de révision de la loi fédérale sur la protection des données (P-LPD[1]).[2]

I. Introduction

Les fuites de données *(data leaks)* qui ont occupé les tribunaux suisses ces dernières années ont souvent eu pour origine un collaborateur au sein de l'entreprise.

Il en est allé ainsi de la fuite massive de données de clients d'une grande banque suisse en 2010, vendues ensuite au *Land* de Rhénanie-du-Nord–Westphalie en 2010[3]. Cette fuite eut pour conséquences l'ouverture de procédures pénales en Allemagne pour évasion fiscale contre les clients de la banque, contre celle-ci et contre certains de ses employés. L'on pense également à cet autre employé de banque intérimaire, qui transféra 2700 données de clients sur sa messagerie électronique privée avant de les proposer à la vente aux autorités allemandes[4]. L'on pense inévitablement aussi à l'*affaire Falciani* et à la fuite des 120 000 données de clients anciens et actuels, proposées à diverses autorités étrangères en 2008[5].

L'on se réfère enfin – actualité cinématographique oblige[6] – aux *Panama Papers,* soit la fuite, depuis une étude d'avocats, de 11,5 millions de documents confidentiels portant sur la période de 1970 à 2016 et plus de 214 000 sociétés *offshore*[7]. Cette étude d'avocats avait d'ailleurs suspecté un employé de sa filiale genevoise d'avoir participé à cette fuite de données. La procédure pénale fut toutefois classée fin 2017.

Ces fuites engendrent d'importants dégâts de réputation. Elles enseignent que le risque peut provenir de l'intérieur ou de l'extérieur de l'étude mais qu'*elles ont toujours une composante interne,* à tout le moins sous la forme d'une défaillance de sécurité, organisationnelle ou technique.

Ces précédents doivent amener les avocats suisses à s'interroger sur les accès aux dossiers des clients conférés au sein de leurs études: tous les avocats et employés doivent-ils nécessairement avoir accès à l'intégralité de la base de données des clients? Conviendrait-il de limiter cet accès ainsi que la durée de conservation des dossiers?

II. Qui peut et doit avoir accès aux dossiers des clients au sein de l'étude?

1. Absence de règles spécifiques à la profession d'avocat

La gestion des accès internes *(Berechtigungsmanagement)* aux dossiers des clients d'une étude d'avocats est l'une des mesures de sécurité préventives visant à limiter les risques de violation d'atteinte à la personnalité[8].

1 Projet de loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15. 9. 2017, *in:* FF 2017 p. 6803 ss.
2 L'auteur remercie CINDY LERIN, MLaw et doctorante à l'université de Fribourg, pour sa relecture attentive du présent texte.
3 Tribunal pénal fédéral (TPF), jugement SK.2011.21 du 15. 12. 2011.
4 TPF, jugement SK.2013.26 du 22. 8. 2013.
5 TPF, jugement SK.214.46 du 27. 11. 2015.
6 *The Laundromat* de Steven Soderbergh, diffusé le 18. 10. 2019.
7 Pour plus de détails: www.icij.org/investigations/panama-papers (dernière consultation le 11. 11. 2019).
8 DOMENIG B./MITSCHERLICH C., Datenschutzrecht für Schweizer Unternehmen, Berne 2019, n. 443–445, p. 123.

Ces mesures de sécurité font l'objet, en droit suisse, de règles spécifiques pour certains types d'activités. Ainsi en va-t-il du domaine bancaire, où la FINMA a notamment émis une circulaire[9] imposant à ses assujettis la mise en œuvre d'une stratégie et d'un *monitoring* des risques, dont la fuite de données. La FINMA avait également émis, dès 2013, des recommandations précisant que *«l'organisation du secteur informatique d'une banque est l'un des facteurs les plus importants pour que l'autorisation […] garantisse le respect d'une activité irréprochable […]. La structure organisationnelle du système informatique doit être clairement définie, mise en œuvre, documentée et contrôlée, notamment en ce qui concerne l'accès aux systèmes informatiques»*[10]. Une autre circulaire de la FINMA[11] définit le concept de sécurité des données pour les banques et les principes de bonne pratique dans la gestion des données électroniques des clients. Le premier de ces principes est la nécessité, pour le conseil d'administration, de mettre en œuvre et de piloter une bonne gouvernance, qui doit intégrer un cadre formel et complet assurant la confidentialité des données, qui dépend de la taille et de la complexité de la banque[12]. Des règles semblables sont applicables aux assureurs[13].

Les autorités cantonales de surveillance des avocats n'émettent pas de telles circulaires. Sans aller aussi loin que les banques et les assureurs, qui disposent la plupart du temps de ressources supérieures à celles des études d'avocat, la sécurité des données des clients se pose tout autant pour les études d'avocats.

L'avocat est pour sa part soumis à l'obligation de diligence dans l'exécution de son mandat (art. 398 al. 2 CO). Cette obligation figure également à l'art. 12 let. a LLCA sous l'angle des règles professionnelles et, s'agissant du secret professionnel, à l'art. 13 LLCA, lequel impose à l'avocat de veiller à la préservation du secret, y compris de la part de ses employés et de ses auxiliaires (art. 13 al. 2 LLCA). L'art. 2.3 CCBE[14] consacre enfin le secret professionnel et l'importance de la confidentialité pour les avocats européens.

De ces règles découle l'obligation de l'avocat de protéger les données de ses clients selon les règles de l'art, ou selon l'état actuel de la technique[15], ce qui implique la mise en œuvre de mesures techniques et organisationnelles de protection des données des clients[16].

2. Le droit de la protection des données

A) Assujettissement des études d'avocats à la LPD et au RGPD

Le droit de la protection des données (suisse et européen) réglemente les activités de collecte, de traitement et d'utilisation des données. Il donne à l'individu ainsi qu'aux autorités de surveillance de l'État les moyens de contrôler ces activités, de s'assurer de droits complets d'accès, de rectification, d'annulation et d'action judiciaire. Ces normes, qui ont pour but de protéger la vie privée, complètent les devoirs professionnels des avocats, en particulier l'obligation de confidentialité et de secret professionnel, dont la finalité est d'assurer et de préserver le rapport de confiance entre l'avocat et son client[17].

Une partie minoritaire de la doctrine allemande soutient que les dispositions sur la protection des données sont inapplicables aux données couvertes par le secret professionnel de l'avocat. Cet avis est rejeté par la doctrine dominante qui considère qu'en cas de conflit entre ces normes, le secret professionnel prévaut sur les dispositions du droit de la protection des données.[18]

Les études d'avocats sont ainsi soumises au droit suisse de la protection des données en tant que personne privée au sens de l'art. 2 LPD, quelle que soit leur forme juridique[19]. Les avocats suisses sont également soumis au RGPD[20] s'ils assument des mandats pour des personnes physiques *«qui se trouvent»* dans l'Union européenne[21]. Enfin, la révision totale de la LPD, qui ambitionne d'adapter le droit suisse aux standards européens, avance, bien que par à-coups[22].

La fonction de responsable de traitement des données revêtue par l'avocat engendre d'importantes conséquences déjà discutées dans de précédentes contribu-

9 FINMA, circulaire 2017/1 du 22. 9. 2016, *Corporate governance, risk management and internal controls at banks.*
10 FINMA, bulletin 4/2013 p. 68 ss.
11 FINMA, circulaire 2008/21, *Operational Risks;* voir son annexe 3.
12 MEIER K., Bankaufsichtsrechtliche Relevanz des Datenschutzgesetzes, *in:* Emmenegger Susan, Banken und Datenschutz, Bâle 2019, p. 1 ss, p. 6 s. et p. 13.
13 FINMA, circulaire 2017/2 du 7. 12. 2016, *Corporate governance – insurers.*
14 Code de déontologie des avocats européens.
15 CHAPPUIS B./ALBERINI A., Secret professionnel de l'avocat et solutions *cloud, in:* Revue de l'avocat 2017 p. 337 ss, p. 340.
16 DORTHE A., Etudes d'avocats: se mettre en conformité avec la LPD et le RGPD, *in:* plaidoyer 4/19, p. 12 ss, p. 15; CHAPPUIS B., La profession d'avocat, tome II, 2e éd., Genève 2017, p. 30.; voir ég. JEANNERET V., Le *«Risk Management»* dans une étude d'avocats, *in:* Défis de l'avocat au XXIe siècle: Mélanges en l'honneur du Bâtonnier Dominique Burger, Genève 2008, p. 397 ss, p. 401.
17 ATF 117 Ia 341, consid. 6.
18 KAZEMI R./LENHARD T., Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei, 3e éd., Bonn 2017, n. 13 à 15 p. 7 s.
19 Préposé fédéral à la protection des données, Droits de la personne concernée en matière de traitement des données personnelles, Berne 2014, p. 5 (www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/guides/droits-de-la-personne-concernee-en-matiere-de-traitement-des-don.html; dernière consultation le 10. 11. 2019); DORTHE, p. 12.
20 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27. 4. 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données; RGPD).
21 Art. 3 ch. 2 RGPD; une étude d'avocats suisse peut également être soumise au RGPD à d'autres conditions, notamment lors de ciblages de clients dans l'Union européenne, p. ex. par le biais d'un site internet. Sur ces questions, voir PFAFFINGER M., DSGVO: Extraterritoriale Wirkung und konkrete Pflichten für die Banken, *in:* Emmenegger Susan, op. cit., p. 17 ss, p. 25 ss; DOMENIG/MITSCHERLICH, p. 3–5; FREI N., Die Datenschutz-Grundverordnung und die Schweiz, *in:* Epiney/Sangsue, Datenschutz und Gesundheitsrecht, Zurich/Bâle/Genève 2019, p. 79 ss, p. 85 ss; AMIGUET A./FISCHER P., Changement de paradigme en matière de protection des données, *in:* Revue de l'avocat 1/2018, p. 28 ss, p. 30.
22 Le 25. 9. 2019, le Conseil national a adopté le projet de loi qui doit désormais être examiné par le Conseil des États.

tions[23]: à côté du devoir d'information du client sur le traitement de ses données, de la nécessité de s'assurer d'un consentement préalable des personnes concernées, de l'établissement d'un registre de traitement, de l'adaptation recommandée du modèle de lettre d'engagement, l'élaboration de *règles internes clarifiant l'accès aux dossiers des clients* est sans aucun doute une règle de bonne pratique à mettre en œuvre pour assurer un protection efficace des données à titre préventif. La doctrine allemande parle de *Datensicherheitsmanagement*[24]. Elle insiste sur la nécessité de documenter les concepts et les processus de sécurité[25], discutés ci-après.

B) Mesures techniques et organisationnelles pour éviter des accès inappropriés

La LPD exige de l'avocat qu'il protège les données personnelles contre tout traitement non autorisé, dont le vol interne ou externe de données, par des *«mesures techniques et organisationnelles adéquates»* (art. 7 al. 1 LDP). Cette obligation générale est précisée aux art. 7 ss OLPD[26], notamment par l'obligation de protéger les données *«de manière appropriée»* contre le vol ou une utilisation illicite (art. 7 al. 1 let. d OLPD). En présence d'un «traitement automatisé» de données personnelles, soit tout traitement effectué par un procédé automatisé (par ex. un logiciel informatique)[27], le maître du fichier doit notamment mettre en place un «contrôle d'accès» assurant que les personnes autorisées ont accès uniquement aux données personnelles *dont elles ont besoin pour accomplir leurs tâches* (art. 8 al. 1 let. g OLPD). Ce contrôle doit également permettre l'identification *a posteriori* des personnes introduisant des données personnelles dans le système automatisé, les données introduites et le moment de leur introduction (let. h). Ces mesures doivent en particulier tenir compte du but, de la nature et de l'étendue du traitement des données, de l'évaluation des risques potentiels pour les personnes concernées et du développement technique (art. 8 al. 2 OLPD).

Les processus internes de traitement de données personnelles, qui retranscrivent la bonne pratique de l'étude d'avocats par rapport à l'accès aux données, doivent être pensés conformément au *principe de la proportionnalité* (art. 4 al. 2 LPD). Ce principe exige que le traitement des données soit raisonnable pour la personne concernée tant au regard de sa finalité que *par les moyens (ou la manière) dont le traitement est effectué* (voir l'art. 4 al. 3 LPD), sans quoi la personne concernée peut se prévaloir d'une atteinte illicite à sa personnalité[28].

L'appréciation de la proportionnalité dans la méthode de traitement des données du client doit en principe se faire au cas par cas, c'est-à-dire en tenant compte des circonstances objectivement pertinentes pour chaque client. Dans la pratique, en présence d'un grand nombre de données de clients, il est admis et même recommandé d'aligner le traitement des données de manière standardisée[29], de sorte à permettre aux différents collaborateurs d'une étude d'avocats de mettre en œuvre ces principes de manière simple et efficace.

Si une étude d'avocats regroupe toutes les données de ses clients dans un seul fichier de données automatisé, et si ce fichier est utilisé en même temps pour diverses tâches (par exemple le traitement des données relatives à un mandat de conseil, la facturation et la correspondance, et éventuellement pour d'autres buts), il conviendrait en règle générale, en application du principe de la proportionnalité, que les collaborateurs *n'aient accès qu'aux données dont ils ont besoin pour effectuer leur travail.* ROSENTHAL/JÖHRI donnent l'exemple d'une société active dans la vente de marchandises, où les vendeurs ne devraient en principe pas avoir d'accès au mode de paiement du client, donnée qui ne les concerne pas, tandis que les comptables ne devraient pas avoir accès aux détails des achats effectués[30].

Le Préposé fédéral à la protection des données recommande pour sa part de *restreindre l'accès aux seules données utiles à chaque collaborateur,* de sorte à limiter les risques d'une mauvaise utilisation des données et à prévenir les abus. Il recommande également de définir *des règles d'accès et un mécanisme d'autorisation* par rapport aux fonctions des collaborateurs. Le système d'information devrait être organisé de telle manière à ce que des accès différenciés soient accordés aux utilisateurs et que ceux-ci n'aient accès qu'aux données qu'ils doivent effectivement traiter[31].

Ces obligations sont maintenues et précisées dans le P-LPD, le devoir d'assurer la sécurité des données étant une exigence de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel signée par le Conseil fédéral le 30.10.2019 (art. 7) et du RGPD (art. 32). L'art. 7 P-LPD vise à imposer aux responsables de traitements, selon l'approche fondée sur les risques, des mesures organisationnelles et techniques appropriées, et une sécurité adéquate des données personnelles des clients par rapport au risque encouru[32].

---

23 AMIGUET/FISCHER, p. 32.
24 LAUE P./KREMER S., Das neue Datenschutzrecht in der betrieblichen Praxis, Cologne 2018, n. 31 p. 261.
25 LAUE/KREMER, n. 34 p. 262.
26 Ordonnance relative à la loi fédérale sur la protection des données du 14.6.1993 (OLPD; RS 235.11).
27 Message du Conseil fédéral du 23.11.1988 concernant la loi fédérale sur la protection des données, FF 1988 II 421 ss, p. 425, qui évoque déjà les «nouvelles technologies».
28 ROSENTHAL D./JÖHRI Y., Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, 2008, n. 24 p. 85.
29 ROSENTHAL/JÖHRI, n. 23 p. 85.
30 LES MÊMES, n. 25 p. 85: *«[…] so verlangt es der Verhältnismässigkeitsgrundsatz, dass den Personen in den betreffenden Bereichen immer nur Zugang zu jenen Daten gewährt wird, die sie für ihre Aufgabe benötigen.»*
31 Préposé fédéral à la protection des données, Guide relatif aux mesures techniques et organisationnelles de la protection des données, 2015, p. 11.
32 Message du Conseil fédéral du 15.9.2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, *in:* FF 2017 6565 ss, p. 6642.

Au niveau européen, l'art. 25 RGPD impose au responsable du traitement la mise en œuvre des mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel soient nécessaires au regard de chaque finalité spécifique du traitement traitées, tant au niveau de leur quantité, de leur étendue, de leur durée de conservation que de leur *accessibilité.*

L'on constate en pratique, notamment dans les études d'avocats de petite à moyenne taille, que de nombreux collaborateurs ont généralement accès à un grand nombre de données de clients. Il est par conséquent recommandé de documenter et de mettre en place, avec l'appui des informaticiens de l'étude, des règles organisationnelles et techniques[33] sur l'accès aux dossiers des clients déterminant:

– Les personnes ayant accès au dossier du client; l'étude doit être en mesure de motiver les raisons pour lesquelles ses collaborateurs ont accès à certaines catégories de données personnelles.
  Les *avocats appelés à travailler effectivement sur le dossier* ainsi que *leurs assistant(e)s* et leurs remplaçant(e)s doivent nécessairement pouvoir accéder aux données d'un mandat spécifique puisque ces intervenants doivent exécuter le mandat en faveur du client.
  Il en va de même selon nous des personnes qui, au sein de l'étude d'avocats, assument des tâches de gestion et de *risk management.* Cet accès doit leur permettre un contrôle de qualité de l'activité réalisée et éviter les *malpractices*[34]. Ces finalités justifiant l'accès aux données sont dans l'intérêt du client.
  Les *membres du service de comptabilité* de l'étude doivent avoir accès aux données relatives à la facturation (*time-sheet,* notes d'honoraires et coordonnées du client pour l'envoi des notes d'honoraires). Il peut également se justifier que d'autres données leur soient accessibles, par exemple pour déterminer un assujettissement des honoraires à la TVA.
  Les *informaticiens* (internes ou externes) ne devraient pas avoir accès, de manière unilatérale, à l'intégralité des données des clients de l'étude, en tout temps. On l'a vu, il s'agit d'une catégorie de collaborateurs ou d'auxiliaires à risque, de par leur fonction et leur connaissance du système informatique d'une entreprise. À titre de mesures d'organisation, le contrat de services informatiques entre l'étude et une société informatique externe devrait prévoir que celle-ci n'accédera qu'aux données indispensables pour décrire et résoudre les incidents informatiques rencontrés par l'étude et/ou ses collaborateurs, ainsi que l'engagement de la société informatique à ne traiter les données qui lui ont été communiquées, ou auxquelles elle a accès, que pour les seules fins nécessaires à l'exécution du contrat. Le contrat pourra également prévoir un mécanisme de preuve et de contrôle permettant à l'étude d'avocat de s'assurer que toutes les exigences du secret professionnel, de la protection des données et de la sécurité des données sont bien appliquées conformément au contrat[35].
– Les personnes définissant cet accès; il est souhaitable de prévoir qui détermine l'accès au dossier d'un client (et le modifie). Il devrait selon nous s'agir de l'associé responsable du dossier, lequel est généralement le plus à même de choisir les personnes habilitées à accéder aux données. On pourrait également songer à prévoir une personne de substitution en cas d'absence du responsable, par exemple les associés en charge du *risk management* de l'étude.

La plupart des logiciels de gestion de documents adaptés aux études d'avocats, comme par exemple *Smartlex*[36], permettent facilement de limiter l'accès à certaines personnes ou catégories de collaborateurs d'une étude, sans coût supplémentaire pour l'étude.

Pour s'assurer d'une mise en œuvre efficace des directives internes, des cours de sensibilisation interne à l'attention des collaborateurs et des assistants peuvent s'avérer utiles, de même que la mise en œuvre de contrôles périodiques sur les restrictions d'accès.[37]

C) Conséquences en termes d'utilisation du know-how de l'étude

Cette limitation d'accès aux dossiers peut engendrer des frustrations chez les collaborateurs d'une étude, notamment pour ceux qui ont l'habitude d'utiliser des documents extraits de la base de données informatisée de l'étude comme modèles pour l'exécution d'autres mandats.

Si l'on comprend l'intérêt pratique des collaborateurs à pouvoir accéder à des dossiers avec lesquels ils n'ont pas d'activité, cette finalité, propre à l'étude, semble toutefois difficilement justifiable à l'égard du client sous l'angle du principe de la finalité du traitement (art. 4 al. 3 LPD), selon lequel les données ne peuvent être traitées que dans le but indiqué lors de leur collecte[38].

Il sera par conséquent utile de prévoir, en parallèle à la mise en place des processus et directives d'accès aux dossiers, des modèles d'actes *anonymisés* à disposition de l'ensemble des collaborateurs, pour permettre l'utilisation du *know-how* de l'étude.

III. Jusqu'à quand une étude doit-elle et peut-elle conserver les dossiers de ses clients?

La LPD de 1992 prévoyait déjà, pour le traitement des données par un organe fédéral, que les vastes stocks de

33 REBER M., Privacy by Design & Privacy by Default, *in:* Emmenegger Susan, op. cit., p. 54 s.; SCHRÖDER G., Datenschutzrecht für die Praxis, 3e éd., Munich 2019, p. 214.
34 JEANNERET, p. 411.
35 DOMENIG/MITSCHERLICH, p. 50–62.
36 Pour une liste comparative des logiciel de gestion de documents pour études d'avocats, voir par exemple: https://uptimelegalworks.com/2019/01/16/best-legal-document-management-software-2019 (dernière consultation le 11. 11. 2019).
37 REBER, p. 55.
38 Sur le principe de finalité, voir METILLE S., Internet et droit: Protection de la personnalité et questions pratiques, Genève 2017, p. 85 s.

données collectées par un traitement automatisé devaient être détruits ou à tout le moins anonymisés dès que les données perdent leur intérêt public, afin d'éviter des atteintes à la personnalité, sauf si la conservation de certaines de ces données est nécessaire à titre de preuve, par mesure de sûreté ou en vue d'une éventuelle demande de révision[39].

Pour les responsables de traitement privé, on l'a vu, la LPD et le RGPD requièrent un traitement *proportionné* des données personnelles des clients d'une étude.

Sous l'angle du RGPD (art 5 al. 1 let. e), ce principe signifie que le responsable du traitement ne doit conserver les données personnelles que *«pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées».* Une période de conservation plus longue n'est autorisée qu'à des fins d'archives d'intérêt public, de recherches scientifiques ou historiques, ou de statistiques. Le préambule du RGPD parle pour sa part de limiter la durée de conservation «au strict minimum». Le législateur européen recommande au responsable du traitement de fixer des délais pour l'effacement des données ou pour un examen périodique[40]. Il est à cet égard important de relever qu'un archivage des données ou des restrictions (même strictes) d'accès aux données personnelles par des mesures organisationnelles ne satisfont pas à l'obligation d'effacement[41].

L'art. 5 al. 4 P-LPD, dans sa version présentée dans le message du Conseil fédéral du 15. 9. 2017, impose lui aussi la destruction des données ou leur anonymisation *dès qu'elles ne sont plus nécessaires au regard des finalités du traitement,* rappelant que cette obligation découle déjà aujourd'hui implicitement du principe général de la proportionnalité mais que *«le Conseil fédéral estime important, compte tenu des évolutions technologiques et des capacités presque illimitées de stockage, de la mentionner expressément»*[42].

Il résulte de ce qui précède que les dossiers des clients d'une étude d'avocats ne devraient pas être conservés indéfiniment, que ce soit sous format papier ou électronique.

Leur conservation doit se limiter à une durée n'excédant pas celle nécessaire au regard des finalités du traitement (art. 4 al. 2 LPD; 5 al. 1 let. e RGPD et 5 al. 4 P-LPD), conformément au principe de limitation de la conservation des données personnelles.

Il est ainsi souhaitable que les études d'avocats prévoient une politique de conservation des données personnelles de leurs clients et le processus de destruction des données physiques (documents) et informatiques, également dans la lettre d'engagement, sous l'angle du devoir d'information (art. 17 al. 2 P-LPD; 13 s. RGPD). La durée de conservation nécessaire des données personnelles peut être déterminée en ayant notamment à l'esprit les bases légales et principes suivants:

- les mandats de contentieux terminés et archivés depuis plus de dix ans devront en règle générale être détruits (art. 60 CO pour les délais maximaux du droit suisse en responsabilité civile et art. 127 CO en matière contractuelle). Par exception, en cas de mort d'homme ou de lésions corporelles résultant d'une faute contractuelle, les dossiers devront être conservés 20 ans[43];
- pour les autres mandats, notamment de conseil, ou les mandats atypiques, une conservation plus longue peut représenter un intérêt, par exemple en matière immobilière (par ex. pour le calcul de l'impôt en cas de plus-value en cas de revente) ou successorale, ou si des prescriptions civiles ou pénales de droit étranger plus longues s'appliquent.

Les dispositions légales suivantes devront notamment également être prises en considération dans l'appréciation de la durée de conservation:

- art. 958f CO: les livres, les pièces comptables, le rapport de gestion et le rapport de révision de la société sont conservés dix ans à compter de la fin de l'exercice;
- art. 46 LTr et art. 73 al. 2 OLT 1: toute documentation pertinente lors d'une enquête sur les infractions au droit du travail sera conservée cinq ans au minimum après l'expiration de sa validité;
- art. 41 al. 2 LPP: les actions en recouvrement de créance se prescrivent par cinq ans quand elles portent sur des cotisations ou des prestations périodiques, par dix ans dans les autres cas. Par conséquent, il est recommandé de conserver les données relatives aux régimes de retraite durant dix ans;
- art. 7 al. 3 LBA: les documents établis en vertu de l'art. 7 al. 1 LBA doivent être conservés dix ans après la cessation de la relation d'affaires ou après la fin de la transaction.

IV. Conséquences en cas de traitement inapproprié des données

En présence d'une faille dans la sécurité des données ou d'un dispositif de sécurité insuffisant, la personne concernée par les données peut invoquer une atteinte à sa personnalité du simple fait que les mesures de sécurité requises n'ont pas été respectées[44]. Le lésé peut faire valoir les actions concernant la protection de la personnalité selon les art. 28, 28*a* et 28/ CC[45], dont l'action en dommages-intérêts et en réparation du tort moral prévue à l'art. 28*a* al. 3 CC[46].

---

39 Art. 21 aLPD; FF 1988 II p. 421 ss, p. 478 s.
40 RGPD, préambule, ch. 39; ég. DOMENIG/MITSCHERLICH, n. 347 p. 103.
41 LAUE/KREMER, n. 47 s., p. 177 s.
42 Message du Conseil fédéral du 15. 9. 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 p. 6565, p. 6645 s.
43 Nouvel art. 128*a* CO, qui entrera en vigueur le 1. 1. 2020.
44 STEINAUER P.-H./FOUNTOULAKIS C., Droit des personnes physiques et de la protection de l'adulte, Fribourg 2014, n. 707.
45 WERRO F., La responsabilité civile, 3e éd., Berne 2017, n. 1506, p. 428.
46 Pour des exemples de dommages indemnisables: cf. LAUE/KREMER, n. 5 p. 370.

À ce risque s'ajoutent les sanctions prévues par le droit de la protection des données. Alors que les sanctions actuelles de la LPD sont peu dissuasives, celles prévues par le P-LPD et le RGPD le sont davantage: le P-LPD prévoit une amende de CHF 250 000.– pour le responsable du traitement qui viole intentionnellement son devoir d'information de la personne concernée (art. 54 P-LPD) ou faillit à son devoir de diligence (art. 55 P-LPD). Si le RGPD s'applique à l'étude d'avocats, celle-ci est également soumise aux décisions des autorités de contrôle de l'UE dont les amendes – certes utilisées en ultime recours – peuvent atteindre 20 millions d'euros (ou 4% du chiffre d'affaires global, le montant le plus élevé étant retenu; art. 77 ss RGPD)[47]; ceci sans compter, le cas échéant, les frais et les éventuels dommages et intérêts suite à un recours en justice et les dégâts, souvent irréparables, en termes de réputation.

Aussi, il est important de relever que le P-LPD renforce et élargit les pouvoirs du Préposé. Dès l'entrée en vigueur de la loi révisée, celui-ci pourra ouvrir d'office ou sur dénonciation une enquête contre une personne privée (art. 43 P-LPD) et pourra prononcer les décisions nécessaires au respect de cette loi. L'insoumission à une décision du Préposé entraîne une amende pouvant elle aussi s'élever à CHF 250 000.–.

47 DOMENIG/MITSCHERLICH, n. 42 p. 13.