Droit de la responsabilité

Journée de la responsabilité civile 2018

Responsabilité civile et nouvelles technologies

Édité par
Christine Chappuis et Bénédict Winiger

Avec la collaboration d'Arnaud Campi et de Dino Vajzovic

UNIVERSITÉ DE GENÈVE
FACULTÉ DE DROIT

Schulthess
ÉDITIONS ROMANDES

Collection Genevoise

Journée de la responsabilité civile 2018

Responsabilité civile et nouvelles technologies

Édité par
Christine Chappuis et Bénédict Winiger

Avec la collaboration d'Arnaud Campi et de Dino Vajzovic

UNIVERSITÉ DE GENÈVE
FACULTÉ DE DROIT

Schulthess
ÉDITIONS ROMANDES
§ 2019

Christine Chappuis / Bénédict Winiger (éds), *Responsabilité civile et nouvelles technologies,*
Collection Genevoise, Genève / Zurich 2019, Schulthess Éditions Romandes

ISBN 978-3-7255-8756-8

www.schulthess.com

Diffusion en France : Lextenso Éditions, 70, rue du Gouverneur Général Éboué, 92131 Issy-les-Moulineaux Cedex
www.lextenso-editions.com

Diffusion en Belgique et au Luxembourg : Patrimoine, 119, avenue Milcamps, 1030 Bruxelles

Information bibliographique de la Deutsche Nationalbibliothek
La Deutsche Nationalbibliothek a répertorié cette publication dans la Deutsche Nationalbibliografie ; les données bibliographiques détaillées peuvent être consultées sur Internet à l'adresse http://dnb.d-nb.de.

Sommaire

Les nouvelles technologies et la responsabilité des avocats

La cybersécurité et l'intelligence artificielle

Jérôme Gurtner, docteur en droit*

Table des matières

* L'auteur tient à remercier Mme Diane Zinsel, journaliste à l'agence de presse suisse Keystone-ATS, ainsi que Mme Elodie Hogue, titulaire du brevet d'avocat, pour leur relecture de la présente contribution. Plusieurs ouvrages utiles à la préparation de la présente contribution ont été financés à l'aide du montant du Prix Walther Hug, qui a récompensé la thèse de doctorat de l'auteur en 2017. L'auteur tient à remercier la Fondation Professeur Walther Hug pour le soutien qu'elle apporte à la recherche juridique suisse.

I. Introduction générale

L'objectif de la présente contribution est d'examiner deux sujets susceptibles d'impliquer la responsabilité des avocats dans le contexte des nouvelles technologies. La première partie sera consacrée à la cybersécurité (II) et la seconde à l'intelligence artificielle (ci-après : l'IA) (III). Nous terminerons par des conclusions (IV).

II. La responsabilité des avocats et la cybersécurité

Après une introduction exposant l'importance et les enjeux de la cybersécurité pour les avocats (A), l'auteur présentera les menaces et les vulnérabilités les plus fréquentes susceptibles de toucher les cabinets d'avocats (B). Il examinera les conséquences d'une atteinte à la cybersécurité et les conditions qui doivent être remplies pour qu'un avocat engage sa responsabilité (C). L'auteur clôturera cette première partie en suggérant aux avocats quelques recommandations pour limiter leur exposition aux cyber-risques (D).

A. Introduction

La cybersécurité peut être définie comme l'ensemble des mesures prises pour protéger un accès ou une utilisation non autorisée de données électroniques.

Les cabinets d'avocats sont des cibles attractives pour plusieurs raisons[1]. Ils recueillent, stockent et utilisent des données très sensibles de leurs clients, tout en utilisant parfois des mesures de protection qui peuvent être inférieures à celles déployées par leurs clients. De plus, les informations en possession des cabinets d'avocats sont plus intéressantes pour les pirates informatiques et moins volumineuses que celles détenues par les clients des avocats.

Les études d'avocats sont des cibles non seulement pour les entreprises privées à la recherche d'informations (fusion/acquisition, accords commerciaux, etc.), mais également pour les entités gouvernementales luttant contre le crime organisé et le terrorisme[2].

Les petites études d'avocats peuvent être exposées à plus de risques, en raison notamment d'un niveau de protection plus faible et de la présence en interne de moins d'experts en informatique[3].

Cependant, les grands cabinets d'avocats ne sont pas épargnés. En 2016, la Division Cyber du FBI a publié un avertissement d'après lequel les pirates informatiques ciblent spécifiquement les cabinets d'avocats internationaux afin d'obtenir des données confidentielles[4]. L'étude d'avocats Mossack Fonseca, située au Panama, a été impliquée dans la plus importante atteinte à la protection des données jamais signalée en termes de volume de données volées[5]. La brèche comprenait 11,5 millions de documents – appelés les « Panama Papers » – qui dataient de 1970 à fin 2015, représentant 2,6 téraoctets de données divulguées[6].

Le ministre de l'intérieur des Pays-Bas a reconnu en décembre 2014 que les services secrets néerlandais avaient espionné le cabinet d'avocats Prakken d'Oliveira pendant plusieurs années, sans autorisation judiciaire, sur

1 ABA Formal Opinion 477R du 11 mai 2017 et les réf. cit.

2 Sur la question de la surveillance étatique, voir « National Security : A Free Licence for Government surveillance ? », organisé par le CCBE lors de la 11ème conférence internationale CPDP 2018, les 24, 25, et 26 janvier 2018 à Bruxelles, disponible sur : https://www.youtube.com/watch?v=ByUtjDJ19L0 (consulté le 22.07.2019). Voir aussi, CCBE, *Recommandations du CCBE sur la protection des droits fondamentaux dans le contexte de la « sécurité nationale »*.

3 WRIGHT, *Cyber Security Toolkit*, p. 3.

4 FRIEDMAN, *FBI Alert*.

5 THOMSON, *Understand Cybersecurity Risks*, Chapitre II, I.

6 THOMSON, *Understand Cybersecurity Risks*, Chapitre II, I.

la base d'un règlement interne confidentiel des services secrets[7]. Le cabinet d'avocats, l'Association néerlandaise des avocats pénalistes et le Conseil des barreaux européens (ci-après : CCBE), ont porté l'affaire devant le tribunal d'arrondissement de La Haye contre l'État néerlandais. En juillet 2015, le tribunal a jugé que la surveillance des avocats par l'agence de renseignements constituait une violation des droits fondamentaux ; il a ordonné à l'État de cesser toute interception des communications entre les clients et les avocats sous le régime actuel dans les six mois à venir[8]. La décision a été confirmée par la Cour d'appel néerlandaise le 27 octobre 2015.

B. Les menaces et les vulnérabilités les plus fréquentes

La plupart des failles de sécurité et des fuites de données sont le fruit d'inadvertance ou de malveillance de la part d'employés[9]. L'analyse de ces violations est éclairante : la plupart auraient pu être évitées[10]. En ce qui concerne le cabinet d'avocats Mossack Fonseca, les experts en sécurité ont estimé que l'étude employait des logiciels désuets avec des vulnérabilités critiques qui étaient largement connues des pirates informatiques[11].

D'après un rapport publié en 2019 par le cabinet d'avocats Baker & Hostetler, spécialisé en protection des données et en cybersécurité, sur un total de plus de 750 affaires traitées en 2018 par le cabinet, les cinq incidents les plus fréquents étaient l'hameçonnage (« phishing ») (37 %), les intrusions dans le réseau (30 %), les divulgations par inadvertance (12 %), le vol ou la perte de supports ou d'enregistrements (10 %), et la mauvaise configuration du système (4 %)[12].

---

7 Le renseignement néerlandais met les avocats de Prakken d'Oliveira sur écoute, disponible sur : https://www.prakkendoliveira.nl/en/news/2014/dutch-intelligence-service-aivd-taps-prakken-d-oliveira-lawyers [https://perma.cc/A9S6-MFG8].

8 CCBE, *Recommandations du CCBE*, p. 31.

9 Dans ce sens : CHAPPUIS/ALBERINI, *Secret professionnel*, p. 342. Voir aussi BONDALLAZ, *Le protection des personnes*, p. 36-37, qui met en évidence la prépondérance du facteur humain dans la liste des erreurs les plus fréquemment commises en matière de sécurité informatique. Selon un rapport publié en 2019, l'employé était responsable dans 55 % des cas (BAKERHOSTETLER, *2019 Data Security Incident*, p. 7).

10 THOMSON, *Understand Cybersecurity Risks*, chapitre II, II. D'après un rapport publié en 2019, 95 % des atteintes en 2018 auraient pu être évitées (INTERNET SOCIETY, *2018 Cyber Incident*, p. 3).

11 THOMSON, *Understand Cybersecurity Risks*, chapitre II, III. A.

12 BAKERHOSTETLER, *2019 Data Security Incident*, p. 2.

C. Les conséquences d'une atteinte à la cybersécurité

1. Les premières répercussions

Au-delà des aspects juridiques qui seront examinés ci-dessous, les conséquences d'une atteinte à la cybersécurité peuvent être désastreuses. On mentionnera la perte de clients actuels et futurs, la perte de réputation (de la personne responsable de l'atteinte et de l'étude d'avocats), la démission d'associés et de membres du personnel (et la difficulté à en recruter de nouveaux), la perte de temps, la perte de revenus, la perte de soutien financier, l'augmentation des coûts de l'assurance responsabilité civile professionnelle et les coûts d'une mise à niveau informatique[13].

Il est difficile de survivre à une atteinte à la cybersécurité. L'étude Mossack Fonseca a annoncé en mars 2018 qu'elle cessait ses activités, évoquant des dommages irréparables causés à sa réputation[14].

2. La responsabilité disciplinaire

L'avocat est soumis au secret professionnel pour toutes les affaires qui lui sont confiées par ses clients dans l'exercice de sa profession ; cette obligation n'est pas limitée dans le temps et est applicable à l'égard des tiers. Le fait d'être délié du secret professionnel n'oblige pas l'avocat à divulguer des faits qui lui ont été confiés (art. 13 al. 1 de la Loi fédérale sur la libre circulation des avocats ; ci-après : LLCA ; RS 935.61). Le secret professionnel est si important qu'il ne peut exister de procès équitable sans celui-ci[15].

Selon la doctrine, l'avocat viole son secret professionnel s'il *communique* oralement, par écrit, par des gestes ou par la remise de documents des faits soumis au secret[16]. Cela signifie-t-il, dans le contexte de la cybersécurité et des données électroniques, que la violation du secret professionnel doit nécessairement impliquer une communication de l'avocat ? En d'autres termes, est-ce que des failles ou des vulnérabilités dans un système informatique, qui permettraient à des tiers d'accéder à des données soumises au secret professionnel, seraient suffisantes pour engager la responsabilité disciplinaire de l'avocat ? Il s'agit d'une question importante qui est tranchée de manière différente par la doctrine.

Walter FELLMANN estime qu'une violation de l'art. 13 LLCA peut être sanctionnée disciplinairement en cas de *simple négligence*, et même *à titre*

---

13 WRIGHT, *Cyber Security Toolkit*, p. 39 à 45.

14 MICHEL, *Panama Papers*.

15 CCBE, *Recommandations du CCBE*, p. 10 à 11 et les réf. cit.

16 BOHNET/MARTENET, *Droit de la profession d'avocat*, N 1843.

préventif en cas de *mise en danger grave*, sans que le secret professionnel ne soit effectivement révélé[17] ; disposition qui doit être distinguée de l'art. 321 du Code pénal (ci-après : CP ; RS 311.0) dont la révélation est un élément constitutif objectif de l'infraction. Sébastien FANTI indique que ne pas crypter ou sécuriser des messages électroniques engagerait automatiquement la responsabilité disciplinaire et civile de l'avocat[18]. Kaspar SCHILLER considère en revanche que la *simple possibilité* ou le *simple risque* de connaissance n'est pas suffisant[19]. Hans NATER et Gaudenz G. ZINDEL estiment qu'il y a une violation du secret professionnel lorsqu'une personne non autorisée a *effectivement pris connaissance* des renseignements confidentiels[20]. Une décision de la Commission des avocats du canton de Soleure du 25 mars 2004 souligne qu'il doit être clair quels renseignements confidentiels ont été divulgués et à qui ces derniers l'ont été ; une *simple suspicion* de violation du secret professionnel n'est *pas suffisante*[21].

A notre avis, un avocat doit pouvoir être sanctionné au sens de l'art. 13 LLCA sans qu'un secret ne soit nécessairement révélé, interprétation qui est corroborée par l'énoncé du texte légal et par le but de la norme. L'art. 13 LLCA ne doit pas être confondu avec la violation du secret contractuel (qui exige un préjudice) ou la violation de l'art. 321 CP (qui exige une révélation). Dans le contexte des nouvelles technologies, il y a un intérêt public important à ce que cette disposition soit comprise dans ce sens. Il suffit de citer l'exemple mentionné par Hans NATER et Gaudenz G. ZINDEL pour s'en convaincre. Ces auteurs expliquent qu'il n'y a pas de violation du secret professionnel lors d'une communication téléphonique avec une fenêtre ouverte dans un bureau situé au rez-de-chaussée[22]. Si l'on transpose cet exemple aux nouvelles technologies, p. ex. à l'utilisation d'un serveur *cloud* qui serait ouvert au public et non sécurisé, plusieurs milliards de personnes seraient devant la fenêtre et n'auraient plus qu'à tendre l'oreille pour écouter la conversation. Est-ce qu'une telle situation n'exige pas que l'avocat soit sanctionné à titre préventif pour sauvegarder l'intérêt public ?

Le Tribunal fédéral n'a pas encore tranché cette question. Il a cependant indiqué dans un arrêt que l'obligation de garantir le secret professionnel appartient au devoir d'exercer la profession d'avocat avec soin et diligence (art. 12 let. a LLCA)[23]. Dans cette affaire, le Tribunal fédéral a considéré que le

17 FELLMANN, *Anwaltsrecht*, N 535 et N 626.

18 FANTI, *Courrier électronique*, p. 493.

19 SCHILLER, *Anwaltsrecht*, N 576. Pour une critique de cet avis : FELLMANN, *Anwaltsrecht*, N 628 et 629.

20 BGFA-NATER/ZINDEL, art. 13, N 198.

21 Décision de la Commission des avocats du canton de Soleure du 25 mars 2004, consid. 2.7, disponible sur : http://www.appl.so.ch/appl/ger/daten/ger2004/05.pdf [https://perma.cc/NX9Z-R5NK].

22 BGFA-NATER/ZINDEL, art. 13, N 198, exemple cité à la note de bas de page 330.

23 TF arrêt 2C_247/2010 du 16 février 2011, consid. 7.1.

fait même de déposer un dossier confidentiel dans un restaurant accessible au public viole le devoir de diligence de l'avocat, d'autant plus que le dossier en question avait été remis à un serveur dont l'avocat ne connaissait pas le nom et qu'il n'avait pas informé le propriétaire du restaurant de ce dépôt. L'avocat n'avait pas non plus veillé à ce que les documents soient conservés en lieu sûr jusqu'à ce qu'ils soient récupérés[24]. Cet arrêt peut à notre sens s'appliquer par analogie aux données électroniques déposées sur un serveur *cloud* non sécurisé et accessible au public. Ainsi, le fait de ne pas prendre des mesures de sécurité adéquates pourrait déjà violer l'art. 12 let. a LLCA[25].

Par ailleurs, le respect du secret professionnel doit être évalué à l'aune des mesures prises par l'avocat. Hans NATER et Gaudenz G. ZINDEL estiment que les avocats doivent s'assurer que le cabinet est organisé comme *un système fermé* dont les informations confidentielles ne s'échappent pas[26]. Une telle exigence n'est pas réaliste dans le contexte de l'informatique. Les experts en cybersécurité estiment en effet que le seul ordinateur complétement sécurisé est un ordinateur que personne ne peut utiliser ; l'idée de fabriquer une boîte noire dans laquelle personne ne peut entrer a donc été abandonnée[27]. Il subsistera toujours une certaine quantité de cyber-exposition, aucun programme de prévention et d'atténuation de la cyber-vulnérabilité n'étant impénétrable[28]. Comme le relèvent Dominik WAGNER et Sonia ZWIRNER, la norme de sécurité requise ne peut jamais être une sécurité absolue[29]. Katia FAVRE estime quant à elle que les mesures de sécurité devraient être proportionnées et ne pas exclure l'utilisation des technologies de l'information[30]. Ces avis rejoignent celui du CCBE qui indique que la question n'est pas de savoir si des failles de sécurité peuvent être évitées, mais plutôt de savoir comment les avocats peuvent démontrer qu'ils ont réfléchi à la question, trouvé des solutions et pris *les mesures préventives nécessaires*[31].

Concernant les obligations de l'avocat en lien avec les nouvelles technologies, le droit suisse est muet. Aux États-Unis, en 2012, l'*American Bar Association* (ci-après : l'ABA) a modifié le commentaire du chiffre 1.1 des *Model Rules of Professional Conduct* (ci-après : *Model Rules*). Ce commentaire a désormais la teneur suivante : pour maintenir les connaissances et les

---

24 TF arrêt 2C_247/2010 du 16 février 2011, consid. 7.4.

25 *Contra* : BARTH, *Utilisation des nouvelles technologies*, p. 6.

26 BGFA-NATER/ZINDEL, art. 13, N 77 ; voir aussi SCHILLER, *Anwaltsrecht*, N 1157 et 1377.

27 War Games : Tracing the History of Cyber Security, in Knowledge@Wharton, The Wharton School, University of Pennsylvania, le 9 juin 2016, disponible sur : http://knowledge.wharton.upenn.edu/article/the-secret-history-of-cyber-war/ [https://perma.cc/6QFD-P2FL].

28 KALINICH/RHYNER, *Cyber Insurance for Law Firms*.

29 WAGNER/ZWIRNER, *Cyber Risk in Anwaltskanzleien*, p. 176.

30 FAVRE, *Sorgfaltspflichten*, p. 159.

31 CCBE, *Renforcement de la sécurité informatique*, p. 26.

compétences requises, un avocat doit se tenir informé de l'évolution du droit et de sa pratique, *y compris les avantages et les risques associés à la technologie*, poursuivre ses études et sa formation et se conformer à toutes les exigences en matière de formation juridique continue auxquelles il est assujetti. Une règle spécifique prévoit en outre qu'un avocat doit faire *des efforts raisonnables* pour empêcher la divulgation par inadvertance ou non autorisée de renseignements relatifs à la représentation d'un client ou l'accès non autorisé à ces renseignements[32]. Le commentaire de cette règle explique que l'accès non autorisé à l'information relative à la représentation d'un client ou la divulgation accidentelle ou non autorisée de cette information ne constitue pas une violation si l'avocat a fait *des efforts raisonnables* pour empêcher l'accès ou la divulgation. Dans un avis de 2006, le « New Jersey Advisory Committee on Professional Ethics » a souligné que ces efforts raisonnables ne signifient pas que l'avocat garantit une sécurité absolue[33].

Les facteurs à prendre en considération pour déterminer le caractère raisonnable des efforts de l'avocat comprennent notamment[34] :

- La sensibilité des informations ;
- La probabilité de divulgation si des mesures de protection supplémentaires ne sont pas prises ;
- Le coût de l'utilisation des mesures de protection supplémentaires ;
- La difficulté de mettre en œuvre les mesures de protection ; et
- La mesure dans laquelle ces dernières nuisent à la capacité de l'avocat de représenter ses clients (p. ex. en rendant un dispositif ou un logiciel important trop difficile à utiliser).

Les avocats devraient analyser, au cas par cas, la façon dont ils communiquent par voie électronique avec leurs clients, en appliquant les critères mentionnés ci-dessus pour déterminer quel effort est raisonnable[35]. Dans ce contexte, il est fondamental que les avocats discutent avec leurs clients pour déterminer quelles mesures doivent être mises en œuvre.

Cette manière de procéder est pertinente dans la mesure où ces critères peuvent s'adapter aux évolutions technologiques. Il est en effet illusoire de s'appuyer uniquement sur des prescriptions techniques et des normes de sécurité qui évoluent régulièrement. Nous suggérons que ces critères s'appliquent en Suisse également.

---

32 ABA Model Rule 1.6 c.

33 ADVISORY COMMITTEE ON PROFESSIONAL ETHICS, *New Jersey Ethics Opinion 701*.

34 ABA Model Rule 1.6, commentaire 18.

35 ABA Formal Opinion 477R, p. 5.

A notre avis, un avocat devrait pouvoir – dans certains cas admis de manière restrictive – échapper à une sanction disciplinaire en prouvant qu'il a pris toutes les mesures préventives nécessaires. Cette solution aurait l'avantage d'atténuer la rigueur de notre interprétation de l'art. 13 LLCA et d'encourager les avocats à ne pas rester inactifs.

Relevons enfin que les conditions générales d'assurance (ci-après : CGA) des assurances responsabilité civile professionnelles ne prennent souvent pas en charge les frais en rapport avec des procédures pénales, policières, disciplinaires ou administratives[36]. Il est en revanche parfois possible de conclure une couverture supplémentaire offrant une protection juridique dans le cadre de ces procédures.

3. La responsabilité pénale

L'art. 321 ch. 1 CP prévoit que les avocats, ainsi que leurs auxiliaires, qui auront révélé un secret à eux confié en vertu de leur profession ou dont ils avaient eu connaissance dans l'exercice de celle-ci, seront, sur plainte, punis d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Déjà sous l'empire du droit disciplinaire cantonal, le Tribunal fédéral avait considéré que la répression disciplinaire de la violation du secret professionnel des avocats, qu'elle intervienne à côté d'une peine prononcée en application de l'art. 321 CP ou sans une telle peine, n'est pas contraire au droit fédéral[37]. L'ouverture d'une procédure pénale n'exclut ainsi pas l'ouverture d'une procédure disciplinaire pour les mêmes faits, les deux procédures étant indépendantes l'une de l'autre[38]. Elles ne visent pas non plus les mêmes buts[39].

La violation du secret professionnel est une infraction intentionnelle, étant précisé que le dol éventuel suffit[40]. L'infraction peut être commise par un comportement actif ou par commission par omission (art. 11 CP)[41]. Il n'y a pas d'intention si la divulgation est involontaire, p. ex. si l'avocat laisse accidentellement des dossiers ouverts en présence d'un tiers[42]. La négligence n'est par conséquent pas punissable. Dans le contexte des données électroniques, l'enjeu sera de déterminer si l'absence de mesures de protection doit être qualifiée de dol éventuel ou de négligence consciente ou inconsciente. A ce sujet, nous ne partageons pas l'avis de Dominik WAGNER et Sonia ZWIRNER qui estiment que l'absence de mesures de protection devrait en général être

---

36 Voir p. ex. l'art. 9.1 des CGA de Zurich Compagnie d'Assurances SA, édition du 1er août 2014.

37 ATF 97 I 831, consid. 2b, JdT 1973 I 200.

38 FELLMANN, *Anwaltsrecht*, N 535.

39 TF arrêt 2P.133/2003 du 28 juillet 2003 ; CHAPPUIS, *La profession d'avocat, Tome I*, p. 161.

40 FELLMANN, *Anwaltsrecht*, N 535 et 564 ; CR CPII-CHAPPUIS, art. 321, N 104 et les réf. cit.

41 CR CPII-CHAPPUIS, art. 321, N 70 ; CORBOZ, *Le secret professionnel de l'avocat*, p. 105.

42 FELLMANN, *Anwaltsrecht*, N 564.

qualifiée de dol éventuel[43]. Chaque situation doit être examinée au cas par cas, sans écarter la négligence[44]. A notre avis, l'avocat qui utilise un ordinateur portable pour répondre à des courriels professionnels pendant une conférence à laquelle il assiste, alors qu'il se rend compte que d'autres participants situés à proximité de lui peuvent lire ses courriels sans effort, pourra difficilement prétendre qu'il ne s'est pas représenté la révélation du secret comme possible et qu'il ne l'a pas acceptée pour le cas où elle se produirait. Le dol éventuel devrait dans ce cas être retenu. Il devrait également l'être lorsque l'avocat, qui a égaré son téléphone portable dans un lieu public, permettant à des tiers d'accéder à ses courriels professionnels, savait qu'il devait configurer son appareil avec un mot de passe et un verrouillage automatique de l'appareil, mais a préféré ignorer cette mesure de sécurité pour des raisons pratiques. En revanche, lorsque la mesure de sécurité qui faisait défaut est moins évidente et que le résultat ne paraissait pas aussi inévitable, on admettra plus facilement la négligence. On peut imaginer une négligence dans l'hypothèse où, p. ex., un avocat aurait omis de mettre à jour un logiciel désuet comportant des vulnérabilités critiques, lesquelles auraient permis à des pirates informatiques d'accéder aux dossiers électroniques de l'Etude. Enfin, contrairement à l'art. 13 LLCA, l'infraction pénale de l'art. 321 CP n'est réalisée que si le secret est révélé par la conduite de l'avocat[45].

4. La responsabilité civile

En sa qualité de mandataire, l'avocat est tenu à la bonne et fidèle exécution du mandat (art. 398 al. 2 CO). La doctrine majoritaire considère que le devoir de discrétion est une concrétisation de l'obligation de fidélité au sens de l'art. 398 al. 2 CO[46]. Le comportement du mandataire doit tendre à éviter que des données ne puissent être révélées à des tiers sans autorisation[47].

Contrairement à la protection du secret sous l'angle du droit pénal et du droit disciplinaire, la protection du secret contractuel protège non seulement les informations soumises au secret professionnel, mais également toutes celles que le client souhaite garder secrètes[48]. L'ATF 135 III 597 consid. 3.3 illustre bien cette différence. Tout mandataire assume, même s'il ne l'a pas

---

43 WAGNER/ZWIRNER, *Cyber Risk in Anwaltskanzleien*, p. 179-180.

44 Concernant les degrés de culpabilité intentionnelle et de négligence, voir KILLIAS/KUHN/DONGOIS, *Précis de droit pénal général*, N 321 à 324.

45 FELLMANN, *Anwaltsrecht*, N 560 ; CR CPII-CHAPPUIS, art. 321, N 104.

46 Dans ce sens : BK-FELLMANN, art. 398 CO, N 40 ss ; CHAPPUIS, *La profession d'avocat, Tome I*, p. 162 ; BOHNET/MARTENET, *Droit de la profession d'avocat*, N 1799 et les réf. cit. ; MÜLLER, *Contrats*, N 1983 à 1985, 1994 à 1997. *Contra* : CR COI-WERRO, art. 398 CO, N 13 et 23, qui estime que le devoir de discrétion découle de l'obligation de diligence du mandataire.

47 CR COI-WERRO, art. 398 CO, N 22.

48 BK-FELLMANN, art. 398, N 53 ; BGFA-NATER/ZINDEL, art. 13, N 22 et 194.

expressément promis, une obligation de garder le silence sur les faits dont la divulgation pourrait être préjudiciable au mandant[49]. Celui-ci est ainsi en droit d'exiger du mandataire qu'il lui rende compte de sa gestion et, simultanément, qu'il garde le silence envers les tiers. Au décès du mandant, ces deux obligations passent aux héritiers. En revanche, au regard de l'art. 321 CP, les héritiers du client ne jouissent d'aucune prérogative particulière ; ils demeurent étrangers à la relation ayant existé entre l'avocat et le client décédé, et ce conseil est tenu, sauf à encourir une sanction pénale s'il subsiste un lésé susceptible de déposer plainte, de leur opposer le secret professionnel. Sous menace de sanctions disciplinaires prévues par l'art. 17 LLCA, l'art. 13 LLCA oblige aussi l'avocat à observer le secret professionnel à l'encontre des tiers, sans limitation dans le temps, c'est-à-dire aussi à l'encontre de l'héritier du client[50].

D'après Benoît CHAPPUIS, toute révélation non autorisée de faits couverts par le secret professionnel est susceptible d'exposer l'avocat à sa responsabilité si elle provoque un dommage en lien de causalité avec elle[51]. Walter FELLMANN explique que si la violation de l'art. 13 LLCA constitue simultanément une violation (intentionnelle) de l'infraction pénale prévue à l'art. 321 CP, elle constitue un acte illicite au sens des art. 41 du Code des obligations (ci-après : CO ; RS 220) et 28 du Code civil (ci-après : CC ; RS 210) ainsi qu'une violation de l'obligation de discrétion et de confidentialité en vertu du droit des contrats[52]. Si cela entraîne un dommage, le client a droit à une indemnisation, conformément aux art. 41 et 398 al. 2 CO[53]. Si la divulgation du secret entraîne une atteinte à la personnalité, le client a également droit au paiement d'une somme d'argent à titre de réparation au sens de l'art. 49 al. 1 CO « pour autant que la gravité de l'atteinte le justifie et que l'auteur ne lui ait pas donné satisfaction autrement »[54]. Il convient également de garder à l'esprit qu'une violation de l'art. 13 LLCA n'entraîne pas automatiquement une responsabilité délictuelle ou contractuelle sous l'angle du droit civil, les conditions d'application de ces deux régimes étant différentes.

La question est de savoir dans quelle mesure l'obligation de diligence prévue par le droit du mandat inclut la garantie de la sécurité des données[55]. Une diligence objective est requise[56], c'est-à-dire la diligence qu'un mandataire

---

49 ATF 135 III 597, consid. 3.3 ; BK-FELLMANN, art. 398 CO, N 42 et 43, 63 et 64.

50 ATF 135 III 597, consid. 3.3.

51 CHAPPUIS, *La profession d'avocat, Tome II*, p. 182 ; BOHNET/MARTENET, *Droit de la profession d'avocat*, N 1945.

52 FELLMANN, *Anwaltsrecht*, N 636.

53 FELLMANN, *Anwaltsrecht*, N 636.

54 FELLMANN, *Anwaltsrecht*, N 636.

55 WAGNER/ZWIRNER, *Cyber Risk in Anwaltskanzleien*, p. 169.

56 ATF 133 III 121, consid. 3.1 (concernant un médecin) ; ATF 117 II 563, consid. 2a (concernant un avocat).

consciencieux exercerait dans la même situation[57]. Si l'avocat a un devoir de diligence en matière de sécurité de l'information, il est en revanche difficile de le délimiter abstraitement[58]. A cet égard, s'il existe dans une profession ou dans un secteur de l'économie des règles de l'art généralement reconnues et des règles déontologiques, on peut les prendre en considération pour déterminer la diligence requise[59]. D'après Wolfgang STRAUB, comme de nombreux cabinets d'avocats s'occupent le moins possible des questions informatiques, on pourrait plutôt parler d'un manque de diligence usuel dans la branche[60]. Toutefois, comme le relève cet auteur, une négligence généralisée dans un secteur particulier ne donne pas lieu à un allégement si elle semble inappropriée d'un point de vue objectif. A notre avis, en l'absence de lignes directrices publiées par la Fédération suisse des avocats, il convient de se référer aux conseils publiés par le CCBE[61].

En Suisse, nous n'avons pas connaissance de procédures qui auraient été engagées par des clients contre des avocats sur la base d'une faille dans un système ou d'une fuite de données. D'une part, il est très compliqué, voire impossible, pour un client d'avoir connaissance d'une atteinte à ses données électroniques, sans mentionner le fait que les dommages économiques (perte d'exploitation et de réputation) sont très difficiles à prouver. D'autre part, la procédure sera souvent réglée en dehors des tribunaux (par la voie de l'arbitrage ou d'un arrangement extrajudiciaire), l'avocat ou l'étude d'avocat concerné préférant éviter les retombées négatives d'une telle procédure.

Les assurances responsabilité civile professionnelle ne couvrent en principe pas les cyber événements engageant la responsabilité civile des avocats. D'après les CGA du contrat d'assurance responsabilité civile professionnelle d'AXA (édition juillet 2016), les prétentions pour les dommages en rapport avec le vol de données clients ne sont pas assurées (point B2.15). Il en va de même des prétentions pour les dommages causés aux choses confiées (point B2.21). Il est en revanche possible d'étendre l'assurance responsabilité civile professionnelle en dérogeant au point B2.21 précité. Cette extension couvre les prétentions découlant de dommages dus à des logiciels malveillants (« malware »), tels que des virus ou chevaux de Troie, introduits par un assuré dans des systèmes informatiques de tiers (point C3.1). Dans ce cadre, l'assuré est tenu de mettre en œuvre, de manière avérée, des systèmes de protection usuels et actuels, tels qu'un logiciel antivirus ou un pare-feu (point C3.2). Cette extension couvre uniquement les dommages qui seraient

57 ATF 127 III 328, consid. 3 (concernant un expert) ; ATF 115 II 62, consid. 3a, JdT 1989 I p. 539 (concernant un gérant de fortune) ; TF arrêt 4A_63/2011 du 6 juin 2011, consid. 2 (concernant une fiduciaire).

58 STRAUB, *Durchklick (Teil 1)*, p. 523.

59 CR COI-WERRO, art. 398 CO, N 14 et les réf. cit. ; voir aussi FAVRE, *Sorgfaltspflichten*, p. 9.

60 STRAUB, *Durchklick (Teil 1)*, p. 523.

61 CCBE, *Conseils du CCBE pour le renforcement de la sécurité informatique des avocats*.

causés par un avocat (ou un auxiliaire dont il répond) qui aurait p. ex. introduit un virus dans le système informatique d'un confrère ou d'un client. Elle ne couvre en revanche pas les dommages qui auraient été causés par un virus aux données qui ont été confiées à l'avocat par un client. Ces risques peuvent être couverts par une assurance *ad hoc* appelée « Assurance Cyber Entreprises » (édition janvier 2018). Cette assurance couvre les cyber événements causant un dommage propre (p. ex. les frais de reconstitution des données électroniques et les pertes d'exploitation) et ceux engageant la responsabilité civile (p. ex. les violations de la protection des données et la violation de l'obligation de confidentialité ou la perte d'informations confidentielles).

5. La responsabilité en matière de protection des données

a) Les mesures de sécurité des données

Le traitement des données concernant des personnes physiques et morales effectué par des personnes privées tombe sous le coup de la Loi fédérale sur la protection des données (ci-après : LPD)[62]. L'art. 7 al. 1 LPD prévoit que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. La plupart des données détenues par un cabinet d'avocats sont des données personnelles au sens de la LPD et doivent par conséquent être protégées de manière adéquate[63].

Le règlement général européen sur la protection des données personnelles (ci-après : le RGPD)[64], applicable depuis le 25 mai 2018 dans l'ensemble des États membres, concerne aussi les avocats et les études d'avocats[65]. D'après l'art. 32 par. 1 RGPD, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles *appropriées* afin de garantir un niveau de sécurité *adapté au risque*, y compris entre autres, selon les besoins : la pseudonymisation et le chiffrement des données à caractère personnel (point a) ; des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes de systèmes et des services de traitement (point b) ; des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans les délais appropriés

62 LPD ; RS 235.1.

63 WAGNER/ZWIRNER, *Cyber Risk in Anwaltskanzleien*, p. 170.

64 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 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.

65 En France, voir p. ex. CONSEIL NATIONAL DES BARREAUX/BARREAU DE PARIS/CONFERENCE DES BATONNIERS, *Guide pratique*. En Slovaquie, voir aussi SLOVAK BAR ASSOCIATION, *Code of Conduct for Processing of Personal Data by Lawyers under the EU GDPR*.

en cas d'incident physique ou technique (point c) ; et une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement (point d). La violation de l'art. 32 RGPD peut être sanctionnée par une amende administrative pouvant s'élever jusqu'à dix millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (art. 83 par. 4 point a) RGPD). De plus, le responsable du traitement est tenu de réparer le préjudice matériel ou moral subi par une personne du fait de la violation du règlement (art. 82 par. 1 RGPD).

En Suisse, le projet de Loi fédérale sur la protection des données[66] précise que 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 (art. 7 al. 1 P-LPD). Le message explique que cette disposition *matérialise l'approche fondée sur les risques*[67]. Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre seront élevées[68]. Ces mesures doivent permettre d'éviter toute violation de la sécurité des données (art. 7 al. 2 P-LPD), soit toute violation de la sécurité entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite (art. 4 let. g P-LPD). Les exigences minimales en matière de sécurité des données personnelles seront édictées par le Conseil fédéral (art. 7 al. 3 P-LPD).

Contrairement au RGPD, le projet ne confère pas à l'autorité de contrôle le pouvoir d'infliger des sanctions administratives. Il confère en revanche au Préposé fédéral à la protection des données et à la transparence (ci-après : PFPDT) la compétence de prononcer un certain nombre de mesures administratives qui, en cas de non-respect, pourront entraîner des sanctions pénales (art. 57 P-LPD). En compensation, les dispositions pénales du projet ont été renforcées[69]. Sous le titre « violation des devoirs de diligence », l'art. 55 let. c P-LPD prévoit que les personnes privées qui, intentionnellement, ne respectent pas les exigences minimales en matière de sécurité des données personnelles édictées par le Conseil fédéral selon l'art. 7 al. 3 P-LPD seront, sur plainte, punies d'une amende de 250'000 francs au plus.

66 Le projet devrait être examiné par le Conseil national à la session d'automne 2019.

67 FF 2017 6565, p. 6650.

68 FF 2017 6565, p. 6650.

69 FF 2017 6565, p. 6594.

b) L'obligation d'annoncer les violations de la sécurité des données

En Suisse, la LPD ne prévoit aucune obligation d'annoncer les violations de la sécurité des données.

D'après le RGPD, toute violation de données à caractère personnel doit être notifiée à l'autorité de contrôle par le responsable du traitement, dans les meilleurs délais et, si possible, *72 heures au plus tard après en avoir pris connaissance*, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physique (art. 33 par. 1 RGPD).

Il conviendra également, lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, d'informer directement la personne concernée de la violation (art. 34 par. 1 RGPD). La communication à la personne concernée ne sera pas nécessaire, notamment si des mesures techniques et organisationnelles ont rendu les données incompréhensibles pour toute personne (p. ex. en cas de chiffrement) ou des mesures ont été prises pour que le risque ne soit plus « susceptible de se matérialiser » (art. 34 par. 3 points a) et b) RGPD). Le RGPD autorise en outre une communication publique si la communication à la personne concernée exigerait des efforts disproportionnés (art. 34 par. 3 point c) RGPD). Si le cabinet d'avocat n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au par. 3 de l'art. 34 RGPD est remplie (art. 34 par. 4 RGPD).

Les violations des art. 33 et 34 RGPD peuvent être sanctionnées par une amende administrative pouvant s'élever jusqu'à dix millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (art. 83 par. 4 point a) RGPD).

En Suisse, l'art. 22 P-LPD instaure également une obligation d'annoncer toute violation de la sécurité des données personnelles. L'alinéa 1 dispose que le responsable du traitement annonce au préposé *dans les meilleurs délais* toute violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Selon l'alinéa 4, le responsable du traitement informe la personne concernée lorsque cela est nécessaire à sa protection ou lorsque le préposé l'exige. Le message explique, à cet égard, qu'il existe une marge d'appréciation assez large pour déterminer si la première condition est réalisée et qu'il faut notamment se demander si l'information peut réduire les risques pour la

personnalité ou les droits fondamentaux de la personne concernée, en lui permettant notamment de prendre les dispositions nécessaires pour se protéger (modification des données d'accès ou du mot de passe, p. ex.)[70]. L'alinéa 5 permet en outre au responsable du traitement, dans des cas particuliers, de restreindre l'information de la personne concernée, la différer ou y renoncer. Enfin, l'alinéa 6 prévoit qu'une annonce fondée sur l'article 22 P-LPD ne peut être utilisée dans le cadre d'une procédure pénale contre la personne tenue d'annoncer qu'avec son consentement. D'après le message, ce consentement est requis dans la mesure où l'obligation d'annoncer les violations de la sécurité des données personnelles peut entrer en conflit avec le droit de ne pas contribuer à sa propre incrimination[71].

De manière incompréhensible, le projet ne prévoit aucune sanction en cas de non-respect de l'obligation d'annoncer les violations de la sécurité des données[72]. Tout au plus, le PFPDT pourrait ordonner à un responsable du traitement d'annoncer les violations des données au sens de l'art. 22 P-LPD (voir art. 45 al. 3 let. f P-LPD). C'est ensuite le non-respect de cette décision qui pourrait ouvrir la voie à une sanction pénale pour insoumission à cette décision (art. 57 P-LPD). A notre avis, cette absence de sanction rend l'obligation d'annonce inefficace. Dans la majorité des cas, seul le responsable du traitement des données aura connaissance d'une violation des données ; l'obligation d'annonce – même si elle est contraignante – permet de rétablir un certain équilibre dans le contexte des données numériques. En l'état actuel du projet, nous ne voyons pas ce qui inciterait le responsable du traitement des données à annoncer spontanément une violation. Les concepteurs du projet pensent peut-être qu'il annoncera spontanément la violation des données pour bénéficier du régime de l'art. 22 al. 6 P-LPD, qui précise qu'une annonce effectuée en application de l'art. 22 P-LPD ne pourra être utilisée dans une procédure pénale engagée contre la personne soumise à l'obligation d'annoncer qu'avec le consentement de celle-ci. Les contours de cette disposition sont cependant peu clairs. S'appliquera-t-elle uniquement au PFPDT ou également au client de l'avocat informé de la violation de ses données ? Dans ce second cas, nous ne voyons pas comment il serait possible d'empêcher un client informé d'une violation de ses données de déposer une plainte pénale contre un avocat au sens de l'art. 321 CP et – encore moins – de conditionner le dépôt de cette plainte au consentement de l'avocat. De plus, une telle annonce n'exclurait *a priori* pas l'ouverture d'une procédure disciplinaire pour violation du secret professionnel (art. 13 LLCA) ou l'introduction d'une action civile (si la personne concernée est informée par le PFPDT de la violation de ses données). Ainsi, l'avocat aura rapidement pris la

70 FF 2017 6565, p. 6681-6682.

71 FF 2017 6565, p. 6682.

72 Voir aussi à ce sujet : METILLE, *Annoncer les failles de sécurité*, p. 866.

décision qui sauvegarde ses seuls intérêts personnels : taire la violation des données de son client. A ce sujet, le projet fait preuve d'une naïveté déconcertante, à tel point qu'il est permis de se demander s'il est encore utile de prévoir une obligation d'annonce dont les contours semblent plus facultatifs qu'obligatoires.

A noter que dans le contexte de la réglementation des sociétés d'avocats et d'une future loi règlementant la profession d'avocat en Suisse, l'auteur avait suggéré la mise en place d'une obligation d'annonce à l'autorité de surveillance des avocats en cas de violation des règles professionnelles[73], ce qui aurait inclus l'obligation d'annoncer les failles de sécurité lorsque les données compromises sont soumises au secret professionnel de l'avocat. Il est intéressant de relever que l'ABA a récemment rendu un avis, sous l'angle des règles professionnelles de l'avocat, estimant que les avocats ont l'obligation d'aviser leurs clients en cas d'atteinte à la sécurité des données en vertu du chiffre 1.4 des *Model Rules*[74]. A notre sens, on peut se demander si une obligation similaire ne devrait pas, en Suisse également, être déduite des règles professionnelles de l'avocat, en particulier de l'art. 12 let. a LLCA.

D. Les recommandations pour réduire les risques

Dans le cadre de cette contribution, nous formulons quelques recommandations non exhaustives. Les avocats et les cabinets d'avocats devraient :

- S'assurer que le personnel de l'étude est régulièrement formé concernant la sécurité des données. La cybersécurité exige une formation de haut en bas, c'est-à-dire qu'il faut prendre en charge le personnel dès son arrivée tout en l'informant régulièrement de tout développement ou changement important ; formation qui devrait être dispensée à tous les niveaux de l'entreprise (y compris aux associés)[75] ;
- Prévoir un mot de passe pour accéder à chacun de leurs appareils (y compris les téléphones portables et les tablettes), ainsi qu'un verrouillage automatique de ces derniers après une certaine inactivité[76] ;
- Mettre à jour régulièrement leurs systèmes d'exploitation et leurs logiciels[77] ;

---

73 GURTNER, *La réglementation des sociétés d'avocats*, p. 384 ss.

74 ABA Formal Opinion 483.

75 WRIGHT, *Cyber Security Toolkit*, p. 78.

76 BANDLER, *Cybersecurity*, Emplacements Kindle 2414 et 2425.

- Installer des logiciels antivirus et des logiciels de protection contre les logiciels malveillants sur les ordinateurs de bureau et les appareils mobiles[78]. Il est utile à ce sujet de consulter des tests indépendants, les logiciels les plus connus n'étant pas forcément les plus performants[79] ;
- En l'absence de programmes de chiffrement standard (p. ex. *Secure Sockets Layer* [SSL] ou *Transport Layer Security* [TLS]) chiffrant[80] les courriels de bout en bout (c'est-à-dire pas uniquement chiffrés sur le serveur de courriels, mais aussi pendant la transmission), utiliser un logiciel pour chiffrer les pièces jointes[81] ;
- En cas de besoin, chiffrer les appareils mobiles (téléphones portables, tablettes, ordinateurs portables, etc.) et les supports de données (clés USB, disques durs externes, etc.), étant précisé que le simple fait d'exiger un mot de passe ne signifie pas qu'un appareil ou un support est réellement chiffré[82]. Le chiffrement est essentiel pour assurer une confidentialité maximale[83] ;
- Eviter d'utiliser les Wi-Fi publics dans les aéroports, les hôtels et les cafés qui n'ont souvent pas de dispositifs de sécurité nécessaires pour protéger les données confidentielles des clients[84] ;
- Eviter de stocker des documents dans un service *cloud* comme Dropbox. Ce dernier doit être considéré comme un dépôt public et les documents sensibles doivent être chiffrés avant d'y être placés[85]. Le barreau

---

77 Le cabinet d'avocats panaméen Mossack Fonseca employait des logiciels désuets avec des vulnérabilités critiques qui étaient largement connues des pirates informatiques (THOMSON, *Understand Cybersecurity Risks*, Chapitre 2, II.).

78 CCBE, *Conseils du CCBE pour le renforcement de la sécurité informatique des avocats*, p. 14.

79 Voir p. ex. : https://www.av-test.org/fr/ ; https://www.av-comparatives.org/. Voir aussi la liste proposée par BANDLER, *Cybersecurity*, Emplacements Kindle 2438 et 2449, qui suggère notamment d'utiliser la version gratuite de Malwarebytes, disponible sur : https://fr.malwarebytes.com/ (consultés le 22.07.2019).

80 FURRER et al., *Legal Tech*, p. 11, définissent le chiffrage comme suit : « Méthodes et algorithmes qui convertissent les données sous une forme illisible à l'aide de codes ou de clés numériques ou électroniques. En même temps, il est garanti que seules les données illisibles peuvent être à nouveau décryptées seulement avec la bonne clé ».

81 En utilisant p. ex. le logiciel 7-Zip, disponible sur : https://www.7-zip.org (consulté le 22.07.2019). Pour les détails de la procédure, voir WRIGHT, *Cyber Security Toolkit*, p. 126. En termes de confidentialité, Wolfgang STRAUB et Peter WRIGHT comparent l'envoi de courriels non cryptés à l'envoi de cartes postales, qui peuvent être lues librement par toutes les personnes impliquées dans le transport (STRAUB, *Durchklick (Teil 1)*, p. 522 ; WRIGHT, *Cyber Security Toolkit*, p. 114).

82 WRIGHT, *Cyber Security Toolkit*, p. 127-128. Il est utile de préciser que les iPhones et IPads (Apple) sont chiffrés par défaut lorsqu'un mot de passe est activé (BANDLER, *Cybersecurity*, Emplacement Kindle 3493).

83 Concernant les avantages et les inconvénients du chiffrement, voir BANDLER, *Cybersecurity*, Emplacement Kindle 3505.

84 THOMSON, *Understand Cybersecurity Risks*, Chapitre 2, III. G ; WRIGHT, *Cyber Security Toolkit*, p. 111.

85 THOMSON, *Understand Cybersecurity Risks*, Chapitre 2, III. G.

slovaque déconseille p. ex. aux avocats d'utiliser dans l'exercice de leur profession des courriels ou des services de stockage proposant des services gratuits de *cloud* qui ne sont pas sûrs, de stocker des données dans des endroits qui ne garantissent pas la protection requise des données personnelles (en dehors de l'Espace Économique Européen) et qui sont la cible de pirates et de logiciels malveillants (malware) (comme Gmail, Google Drive, Hotmail, OneDrive, iCloud ou Dropbox)[86] ;

- Placer les appareils mobiles avec les bagages à main à bord de l'avion plutôt que dans les bagages enregistrés en soute[87] ;
- Sécuriser l'enlèvement et le recyclage des supports électroniques employés par les avocats, étant précisé que les scanners et les photocopieuses modernes renferment très souvent une mémoire ou un disque dur[88] ;
- Réfléchir aux conséquences de l'utilisation de services de prestataires américains en matière d'archivage ou de stockage de données, même si les serveurs de ces prestataires sont situés en Suisse ou dans l'Union européenne. Depuis l'adoption aux États-Unis le 23 mars 2018 du *Clarifying Lawful Overseas Use of Data Act* (aussi appelé le « Cloud Act »), toute société américaine au sens du droit américain, c'est-à-dire une société incorporée aux États-Unis ainsi que les sociétés contrôlées par elle, doit communiquer aux autorités américaines, à leur demande, les données placées sous son contrôle *sans considération du lieu où ses données se trouvent stockées*. Le CCBE a récemment publié un document concernant le Cloud Act dans lequel il indique être « particulièrement préoccupé » par le fait que cette nouvelle réglementation ne tient pas compte du secret professionnel de l'avocat dans l'Union européenne[89].
- Envisager la conclusion d'une assurance cyber-risque.

---

86 SLOVAK BAR ASSOCIATION, *Code of Conduct for Processing of Personal Data by Lawyers under the EU GDPR*, p. 24-25.

87 CCBE, *Conseils du CCBE pour le renforcement de la sécurité informatique des avocats*, p. 13. Concernant la sécurité lors des voyages, voir BANDLER, *Cybersecurity*, chapitre 12.

88 CCBE, *Conseils du CCBE pour le renforcement de la sécurité informatique des avocats*, p. 15. Pour une liste des étapes à suivre, voir BANDLER, *Cybersecurity*, annexe 6 (pour les téléphones portables et les tablettes) et annexe 7 (pour les ordinateurs portables et les ordinateurs de bureau).

89 CCBE, *Évaluation du CCBE de la loi CLOUD Act des États-Unis*, p. 9-12.

III. La responsabilité des avocats et l'intelligence artificielle

Après une introduction (A), l'auteur présentera quelques applications utilisant l'intelligence artificielle (ci-après : l'IA) (B), avant d'aborder les conséquences de l'IA pour les avocats (C). Il discutera ensuite de l'utilisation des nouvelles technologies en tant que devoir de diligence de l'avocat (D), puis examinera la question de l'imputation de la responsabilité lors de l'utilisation de l'IA (E). Ce chapitre se terminera par une mise en garde des avocats concernant l'utilisation des algorithmes[90] (F).

A. Introduction

Nick BOSTROM définit l'IA comme suit : des machines qui correspondent à l'intelligence générale des humains, c'est-à-dire qui possèdent un bon sens et une capacité réelle à apprendre, raisonner et planifier pour relever des défis complexes en matière de traitement de l'information dans un large éventail de domaines naturels et abstraits[91]. Il existe une multitude de définitions de l'IA ; elles peuvent être classées en fonction de quatre objectifs différents à atteindre : penser humainement, agir humainement, penser rationnellement ou agir rationnellement[92].

En 1961, Marvin Lee MINSKY, pionnier de l'IA, pensait déjà que nous étions à l'aube d'une ère qui serait fortement influencée, et très probablement dominée, par des machines intelligentes résolvant des problèmes[93]. Moins de soixante ans plus tard, l'IA est partout, sans que nous nous en rendions forcément compte : elle est utilisée par le moteur de recherche de Google, par l'assistant Google, par Amazon pour proposer à ses utilisateurs des ouvrages ou par Facebook pour identifier automatiquement des utilisateurs sur des photos.

L'IA a fait ces dernières années d'importants progrès dans les domaines de la reconnaissance d'images et du traitement automatique du langage naturel. Google a p. ex. récemment dévoilé une application qui permet à un utilisateur de demander à l'assistant Google d'appeler pour lui un salon de coiffure pour

90 FURRER et al., *Legal Tech*, p. 2, définissent les algorithmes comme suit : « Commandes pour les processus numériques avec une instruction d'action sans ambiguïté et un nombre fini d'instructions individuelles pour résoudre un problème ou une classe de problèmes. La fonctionnalité du logiciel résulte de la substance logique ».

91 BOSTROM, *Superintelligence*, p. 3.

92 RUSSEL/NORVIG, *Artificial Intelligence*, p. 2.

93 MINSKY, *Steps Toward Artificial Intelligence*, p. 8.

prendre un rendez-vous ou un restaurant pour réserver une table[94]. Dans ce contexte, l'application est en mesure de dialoguer avec un humain de manière assez convaincante ; possibilité qui était encore inimaginable il y a quelques années.

Dans sa résolution du 16 février 2017, le Parlement européen a souligné que « l'humanité se trouve à l'aube d'une ère où les robots, les algorithmes intelligents, les androïdes et les autres formes d'intelligence artificielle, de plus en plus sophistiqués, semblent être sur le point de déclencher une nouvelle révolution industrielle qui touchera probablement toutes les couches de la société »[95].

Les avocats ne seront pas épargnés. Lors d'une présentation, Andrew ARRUDA, CEO et cofondateur de ROSS Intelligence, indiquait que les avocats comprendront tous à l'avenir comment utiliser et travailler avec les systèmes d'IA de la même façon qu'ils travaillent aujourd'hui avec Word et Excel[96]. Certains auteurs considèrent même que la pratique du droit changera probablement davantage dans les cinq prochaines années que dans les cinquante années passées[97]. Il est donc utile de s'intéresser à ces nouvelles applications qui vont profondément bouleverser la profession d'avocat.

B. Quelques applications utilisant l'IA

1. La révision de documents contractuels

LawGeex est un outil de révision de documents contractuels utilisant l'IA qui a été fondé en 2014[98]. L'IA a été entraînée à revoir des dizaines de milliers d'accords de confidentialité en utilisant l'apprentissage automatique (*machine learning* en anglais) et l'apprentissage profond (*deep learning* en anglais). Selon un rapport publié en 2018[99], vingt avocats expérimentés formés aux États-Unis ont été confrontés à l'algorithme d'IA *LawGeex*. Les avocats avaient quatre heures pour revoir cinq accords de confidentialité. L'IA a atteint un niveau de précision de 94 %, alors que celui des vingt avocats a été en moyenne de 85 %. Il aura fallu en moyenne 92 minutes aux avocats pour revoir les cinq accords, alors que *LawGeex* les a revus en 26 secondes seulement.

---

94 LEVIATHAN/MATIAS, *Google Duplex*. Voir aussi WELCH, *Google Demo*.

95 PARLEMENT EUROPEEN, *Résolution 2015/2103(INL)*, let. B.

96 Innovative Legal Services Forum 2018 (ILSF), le 17 mai 2018, Prague, République tchèque.

97 CONSEIL NATIONAL DES BARREAUX, *Guide de l'avocat numérique*, p. 29.

98 LawGeex, disponible sur : https://www.lawgeex.com/ (consulté le 22.07.2019).

99 LAWGEEX, Comparing the Performance of Artificial Intelligence to Human Lawyers in the Review of Standard Business Contracts, février 2018, disponible sur : https://www.lawgeex.com/AIvsLawyer/.

Une start-up hollandaise, NDA Lynn[100], propose actuellement de réviser gratuitement des accords de confidentialité, le document envoyé par les utilisateurs étant utilisé pour améliorer le modèle. A défaut, le tarif est fixé à 45 euros.

Legartis, une start-up basée à Zurich, propose un logiciel utilisant l'IA pour réviser des documents contractuels[101].

Claudette, acronyme de « automated CLAUse DETecTEr », est un outil qui permet d'évaluer la légalité des contrats de consommation et des politiques de confidentialité proposés en ligne[102].

De manière non exhaustive, on mentionnera encore Legal Robot[103] ou Luminance[104] qui proposent de réviser des documents contractuels.

2. *La justice prédictive*

Jean LASSEGUE et Antoine GARAPON définissent la justice prédictive comme la capacité prêtée aux machines de mobiliser rapidement en langage naturel le droit pertinent pour traiter une affaire, de le mettre en contexte en fonction de ses caractéristiques propres (lieu, personnalité des juges, des cabinets d'avocats, etc.) et d'anticiper la probabilité des décisions qui pourraient intervenir[105].

Aux États-Unis, les chercheurs se sont intéressés très tôt à la justice prédictive[106]. En 2004, ils ont mis au point un modèle permettant de prédire les décisions de la Cour suprême des États-Unis rendues entre 1994 et 2002, représentant 628 affaires[107]. La particularité de ce modèle résidait dans le fait qu'il reposait sur les six variables suivantes : le circuit d'origine ; le domaine juridique de l'affaire ; la partie demanderesse (p. ex. : les États-Unis, un employeur, etc.) ; la partie intimée ; l'orientation idéologique (libérale ou conservatrice) de la décision de l'autorité intimée ; et si le demandeur soutient qu'une loi ou une pratique viole la constitution. En parallèle, des experts ont examiné les mêmes affaires en s'appuyant sur leurs connaissances juridiques et en tenant compte de facteurs non juridiques, comme les préférences politiques des juges. D'après le résultat de l'étude, le modèle a prédit

100 NDA Lynn, disponible sur : https://www.ndalynn.com/ (consulté le 22.07.2019).

101 Legartis, disponible sur : https://www.legartis.ai/ (consulté le 22.07.2019).

102 CLAUDETTE, disponible sur : http://claudette.eui.eu/index.html (consulté le 22.07.2019).

103 Legal Robot, disponible sur : https://www.legalrobot.com/ (consulté le 22.07.2019).

104 Luminance, disponible sur : https://www.luminance.com/ (consulté le 22.07.2019).

105 LASSEGUE/GARAPON, *Justice digitale*, p. 219.

106 KORT, *Predicting Supreme Court Decisions Mathematically* (1957) ; LAWLOR, *What Computers Can Do*, qui supposait déjà en 1963 que les ordinateurs seraient un jour en mesure d'analyser et de prédire l'issue des décisions judiciaires.

107 RUGER et al., *The Supreme Court Forecasting Project*, p. 1150-1209.

correctement 75 % des décisions, alors que les experts sont arrivés à un résultat correct dans 59,1 % des cas. Plus récemment, toujours aux États-Unis, des chercheurs ont développé un modèle de prédiction basé sur plus de 240'000 votes et 28'000 résultats issus de la Cour suprême des États-Unis sur une période de près de deux siècles (1816-2015). Le modèle a atteint une précision de 70,2 % concernant l'issue de la procédure et de 71,9 % concernant les votes des juges[108].

En Europe, en se basant sur les progrès récents du traitement automatique du langage naturel et de l'apprentissage automatique, des chercheurs ont construit un modèle permettant de prédire les décisions de la Cour européenne des droits de l'homme[109]. Ils ont analysé 584 affaires de la Cour, correspondant à trois articles de la Convention européenne des droits de l'homme : l'interdiction de la torture (article 3), le droit à un procès équitable (article 6) et le droit au respect de la vie privée et familiale (article 8). Dans 79 % des cas, l'IA est arrivée à un résultat similaire à ceux des juges. Les chercheurs ont précisé que les jugements de la Cour ont une structure bien distincte, ce qui les rend particulièrement adaptés à l'analyse de texte[110].

Comme l'expliquent Jean-Pierre BUYLE et Adrien VAN DEN BRANDEN, l'analyse prédictive des décisions de justice est rendue plus aisée dans les pays et les systèmes juridiques où l'opinion dissidente est autorisée, ce qui est le cas de la Cour suprême des États-Unis et de la Cour européenne des droits de l'homme[111]. En effet, la connaissance des opinions dissidentes des juges facilite leur profilage et augmente ainsi la prédictibilité de leurs positions futures[112].

En France, la société Case Law Analytics propose de modéliser le processus de décision judiciaire pour présenter à ses clients l'ensemble des décisions qui seraient prises sur un dossier donné[113]. D'après le site Internet de la société, ses services s'adressent aux cabinets d'avocats, aux directions juridiques, aux assurances de protection juridique et aux experts-comptables. La société propose aux cabinets d'avocats de quantifier le risque pour les clients dès le premier rendez-vous, d'avoir de l'information judiciaire quelle que soit la juridiction et de justifier plus précisément des rémunérations variables au succès. La société Predictice, quant à elle, indique pouvoir analyser des millions de décisions de justice en 1 seconde[114].

---

108 KATZ et al., *A general Approach*.

109 ALETRAS et al., *Predicting judicial decisions* ; voir aussi HAWADIER, *L'avocat*, emplacements Kindle 1321-1329.

110 ALETRAS et al., *Predicting judicial decisions*, p. 4.

111 BUYLE/VAN DEN BRANDEN, *La robotisation de la justice*, p. 294.

112 BUYLE/VAN DEN BRANDEN, *La robotisation de la justice*, p. 294.

113 Case Law Analytics, disponible sur : https://www.caselawanalytics.com/ (consulté le 22.07.2019).

114 Predictice, disponible sur : https://predictice.com/ (consulté le 22.07.2019).

Aux États-Unis, la société Premonition se décrit comme donnant un avantage très injuste dans les litiges[115]. Elle indique que son système d'IA est capable d'extraire de grandes quantités de données pour savoir quels avocats gagnent devant quels juges, ce qui augmenterait le taux de succès dans les litiges de 30,7 %.

La justice prédictive va profondément bouleverser le travail du juge et de l'avocat. Certains auteurs estiment que dans quelques années des évaluations prédictives seront produites par chaque partie et figureront au dossier comme une échographie dans un dossier médical[116]. Si les deux parties savent très précisément ce qu'elles pourront obtenir en entamant une procédure judiciaire, il est possible que la justice prédictive mène à une forme de déjudiciarisation, car les parties préféreront opter pour un règlement alternatif du litige[117]. Une autre conséquence est l'effet moutonnier : le juge pourrait être poussé à prendre la même décision que la majorité de ses collègues dans le même type d'affaire[118]. Certains se demandent encore si on ne va pas assister à un appauvrissement de la jurisprudence, dans la mesure où il pourrait y avoir un risque que les algorithmes basés sur la jurisprudence se révèlent très conservateurs et bloquent l'évolution et l'amélioration du droit[119].

3. La recherche juridique

ROSS Intelligence est un outil utilisant l'IA dont le but est de soutenir les activités de recherche juridique[120]. ROSS utilise le traitement automatique du langage naturel et les capacités d'apprentissage automatique pour identifier les sources juridiques pertinentes concernant des questions particulières. Le logiciel est basé sur le système informatique Watson d'IBM. D'après une étude récente[121], ROSS permettrait de réduire le temps de recherche entre 22,3 % et 30,3 %. Par ailleurs, la société a lancé en 2018 un nouveau produit appelé EVA[122], qui permet d'examiner les mémoires juridiques, plus particulièrement de vérifier l'historique des affaires citées et si elles sont toujours pertinentes. De manière intéressante, EVA permet de résumer une affaire sur la base d'une question posée en langage naturel (p. ex. « What is the doctrine of inevitable

115 Premonition, disponible sur : https://premonition.ai/ (consulté le 22.07.2019).

116 LASSEGUE/GARAPON, *Justice digitale*, p. 241.

117 BERTHEREAU, *La justice prédictive*, p. 48. Dans ce sens aussi : BUYLE/VAN DEN BRANDEN, *La robotisation de la justice*, p. 295.

118 BERTHEREAU, *La justice prédictive*, p. 49.

119 BERTHEREAU, *La justice prédictive*, p. 50, qui se demande notamment si le passé doit gouverner le futur.

120 Voir aussi GURTNER, *L'innovation et l'avenir de la profession d'avocat*.

121 Blue Hill Research, ROSS Intelligence and Artificial Intelligence in Legal Research, Numéro du rapport : A0280, janvier 2017.

122 Ross Intelligence, disponible sur : https://eva.rossintelligence.com/ (consulté le 22.07.2019).

discovery ? »), ce qui permet d'éviter de lire l'intégralité d'un jugement et de gagner du temps[123].

En France, Juri'Predis est un moteur de recherche juridique doté de l'IA qui indique « imiter l'indexation humaine de la jurisprudence »[124]. D'après son site Internet, grâce à ses algorithmes, le moteur de recherche serait capable de procéder à une analyse qualitative de la jurisprudence, de réaliser une pré-interprétation des données et les trier pour proposer à l'utilisateur les arguments jurisprudentiels les plus pertinents, d'identifier les jurisprudences constantes, appartenant à un même courant jurisprudentiel, et de trouver les séries jurisprudentielles de cas semblables.

4. Les agents ou robots conversationnels (chatbots)

Andreas FURRER et al. définissent un *chatbot* comme suit[125] :

> *« Système informatique qui peut être contrôlé par le langage naturel. Le système reconnaît la langue et s'appuie sur une base de données interne. L'utilisation de l'intelligence artificielle ouvre de nouveaux domaines d'application, qui permettent également au système de communiquer avec ses utilisateurs en dialoguant ».*

Certains auteurs estiment que les « Lawyer Bots » sont parmi les outils les plus matures qui peuvent déjà générer un retour sur investissement important[126].

L'assurance de protection juridique Coop travaille actuellement sur un projet pilote appelé « Blitzbot ». L'objectif de ce robot est de répondre à des questions juridiques concernant des excès de vitesse en matière de circulation routière[127]. L'outil est basé sur le programme d'IA Watson conçu par IBM dans le but de répondre à des questions formulées en langage naturel[128].

En Allemagne, un cabinet d'avocats a créé un *chatbot* qui permet à ses utilisateurs d'obtenir de l'aide en cas de licenciement ou de réclamer une indemnisation quand un vol est retardé[129].

---

123 Ross Intelligence, How to Generate an Overview on EVA, disponible sur : https://perma.cc/P5Z2-9KDN.

124 Juri'Predis, disponible sur : https://www.juripredis.com/ (consulté le 22.07.2019).

125 Furrer et al., *Legal Tech*, p. 11.

126 ÖHNER/GRAF, *Lawyer Bots*, p. 283.

127 Busse ? Fragen Sie den Blitzbot, Roboter als digitale Juristen, in *SRF*, le 25 juillet 2018, disponible sur : https://www.srf.ch/news/panorama/busse-fragen-sie-den-blitzbot-roboter-als-digitale-juristen [https://perma.cc/JN9A-UXU2].

128 IBM Watson, disponible sur : https://www.ibm.com/watson/ (consulté le 22.07.2019).

129 RATIS Rechtsanwaltsgesellschaft mbH, disponible sur : https://ratis.de/chatbot/ (consulté le 22.07.2019).

Il existe d'autres robots, comme DoNotPay[130] qui élabore gratuitement une argumentation juridique pour contester des contraventions de stationnement[131] ou, plus récemment, qui permet d'obtenir le remboursement du prix d'un billet d'avion ou d'une chambre d'hôtel lorsque le prix a diminué après la réservation.

Dans le même ordre d'idée, on mentionnera encore Flightright[132] ou Fairplane[133].

Le gouverneur de l'État de Californie a récemment signé un projet de loi, visant les agents ou robots conversationnels, qui entrera en vigueur le 1er juillet 2019. Une fois en vigueur, cette réglementation interdira à toute personne d'utiliser un robot pour communiquer ou interagir avec une autre personne dans le but notamment de l'induire en erreur sur son identité artificielle[134]. La personne ne sera cependant pas responsable si elle divulgue de manière claire qu'il s'agit d'un robot.

C. Les conséquences de l'IA pour les avocats

L'IA est à la porte des cabinets d'avocats. Elle vient concurrencer l'avocat sur ce qui fait sa spécificité : son intelligence. Comme le relèvent John O. MCGINNIS et Russel G. PEARCE, les machines intelligentes deviendront meilleures, tant en termes de performance que de coûts[135]. Contrairement aux humains, elles peuvent travailler 24 heures sur 24, sans dormir et sans caféine. Une telle accélération technologique de la puissance de calcul est la différence entre les améliorations technologiquement antérieures et celles qui découlent de l'IA[136]. Qu'est-ce que cela signifie concrètement pour les avocats ? Il est important de bien distinguer les connaissances et le traitement des connaissances (l'expertise).

D'après Stéphane MALLARD, les monopoles des connaissances n'existent plus aujourd'hui, parce que la connaissance est partout[137]. La connaissance n'est plus un actif stratégique ni un facteur différenciant, c'est devenu une

130 DoNotPay, disponible sur : https://www.donotpay.com/ (consulté le 22.07.2019).

131 Voir à ce sujet GURTNER, *L'innovation et l'avenir de la profession d'avocat*, p. 15-16.

132 FLIGHTRIGHT, disponible sur : https://www.flightright.com/ (consulté le 22.07.2019).

133 FAIRPLANE, disponible sur : https://www.fairplane.org/ (consulté le 22.07.2019).

134 Senate Bill No. 1001, Chapter 892, An act to add Chapter to Part 3 of Division 7 of the Business and Professions Code, relating to bots, approuvé par le gouverneur le 28 septembre 2018, disponible sur : http://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=201720180SB1001&version=20170SB100192CHP [https://perma.cc/3MCZ-MS9D].

135 MCGINNIS/PEARCE, *The Great Disruption*, p. 3041.

136 MCGINNIS/PEARCE, *The Great Disruption*, p. 3041.

137 MALLARD, *Disruption*, p. 147.

donnée dont tout le monde dispose à faible coût : une commodité[138]. Comme il le relève très justement, nous continuons à faire appel à des médecins et à des avocats, non pas pour leur connaissance, puisqu'elle est accessible à tous en trois clics, mais pour leur expertise, c'est-à-dire pour leur capacité à comprendre et à traiter la connaissance[139]. Il n'est donc plus tout à fait correct, selon nous, de parler d'asymétrie d'informations dans la relation entre un avocat et son client. On devrait plutôt parler d'asymétrie du traitement des connaissances.

Avec l'arrivée de l'intelligence artificielle, l'expertise pourrait très vite elle aussi devenir une simple commodité accessible à tous[140]. Il est possible que dans un premier temps l'algorithme augmente l'expert (assistance à la conduite dans les voitures, aide à la prise de décision pour les médecins ou les avocats), avant que toute l'expertise lui soit confiée (voiture entièrement autonome sans chauffeur, expertise sans médecins ou avocats)[141].

Une des questions fondamentales est de savoir si l'humain maintiendra un contrôle total sur l'expertise ou s'il acceptera de céder aux machines une partie du contrôle. A notre avis, une partie toujours plus importante des tâches traditionnellement effectuées par les avocats va être confiée à des machines qui seront plus rapides et moins chères[142]. Le recours à la machine va se démocratiser : l'avocat sera technologiquement augmenté – ce qui soulèvera des questions cruciales concernant sa relation avec la machine.

A terme, l'avocat devra se concentrer sur l'excellence de la relation qu'il entretient avec son client. Comme l'expertise sera confiée à des algorithmes, l'empathie sera la nouvelle valeur. Un bon avocat ne sera plus un avocat techniquement bon mais humainement excellent[143]. Les avocats devront s'adapter à ces changements[144].

D. L'utilisation des nouvelles technologies en tant que devoir de diligence

L'avocat est tenu à un devoir de diligence institué tant par le droit civil (art. 398 al. 2 CO) que par le droit administratif (art. 12 let. a LLCA)[145]. Ni la

138 MALLARD, *Disruption*, p. 147.

139 MALLARD, *Disruption*, p. 148.

140 MALLARD, *Disruption*, p. 148.

141 MALLARD, *Disruption*, p. 149.

142 Dans ce sens également : BUYLE/VAN DEN BRANDEN, *La robotisation de la justice*, emplacements Kindle 9026-9036.

143 MALLARD, *Disruption*, p. 154-155.

144 Pour une présentation plus complète de l'évolution de la profession d'avocat, voir GURTNER, *La réglementation des sociétés d'avocats*, p. 7-47.

145 Concernant la relation entre ces deux dispositions, voir ATF 144 II 473, consid. 5.3.1.

doctrine ni la jurisprudence n'ont dégagé de ces règles un véritable devoir de diligence des avocats en lien avec les nouvelles technologies. Et pourtant, un avocat ne peut plus s'appuyer aujourd'hui sur sa seule maîtrise du droit pour éviter d'engager sa responsabilité – et l'avocat de demain le pourra encore moins. Depuis 2012, l'ABA l'a compris en modifiant le commentaire du chiffre 1.1 des *Model Rules*, désormais adoptés par 31 États : un avocat doit comprendre les avantages et les risques liés aux nouvelles technologies. En d'autres termes, il doit être technologiquement compétent – ce qui inclut aussi le devoir de mandater un informaticien ou un autre professionnel lorsque les questions deviennent trop techniques.

Cette obligation ne devrait pas seulement être comprise dans le sens où il faut veiller à ne pas violer son devoir de diligence lors de l'utilisation des nouvelles technologies, mais également dans le sens où la *non-utilisation* des nouvelles technologies pourrait engager la responsabilité de l'avocat. Walter FELLMANN estime p. ex. que si les bases de données donnent accès aux connaissances nécessaires, l'avocat est tenu d'effectuer de telles recherches dans le cadre de son devoir de diligence[146]. Il est ainsi possible qu'à l'avenir les avocats seront légalement tenus d'utiliser l'IA dans le cadre de leur devoir de diligence, que cela soit pour la recherche juridique, la révision de documents contractuels ou l'analyse prédictive[147]. Si cette situation est nouvelle pour les avocats, elle surprendra moins les médecins. Ces derniers ont en effet depuis longtemps recours à des outils dont ils ne sauraient se passer au risque d'engager leur responsabilité. D'après Stuart J. RUSSEL et Peter NORVIG, « [i]f expert systems become reliably more accurate than human diagnosticians, doctors might become legally liable if they *don't* use the recommendations of an expert system »[148]. Ainsi, un avocat qui n'a pas recours à un outil d'analyse prédictive et qui a pris des décisions dommageables pour son client pourra à l'avenir être considéré comme responsable de la même manière qu'un dermatologue pourrait l'être pour des dommages découlant du fait qu'il n'a pas utilisé un système d'IA capable de détecter les cancers de la peau[149].

En résumé, l'utilisation des nouvelles technologies imposent aux avocats de nouvelles obligations qui sont susceptibles de générer de nouvelles responsabilités.

146 FELLMANN, *Anwaltsrecht*, N 1511 ; FELLMANN, *Haftung des Anwaltes*, p. 52.

147 Dans ce sens également : ALARIE et al., *How Artificial Intelligence Will Affect the Practice of Law*, p. 13.

148 RUSSEL/NORVIG, *Artificial Intelligence*, p. 1036.

149 Voir ESTEVA et al., *Dermatologist-Level Classification of Skin Cancer*.

E. L'imputation de la responsabilité

1. Le contexte

L'IA sera utilisée par les avocats pour décider s'il faut agir en justice, prédire l'issue d'une procédure ou préparer l'ébauche d'une argumentation juridique. Qui sera responsable si le client reçoit un mauvais conseil ? Est-ce que l'avocat pourra rejeter toute forme de responsabilité en invoquant la faute d'une machine ?[150]

Au regard du droit de la responsabilité civile, le facteur particulier n'est pas tant l'existence d'une machine, mais bien le développement de son autonomie. Les progrès réalisés ces dernières années dans le domaine de l'IA permettent aux applications d'accomplir des tâches non seulement *automatisées*, mais également *autonomes*, sans la participation d'une personne physique[151]. C'est cette notion d'autonomie qu'il convient d'examiner en premier lieu.

2. La notion d'agent et son degré d'autonomie

En informatique et en IA, les agents sont généralement définis par leur capacité à agir de manière autonome, de percevoir leur environnement, de durer sur une période de temps prolongée, de s'adapter aux changements, de créer et de poursuivre des objectifs[152]. D'après cette définition, une voiture n'est pas un agent si elle requiert un conducteur, alors qu'une voiture autonome est un agent[153]. Un thermostat, qui fonctionne indépendamment après avoir été programmé, est un agent ; même s'il ne fait rien d'autre que d'exécuter un ensemble prédéfini d'étapes en réponse à un ensemble prédéfini de perceptions[154]. Ces agents sont initiés, construits, programmés et utilisés par des humains. En revanche, les humains ne contrôlent pas nécessairement les agents en question.

On opère généralement les distinctions suivantes en fonction du degré de contrôle de l'humain sur la machine :

- *Human in the loop* : L'exemple le plus représentatif est celui des robots chirurgicaux qui fonctionnent le plus souvent sur un modèle maître-esclave, c'est-à-dire par simple téléopération par le praticien, à l'instar

150 Voir KATHRANI, *An "Existential" Shift ?*, qui soulève cette question – sans apporter de réponse.

151 Dans ce sens : JACQUEMIN/HUBIN, *Aspects contractuels*, emplacement Kindle 1918.

152 RUSSEL/NORVIG, *Artificial Intelligence*, p. 4.

153 HILDEBRANDT, *Smart Technologies and the End(s) of Law*, p. 22.

154 HILDEBRANDT, *Smart Technologies and the End(s) of Law*, p. 22-23.

du robot chirurgical Da Vinci[155]. Dans ce cas, l'humain participe activement et reste dans la boucle décisionnelle, si bien qu'il est plus difficile de parler d'autonomie du robot[156]. En réalité, ce degré d'autonomie est plus proche de l'automatisation[157].

- *Human on the loop* : D'autres agents opèrent de façon indépendante, mais sont supervisés par des humains qui peuvent intervenir ou donner l'autorisation d'effectuer certaines actions. Cette autonomie est appelée « l'humain sur la boucle ». Les voitures autonomes, p. ex., sont encore supervisées par un humain qui peut rediriger la voiture[158].
- *Human out of the loop* : L'humain est ici en dehors de la boucle décisionnelle. Il est probable qu'à l'avenir les voitures seront totalement autonomes.

A mesure que l'autonomie des agents augmente (et que ceux-ci font moins d'erreurs), les humains seront déplacés de l'intérieur de la boucle, sur la boucle, puis à l'extérieur de celle-ci[159].

Par ailleurs, les agents peuvent être classés dans différentes catégories en fonction de leur degré d'autonomie. Il s'agit des quatre niveaux suivants[160] :

1. Les agents définis par des algorithmes déterministes :

   Les algorithmes déterministes résolvent les problèmes prévus par le concepteur et fournissent des réponses attendues par le concepteur. Ils se comportent ainsi de manière entièrement prévisible. Par exemple, un algorithme conçu pour traduire le code de la route en code informatique empêchera une voiture autonome de franchir une ligne continue sur la route[161].

2. Les agents basés sur l'apprentissage automatique (*machine learning*) :

   Les algorithmes plus avancés sont capables d'apprendre, ce qui signifie qu'ils améliorent leur comportement par l'expérience (et non en suivant un programme prédéfini). L'apprentissage automatique permet aux algorithmes de détecter les problèmes et les solutions que leurs programmeurs n'avaient pas prévus[162]. Par exemple, une voiture autonome pourrait apprendre, à partir de scénarios modèles ou en observant les autres usagers de la route, qu'elle peut ignorer la règle de

155 Voir à ce sujet NEVEJANS, *Règles européennes de droit civil en robotique*, p. 10.

156 NEVEJANS, *Règles européennes de droit civil en robotique*, p. 10.

157 NOTHWANG et al., *The Human Should be Part of the Control Loop ?*, ch. II let. A.

158 VON UNGERN-STERNBERG, *Artificial Agents*, p. 4.

159 NOTHWANG et al., *The Human Should be Part of the Control Loop ?*, ch. V let. E.

160 Notre classement est inspiré des travaux de HILDEBRANDT, *Smart Technologies and the End(s) of Law*, p. 23 ss, et de VON UNGERN-STERNBERG, *Artificial Agents*, p. 4 ss.

161 VON UNGERN-STERNBERG, *Artificial Agents*, p. 4.

162 VON UNGERN-STERNBERG, *Artificial Agents*, p. 4.

ne pas franchir la ligne continue dans des cas exceptionnels, permettant à la voiture, lorsqu'elle détecte des débris sur la route, de contourner l'obstacle au lieu d'immobiliser le trafic[163]. L'apprentissage automatique s'accompagne de différents degrés d'autonomie. Il est dit *supervisé* lorsque l'algorithme est entraîné sur des données d'apprentissage fournies par le superviseur humain, qui contiennent à la fois les données et les résultats attendus de manière à permettre son fonctionnement autonome sur des jeux de données pour lesquels les résultats sont inconnus, dans un processus de généralisation[164]. L'apprentissage est dit *non supervisé* lorsqu'on ne fournit pas au système de modèle connu *a priori*[165]. Ce type d'algorithme est capable de produire des solutions inattendues, des modèles radicalement neufs, imperceptibles à l'œil humain[166].

3. Les agents basés sur des systèmes multi-agents :

   Il s'agit d'un ensemble d'agents de niveau 1 ou 2 en interaction, qui exécutent leurs propres programmes et négocient entre eux pour atteindre leurs propres objectifs. Pour reprendre l'exemple des véhicules autonomes, ils communiqueront avec l'infrastructure routière, mais aussi avec les autres usagers de la route[167]. Dans ce contexte, il s'agira de déterminer quel agent n'a pas accompli correctement sa tâche, étant relevé qu'aucun agent du système multi-agent n'a une vue de l'ensemble de l'environnement[168].

4. Les agents complets :

   Il s'agit du degré d'intelligence le plus complet[169]. Il s'agit d'agents artificiels ou biologiques capables de survivre en dehors des systèmes informatiques, même s'ils sont constitués comme des systèmes informatiques[170]. Un robot pourrait devenir un agent complet dans le futur, ce qui n'est pas le cas des robots actuels[171].

En résumé, les agents 2, 3 et 4 décrits ci-dessus sont autonomes et imprévisibles. Cette autonomie de l'IA doit être distinguée de

---

163 VON UNGERN-STERNBERG, *Artificial Agents*, p. 4.

164 ROUVROY, *La robotisation de la vie*, emplacement Kindle 484. VON UNGERN-STERNBERG, *Artificial Agents*, p. 5, mentionne comme exemple la spécification de ce qui serait un comportement légal ou illégal des usagers de la route. Voir aussi ACKERMANN, *Artificial Intelligence*, p. 477-478.

165 ROUVROY, *idem*. VON UNGERN-STERNBERG, *Artificial Agents*, p. 5, cite l'exemple d'une voiture autonome qui imiterait le comportement des autres usagers de la route. Voir aussi ACKERMANN, *Artificial Intelligence*, p. 478-479.

166 HILDEBRANDT, *Smart Technologies and the End(s) of Law*, p. 24.

167 VON UNGERN-STERNBERG, *Artificial Agents*, p. 5.

168 HILDEBRANDT, *Smart Technologies and the End(s) of Law*, p. 26.

169 HILDEBRANDT, *Smart Technologies and the End(s) of Law*, p. 27.

170 HILDEBRANDT, *Smart Technologies and the End(s) of Law*, p. 27.

171 HILDEBRANDT, *Smart Technologies and the End(s) of Law*, p. 27-30.

l'automatisation. En effet, contrairement à l'automatisation, le système d'IA est capable de modifier ses états internes ou ses propriétés sans stimuli externes, exerçant un contrôle sur ses actions sans aucune intervention humaine directe[172].

3. *Réflexions concernant le droit actuel et le droit désirable*

a) La responsabilité de l'utilisateur ou du propriétaire de l'IA

La plupart des analyses concernant la responsabilité pour l'utilisation de systèmes intelligents se concentrent sur les utilisateurs humains ou les entités juridiques au nom desquelles ces systèmes sont exploités, en adoptant la fiction juridique selon laquelle tout ce qui découle de ces systèmes est considéré comme émanant des personnes physiques ou morales qui les utilisent[173]. Le Guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur le commerce électronique illustre bien ce principe, en précisant que « les messages de données qui sont créés automatiquement par des ordinateurs, sans intervention humaine directe, devraient être considérés comme « émanant » de la personne morale au nom de laquelle l'ordinateur est utilisé »[174]. La situation est identique pour les robots : ils sont considérés comme des outils ou des moyens d'interaction humaine, ce qui signifie que des règles strictes de responsabilité s'appliquent à l'homme en tant qu'utilisateur de la machine[175].

Une telle solution, qui consiste à placer l'entière responsabilité sur les épaules de l'utilisateur, ne soulève que peu ou pas de difficulté lorsqu'elle s'applique à des systèmes qui ne disposent d'aucune autonome ou d'une autonomie restreinte[176]. En raison de l'autonomie et de l'imprévisibilité de certains agents, il est nécessaire de réfléchir à leur statut juridique, car ces outils ne peuvent pas être comparés à des téléphones ou des fax. S'il est aisé de tenir pour responsable un avocat qui aurait mal utilisé une base de données pour effectuer des recherches juridiques ou aurait adressé un courriel confidentiel à la mauvaise personne, les agents intelligents fonctionnent différemment : les résultats obtenus par ces systèmes ne dépendent pas uniquement des instructions fournies et leur prévisibilité est incertaine. Or la prévisibilité est un facteur clé pour déterminer la responsabilité d'une personne[177]. Dans le cas des agents intelligents, l'utilisateur ne sait pas

172 Voir p. ex. FLORIDI/SANDERS, *On the Morality of Artificial Agents*.

173 DAHIYAT, *Intelligent Agents and Liability*, p. 105.

174 NATIONS UNIES, *Loi type de la CNUDCI*, N 35, p. 29.

175 PAGALLO, *The Laws of Robots*, p. 95.

176 Dans ce sens : DAHIYAT, *Intelligent Agents and Liability*, p. 105.

177 Dans ce sens : DAHIYAT, *Intelligent Agents and Liability*, p. 113.

vraiment comment ils fonctionnent, dans la mesure où le code n'est en général pas accessible et probablement trop complexe pour être étudié. De plus, les agents peuvent apprendre d'eux-mêmes, de telle sorte qu'il est extrêmement difficile pour l'utilisateur de prédire les résultats.

Est-ce qu'il serait dès lors justifié, en raison de son autonomie et de son imprévisibilité, de reconnaître à l'IA une forme de personnalité avec une responsabilité propre ? En d'autres termes, devrait-on créer une personne électronique ?

b) La question de la création d'une personne électronique

Ugo PAGALLO estime que certains robots devraient être considérés comme des agents indépendants plutôt que comme des outils d'interaction humaine[178]. Des règles strictes en matière de responsabilité augmentent le risque que les gens réfléchissent à deux fois avant d'utiliser des robots. D'après cet auteur, pour éviter toute législation empêchant l'utilisation de robots en raison de charges excessives pour les propriétaires de ces machines (plutôt que pour les producteurs et les concepteurs), l'idée que, parfois, seuls « les robots doivent payer » pourrait être la bonne réponse[179]. La Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique va dans ce sens. Elle prévoit notamment ce qui suit[180] :

> *« considérant que, plus un robot est autonome, moins il peut être considéré comme un simple outil contrôlé par d'autres acteurs (tels que le fabricant, l'opérateur, le propriétaire, l'utilisateur, etc.) ; qu'à cet égard se pose la question de savoir si les règles ordinaires en matière de responsabilité sont suffisantes ou si des principes et règles nouveaux s'imposent pour clarifier la responsabilité juridique des divers acteurs en matière de responsabilité pour les actes ou l'inaction d'un robot dont la cause ne peut être attribuée à un acteur humain en particulier, et pour déterminer si les actes ou l'inaction du robot qui ont causé des dommages auraient pu être évités ».*

Nathalie NEVEJANS est très critique concernant ces recommandations. Voici ces propos à ce sujet[181] :

> *« Il nous semble inopportun et malvenu, non seulement de reconnaître l'existence d'une personne électronique, mais également d'établir une quelconque personnalité juridique. Le danger n'est alors pas seulement d'accorder des droits et des obligations à un simple outil, mais aussi de*

178 PAGALLO, *The Laws of Robots*, p. 95.

179 PAGALLO, *The Laws of Robots*, p. 103.

180 PARLEMENT EUROPEEN, *Résolution 2015/2103(INL)*, let. AB.

181 NEVEJANS, *Règles européennes de droit civil en robotique*, p. 18.

> *faire éclater les frontières entre l'homme et la machine, ouvrant ainsi la voie à une confusion entre le vivant et l'inerte, entre l'humain et l'inhumain… De plus, faire émerger une nouvelle sorte de personne – la personne électronique – est un message fort qui pourrait non seulement réanimer avec force la peur de la créature, mais également remettre en cause les fondements humanistes de l'Europe. Accorder le statut de personne à une entité non vivante et non consciente serait donc une erreur, puisque cette solution risquerait à terme de ravaler l'Homme au rang de simple machine ».*

Cette analyse rejoint celle de Bernard HAWADIER, qui estime que « l'homme doit rester responsable de ce qu'il fait, de ce qu'il crée, de ce qu'il construit, même lorsqu'il crée ou construit une machine, si perfectionnée soit-elle, et dotée d'un certain degré d'autonomie »[182]. Le fait que l'agent intelligent opère de manière autonome et pas automatiquement ne devrait pas être utilisé comme une excuse pour exonérer les humains de toute responsabilité[183].

D'autre part, quand bien même l'agent apprend de ses expériences ou de son environnement, ses décisions ne sont pas vraiment volontaires[184]. Si une voiture autonome emboutit un bus au lieu d'écraser un piéton, est-ce que le système avait le choix ? Dans ce contexte, il convient de rappeler que la faute comprend de façon distincte un aspect objectif et subjectif[185]. Pour qu'un comportement objectivement fautif puisse être imputé à son auteur, il faut que ce dernier soit capable de discernement (art. 16 CC), ce qui suppose que la personne ait les facultés de comprendre les conséquences dommageables de son acte et d'agir conformément à cette compréhension[186]. Le concept de faute est dès lors *intimement lié à l'activité humaine* et l'autonomie de l'IA ne peut se confondre avec celle de l'homme[187]. Certes, l'IA a la capacité de prendre des décisions et de les mettre en pratique dans le monde extérieur, indépendamment de tout contrôle ou influence extérieurs ; cette autonomie est cependant de nature purement technique[188]. L'IA n'est pas dotée d'une conscience[189]. Le concept du bien ou du mal n'a pas de sens pour elle. La situation est problématique sous l'angle du droit pénal également : l'IA n'a ni

182 HAWADIER, *L'avocat*, emplacement Kindle 2339-2348.

183 DAHIYAT, *Intelligent Agents and Liability*, p. 112.

184 Dans ce sens : DAHIYAT, *Intelligent Agents and Liability*, p. 108.

185 WERRO, *La responsabilité civile*, N 290 et les réf. cit.

186 WERRO, *La responsabilité civile*, N 305 et les réf. cit.

187 Dans ce sens : JACQUEMIN/HUBIN, *Aspects contractuels*, emplacement Kindle 2716.

188 PARLEMENT EUROPEEN, *Résolution 2015/2103(INL)*, let. AA.

189 Voir toutefois KOOPS et al., *Bridging the Accountability Gap*, p. 559, qui relèvent ce qui suit : « the empirical finding that novel types of entities develop some kind of self-consciousness and become capable of intentional actions seems reasonable, as long as we keep in mind that the emergence of such entities will probably require us to rethink notions of consciousness and moral agency ».

conscience ni volonté[190]. Certains auteurs suggèrent par ailleurs d'enregistrer les robots comme des entreprises[191]. Il faut cependant garder à l'esprit que les personnes morales sont en mesure d'agir que parce qu'un être humain se dessine en filigrane derrière chacune d'entre elles et les représente[192]. C'est donc bien l'homme, doté d'une conscience, qui anime la personne morale. Le concept de la personne morale est ainsi difficilement transposable à l'IA et à son autonomie. Enfin, en admettant qu'une personne électronique soit créée, la question de savoir qui alimenterait le patrimoine de cette nouvelle entité se poserait, dans la mesure où la fonction de la responsabilité civile est de compenser le préjudice subi par le lésé pour le remettre dans la situation qui aurait été la sienne s'il n'avait pas subi une atteinte illicite[193].

En suisse, dans sa réponse du 1er juillet 2015 à l'interpellation intitulée « Nouvelles technologies et appareils autonomes. Cadre légal pour la responsabilité », le Conseil fédéral a estimé que la législation actuelle était suffisante, en relevant qu'un appareil ne peut pas être tenu pour responsable d'un dommage ; seule une personne physique ou morale peut l'être[194]. Le 1er mars 2017, le postulat intitulé « Evaluer la pertinence de créer une personnalité juridique pour les robots » a chargé le Conseil fédéral d'analyser le statut juridique des robots en droit suisse en évaluant, notamment, la pertinence de la création d'une personnalité juridique propre[195]. Le Conseil fédéral a proposé le 26 avril 2017 de rejeter le postulat, en précisant que ceux qui profitent de la nouvelle technologie doivent en supporter les risques, alors que la création d'une personnalité juridique pour les robots aboutirait à l'exact contraire : elle aurait pour conséquence une responsabilité personnelle du robot, c'est-à-dire que son propriétaire ou son possesseur ne serait plus responsable.

A notre avis, l'autonomie et l'imprévisibilité de l'IA ne justifient pas, à elles seules, la création d'une personne électronique. Pour s'en convaincre, il suffit de relever que l'IA est sans doute moins intelligente à l'heure actuelle qu'un insecte, alors que ce dernier pourrait déjà être considéré comme un agent complet[196]. Pourtant, malgré son imprévisibilité, son autonomie, et peut-être même sa dangerosité, il n'a jamais été question d'attribuer la personnalité

---

190 Voir cependant TURNER, *Robot Rules*, p. 204, qui indique que si l'IA devait développer la capacité de désobéir délibérément à des instructions humaines claires, cela pourrait également être considéré comme criminel.

191 PAGALLO, *The Laws of Robots*, p. 104 et les réf. cit.

192 NEVEJANS, *Règles européennes de droit civil en robotique*, p. 17.

193 WERRO, *La responsabilité civile*, N 6 et les réf. cit.

194 Interpellation déposée au Conseil national par le groupe libéral-radical, le 6 mai 2015, N 15.3446.

195 Postulat déposé au Conseil national par Mathias Reynard, le groupe socialiste et le parti socialiste suisse, le 1er mars 2017, N 17.3040.

196 HILDEBRANDT, *Smart Technologies and the End(s) of Law*, p. 30. Voir aussi, *supra*, p. 75.

juridique à un insecte. A notre sens, l'IA doit plutôt être comprise comme une compétence qui devrait être réglementée au niveau éthique et déontologique.

c) Les conséquences pour les avocats

Il est peu probable, dans un avenir proche, que les avocats puissent invoquer l'erreur d'une personne électronique, aussi intelligente et autonome soit-elle, pour se soustraire à leur responsabilité. On peut même penser que les avocats risquent de devoir assumer seul les conséquences du disfonctionnement de l'IA. D'une part, la responsabilité du producteur du système d'IA au sens de la Loi fédérale sur la responsabilité du fait des produits (LRFP ; RS 221.112.944) doit être écartée, car le produit défectueux utilisé par l'avocat – contrairement à celui utilisé par un médecin – ne causera en principe jamais la mort d'une personne, des lésions corporelles ou un dommage à une chose, comme l'exige l'art. 1 LRFP. D'autre part, il est probable que les entreprises qui fourniront ces systèmes d'IA seront localisées à l'étranger et s'exonéreront de toute responsabilité pour les conséquences liées à l'utilisation de leurs outils[197]. Comme le relève Milan MARKOVIC, l'incertitude quant à la responsabilité peut freiner l'adoption de l'intelligence artificielle dans le domaine du droit, mais elle peut aussi mener à un régime où l'avocat demeure le pivot de la représentation juridique, avec la responsabilité ultime des services fournis, bien que la plupart du travail courant soit effectué par des machines intelligentes[198].

Dans ce contexte, il ne faut pas perdre de vue que les attentes à l'égard d'un professionnel comme un avocat doivent être plus élevées qu'à l'égard d'un client qui utiliserait le *chatbot* d'une assurance de protection juridique pour répondre à ses questions juridiques ou de l'utilisateur d'un véhicule autonome qui aurait été instruit d'appuyer sur un bouton rouge en cas de danger. L'avocat est tenu d'exercer sa profession avec soin et diligence (art. 12 let. a LLCA). Ses règles professionnelles lui imposent d'exercer son activité en toute indépendance, en son nom personnel et sous sa propre responsabilité (art. 12 let. b LLCA). D'après le Tribunal fédéral, on doit pouvoir attendre d'un avocat une diligence particulière en relation avec ses connaissances spécifiques et compter, notamment, qu'il conseille et oriente son client quant aux possibilités juridiques ou pratiques qui se présentent à lui dans certaines situations[199]. Un avocat qui utilise l'IA devra exercer un jugement raisonné pour évaluer l'exactitude des faits allégués, ainsi que la pertinence de la

---

197 Comme le relèvent Jean-Pierre BUYLE et Adrien VAN DEN BRANDEN, il est fréquent en pratique pour les fournisseurs de logiciels de préciser que leurs produits sont fournis comme tel (« as is »), sans garantie quant aux éventuelles erreurs de programmation ou de conception ou sans garantie que leur utilisation soit conforme aux besoins ou attentes des utilisateurs (*La robotisation de la justice*, note de bas de page 125).

198 MARKOVIC, *Rise of the Robot Lawyers?*, p. 343.

199 ATF 117 II 563, consid. 2a.

technologie choisie pour résoudre le litige. Ce jugement raisonné est quelque chose que l'IA – que cela soit par le traitement automatique du langage naturel ou l'apprentissage automatique – n'est pas encore en mesure de faire[200]. Contrairement à la machine, qui est capable de traiter une grande quantité d'information en un temps record, l'avocat possède un instinct ; il est capable de douter et – surtout – de faire douter. Il peut expliquer son raisonnement à son client[201]. En outre, l'avocat ne doit pas se déresponsabiliser, raison pour laquelle la loi exige de lui qu'il exerce son activité sous sa propre responsabilité.

Comme nous l'avons vu, l'avocat travaillera dans un premier temps en collaboration avec l'IA[202], ce qui posera des questions concernant sa capacité à rester indépendant[203]. La situation est également délicate, sous l'angle des règles professionnelles, lorsque la machine supplantera entièrement l'activité de l'avocat. Est-ce qu'un avocat qui s'appuierait entièrement sur l'IA pour réviser des documents contractuels, qui seraient ensuite remis à son client sans aucune vérification de sa part, respecterait ses règles professionnelles ? Que penser d'un avocat qui mettrait en place un *chatbot* pour répondre aux questions juridiques de ses clients de manière autonome et sans supervision de sa part ? Dans ces exemples, l'avocat exercerait-il toujours son activité avec soin et diligence au sens de l'art. 12 let. a LLCA ?

Il est important, dans un premier temps, de garder à l'esprit que répondre négativement à ces questions aurait pour conséquence d'entraver la liberté économique de l'avocat de manière conséquente (art. 27 Cst.). En effet, en Suisse, les prestataires de services juridiques non réglementés, comme les banques, les fiduciaires ou les assurances de protection juridique, pourront utiliser ces systèmes sans aucune limite[204]. Il est même permis de penser qu'ils s'appuieront massivement sur l'IA à l'avenir pour fournir leurs services.

En y réfléchissant bien, il serait paradoxal d'imposer à l'avocat l'utilisation des nouvelles technologies, y compris l'IA, dans le cadre de son devoir de diligence[205] et, d'un autre côté, de lui reprocher de violer ce même devoir de diligence lorsqu'il utilise pleinement le potentiel de ces outils. Nous sommes ici confrontés à une nouvelle problématique : l'IA peut effectuer le travail seul et sans aucune supervision humaine, alors que les outils que l'avocat utilise depuis longtemps, comme un correcteur de textes ou une base de données, ne possèdent aucune autonomie.

---

200 Dans ce sens : ALARIE et al., *How Artificial Intelligence Will Affect the Practice of Law*, p. 12.

201 MARKOVIC, *Rise of the Robot Lawyers?*, p. 347-348, qui relève très justement que l'avocat peut être jugé non seulement sur le résultat obtenu, mais aussi sur le raisonnement qui l'a conduit à ce résultat.

202 Voir *supra*, p. 70 ss.

203 Voir *infra*, p. 83 ss.

204 Voir p. ex. le projet pilote de l'assurance de protection juridique Coop, *supra*, p. 69.

205 Voir *supra*, p. 71 ss.

Nous pensons que les réponses à ces questions doivent être tranchées au cas par cas. Certaines activités qui exigent de la créativité, de l'empathie, la capacité de « lire entre les lignes » ne devraient pas être déléguées entièrement à l'IA par l'avocat. De notre point de vue, la décision de recourir ou d'agir en justice ne devrait pas s'appuyer intégralement sur la décision d'un algorithme[206]. Il ne serait en revanche pas problématique, à notre avis, qu'un avocat développe et entraîne un robot ou agent conversationnel pour répondre aux questions juridiques de ses clients, si l'algorithme est capable de déterminer à quel moment il est nécessaire d'inviter le client à prendre contact avec l'avocat. De plus, dans le cadre de son obligation d'exercer sa profession avec soin et diligence, l'avocat devra être totalement transparent avec son client, en l'informant pour quelles activités et dans quelles mesures il s'appuiera sur l'IA pour exécuter son mandat[207]. Si le client est d'accord avec cette manière de procéder et que l'activité peut être déléguée à l'IA, l'avocat ne devrait pas violer son obligation d'exercer sa profession avec soin et diligence. Cependant, s'il s'avère que le travail n'a pas été fait correctement par l'IA et que le client a subi un dommage résultant de l'activité d'une machine, l'avocat engagera sa responsabilité civile et disciplinaire. Concernant la responsabilité civile, nous suggérons d'appliquer les art. 55 et 101 CO.

d) Application par analogie des art. 55 et 101 CO

En attendant l'avènement d'une personnalité électronique et d'une responsabilité du fait de l'IA, nous suggérons que l'IA soit considérée, par analogie, comme un auxiliaire de l'avocat au sens des art. 55 CO (responsabilité de l'employeur) ou 101 CO (responsabilité pour des auxiliaires), au même titre qu'une secrétaire ou un stagiaire[208]. A notre avis, il est justifié de considérer que celui qui tire profit de l'IA doit aussi répondre de ses manquements. Cette solution – contrairement à la responsabilité du fait de l'IA – a l'avantage de ne pas déresponsabiliser l'avocat face à la machine. Un autre avantage du régime des art. 55 et 101 CO réside dans le fait qu'une faute subjective de l'auxiliaire n'est pas nécessaire, l'employeur pouvant engager sa responsabilité même si l'auxiliaire est incapable de discernement[209]. La question concernant la possibilité d'imputer une faute subjective à l'IA pourrait ainsi souffrir de demeurer indécise. En tant que partenaire contractuel de l'avocat, le client pourra se prévaloir de l'art. 101 CO, alors que l'application de l'art. 55 CO – qui nécessiterait que l'IA cause un dommage à un tiers –

206 Dans ce sens également : LEMKE, *L'avenir des services juridiques – Conclusion*.

207 Nous avions suggéré une obligation similaire pour les pratiques multidisciplinaires dans les sociétés d'avocats lorsqu'un service est fourni par un tiers qui n'est pas un avocat inscrit au registre, voir GURTNER, *La réglementation des sociétés d'avocats*, p. 402-403.

208 Voir aussi BLESKIE, *Künstliche Intelligenz*, p. 22 ss. Concernant la responsabilité de l'avocat employant un stagiaire, voir p. ex. ATF 117 II 563 consid. 3a.

209 Voir WERRO, *La responsabilité civile*, N 514 et les réf. cit.

restera plutôt anecdotique. L'avocat sera donc jugé sur la diligence qu'il aurait dû observer s'il avait lui-même exécuté l'obligation[210] – ce qui est conforme à ses obligations professionnelles.

F. Les « boîtes noires » et l'indépendance des avocats

1. L'opacité des algorithmes

La plupart des gens ont une vision beaucoup trop angélique des algorithmes utilisés dans de nombreux domaines, comme la justice, l'éducation, l'accès à l'emploi ou au crédit. Dans son ouvrage « *Weapons of Math Destruction* », Cathy O'NEIL, mathématicienne et *data scientist*, met en garde contre l'utilisation massive et excessive des systèmes prédictifs dans nos sociétés[211]. Elle mentionne plusieurs exemples. Un programme de prédiction du crime développé par la société PredPol traite les anciennes données sur la criminalité et calcule, heure par heure, les endroits où les crimes sont susceptibles de se produire[212]. Comme le relève l'auteur, dans des villes largement ségréguées comme aux États-Unis, même si PredPol prétend ne pas utiliser de critères démographique, ethnique ou socio-économique, le modèle envoie souvent la police dans les quartiers les plus défavorisés où la plupart des habitants sont afro-américains ou hispaniques. Ces derniers seront plus souvent arrêtés pour des petites infractions que dans d'autres quartiers plus riches, créant ainsi un cercle vicieux, alors que d'importants crimes liés à la finance échapperont aux radars. Par ailleurs, plusieurs États utilisent un modèle appelé « LSI-R », ou « *Level of Service Inventory-Revised* » pour évaluer le risque de récidive. Si le questionnaire ne pose pas de questions sur l'appartenance raciale ou ethnique, il tient en revanche compte du casier judiciaire des amis ou des proches des prisonniers[213]. En d'autres termes, une personne que le modèle classera comme étant à haut risque est susceptible d'être sans emploi et de venir d'un quartier où beaucoup de ses amis et de sa famille ont déjà eu des démêlés avec la justice[214]. Ainsi, le modèle lui-même alimente le cercle vicieux et le soutient. C'est ce que Cathy O'NEIL appelle un « WMD », pour « *Weapons of Math Destruction* ».

Dans l'État du Wisconsin, en condamnant un américain, Éric LOOMIS, à six ans de prison pour avoir fui la police dans une voiture volée, un tribunal du Wisconsin s'est en partie appuyé sur un haut risque de récidive calculé par le

210 WERRO, *La responsabilité civile*, N 554.

211 O'NEIL, *Weapons of Math Destruction*.

212 PredPol, disponible sur : http://www.predpol.com/ (consulté le 22.07.2019).

213 O'NEIL, *Weapons of Math Destruction*, p. 26.

214 O'NEIL, *Weapons of Math Destruction*, p. 27.

logiciel Compas[215]. Pourtant, personne ne sait exactement comment fonctionne ce logiciel ; son concepteur refuse de dévoiler l'algorithme propriétaire utilisé par le système. On connaît uniquement le résultat final de l'évaluation des risques que les juges peuvent prendre en considération, parmi d'autres facteurs, pour déterminer la peine. Éric LOOMIS a contesté l'utilisation de l'algorithme devant la Cour suprême du Wisconsin[216] et la Cour suprême des États-Unis[217], en invoquant une violation de son droit à un procès équitable, sans succès[218].

Comme l'explique Cathy O'NEIL, pour créer un modèle, nous faisons des choix sur ce qui est assez important à inclure, en simplifiant le monde dans une version « jouet » qui peut être facilement comprise et à partir de laquelle nous pouvons déduire des faits importants et des actions[219]. Aucun modèle ne peut toutefois inclure toute la complexité du monde ou la nuance de la communication humaine[220]. Les modèles vont refléter des buts et une idéologie. Ils ne sont rien d'autre que des opinions intégrées aux mathématiques[221]. Il faut donc se poser la question suivante : a-t-on éliminé les biais humains ou les a-t-on simplement camouflés avec la technologie[222] ?

L'opacité peut découler d'une volonté intentionnelle de dissimuler un secret (p. ex. pour préserver un avantage concurrentiel ou pour des raisons de sécurité nationale), des compétences particulières requises pour lire un code, ou de l'utilisation d'algorithmes basés sur l'apprentissage automatique[223].

Dans sa résolution du 16 février 2017, le Parlement européen considère que « l'apprentissage automatique offre d'importants avantages à la société en termes d'économie et d'innovation en améliorant considérablement la capacité à analyser les données, mais qu'il pose également des défis pour ce qui est de garantir l'absence de discriminations, un traitement équitable, la transparence et l'intelligibilité des processus décisionnels »[224].

Avec des algorithmes basés sur l'apprentissage automatique, difficilement interprétables et prévisibles, il peut être impossible (ou très difficile) de déterminer si une décision problématique particulière est simplement un

215 ISRANI, *When an Algorithm Helps Send You to Prison*.

216 State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

217 THE Supreme Court of the United States, Eric L. Loomis v. Wisconsin, No 16-6387, disponible sur : https://www.supremecourt.gov/docketfiles/16-6387.htm [https://perma.cc/V6VK-XDAN].

218 Pour plus de détails sur cette affaire et la portée judiciaire du résultat de l'algorithme prédictif aux États-Unis, voir DEFFERRARD/PAPINEAU, *Le pouvoir de jurisdictio des algorithmes*, p. 142-143.

219 O'NEIL, *Weapons of Math Destruction*, p. 20.

220 O'NEIL, *Weapons of Math Destruction*, p. 20.

221 O'NEIL, *Weapons of Math Destruction*, p. 21.

222 O'NEIL, *Weapons of Math Destruction*, p. 25.

223 BURRELL, *How the Machine "Thinks"*.

224 PARLEMENT EUROPEEN, *Résolution 2015/2103(INL)*, let. H.

« bug », la preuve d'un échec systématique ou d'un biais[225]. En réalité, il ne s'agit pas seulement de lire et de comprendre le code, mais aussi de pouvoir comprendre l'algorithme en action, fonctionnant sur des données[226]. Voici les explications de Jenna BURREL à ce sujet[227] :

> *« In a "Big Data" era, billions or trillions of data examples and thousands or tens of thousands of properties of the data (termed "features" in machine learning) may be analyzed. The internal decision logic of the algorithm is altered as it "learns" on training data. Handling a huge number especially of heterogeneous properties of data (i.e. not just words in spam email, but also email header info) adds complexity to the code. Machine learning techniques quickly face computational resource limits as they scale and may manage this, using techniques written into the code (such as "principal component analysis") which add to its opacity. While datasets may be extremely large but possible to comprehend and code may be written with clarity, the interplay between the two in the mechanism of the algorithm is what yields the complexity (and thus opacity) ».*

La raison d'être de l'algorithme est obscurcie, ce qui contribue à représenter les algorithmes basés sur l'apprentissage automatique comme des « boîtes noires »[228]. On sait ce qui entre d'un côté, on constate ce qui sort de l'autre, mais on ne sait pas ce qui se passe entre les deux. D'autre part, plus les algorithmes basés sur l'apprentissage automatique deviennent complexes, plus leur résultat peut initialement apparaître comme magique[229].

Il faut également garder à l'esprit que le traitement algorithmique contraste avec la prise de décision traditionnelle, où les humains peuvent en principe articuler leur raisonnement lorsqu'ils sont interrogés, limités uniquement par leur désir et leur capacité à donner des explications, et la capacité de l'auteur de la question à les comprendre[230]. La raison d'être d'un algorithme peut en revanche être incompréhensible pour l'homme, rendant la légitimité des décisions difficile à contester[231].

En résumé, on commet une erreur en pensant que la prise de décision d'une machine est neutre[232].

---

225 MITTELSTADT et al., *The Ethics of Algorithms,* p. 2.

226 BURRELL, *How the Machine "Thinks"*, p. 5.

227 BURRELL, *How the Machine "Thinks"*, p. 5.

228 MITTELSTADT et al., *The Ethics of Algorithms,* p. 6.

229 ACKERMANN, *Artificial Intelligence*, p. 481.

230 Dans ce sens : MITTELSTADT et al., *The Ethics of Algorithms,* p. 7.

231 MITTELSTADT et al., *The Ethics of Algorithms,* p. 7.

232 Dans ce sens : GANASCIA, *Devons-nous craindre l'intelligence artificielle ?*, p. 78.

2. *La tentative de rendre les algorithmes transparents*

L'art. 22 par. 1 RGPD précise que la personne concernée a le droit de ne pas faire l'objet d'une décision fondée *exclusivement* sur un traitement automatisé, y compris le profilage, *produisant des effets juridiques* la concernant ou *l'affectant de manière significative de façon similaire*.

Ce droit découle de la volonté qu'à l'être humain de ne pas être intégralement soumis à la machine et à ses décisions[233]. Comme l'indique Cécile de TERWANGNE, « c'est là l'expression de la prééminence à accorder à la dignité humaine »[234].

Déterminer quand une décision est *exclusivement* fondée sur un traitement automatisé est sujet à discussion. Que penser p. ex. d'une décision issue d'un traitement automatisé qui ne serait pas activement évaluée par un être humain, mais qui lui serait formellement attribuée ? D'après les lignes directrices adoptées par le Groupe de travail « Article 29 », une décision est fondée exclusivement sur un traitement automatisé lorsqu'il n'y a pas d'intervention humaine dans le processus de décision[235]. Elles ajoutent notamment ce qui suit :

> *« Pour qu'il y ait intervention humaine, le responsable du traitement doit s'assurer que tout contrôle de la décision est significatif et ne constitue pas qu'un simple geste symbolique. Le contrôle devrait être effectué par une personne qui a l'autorité et la compétence pour modifier la décision. Dans le cadre de l'analyse, il convient de tenir compte de toutes les données pertinentes.*
> *Dans le cadre de son analyse d'impact relative à la protection des données, le responsable du traitement devrait identifier et consigner le degré d'intervention humaine dans le processus de prise de décision et le stade auquel cela se produit ».*

Ainsi, cocher une case sur un formulaire ne sera pas suffisant[236]. Dimitra KAMARINOU et al. mentionnent par ailleurs l'exemple suivant[237] :

> *« […] [I]n a medical context, a diagnostics machine might conclude that there is a 90 per cent probability that a data subject has a particular type of tumor and that taking a specific drug or starting chemotherapy may be time sensitive. Even if one or more humans are involved in the design, training and testing of this system, if the machine is tasked with deciding a treatment plan without a human decision maker critically evaluating the diagnostic assessment, this decision will be subject to Article 22, even*

233 DE TERWANGNE, *La réforme de la Convention 108*, p. 104.

234 *Idem*.

235 GROUPE DE TRAVAIL « ARTICLE 29 », *Lignes directrices*, p. 23.

236 KAMARINOU et al., *Machine Learning with Personal Data*, p. 98.

237 KAMARINOU et al., *Machine Learning with Personal Data*, p. 98.

if such a decision was merely an interim preparatory measure before a final decision on an operation, for example, was made ».

A titre d'exemple, le considérant n° 71 du RGPD, qui n'est pas contraignant et sert à interpréter le texte, mentionne le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine comme étant des traitements affectant de manière significative la personne.

Il existe trois exceptions au droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (art. 22 par. 2 RGPD) : lorsque la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement (point a) ; lorsqu'elle est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée (point b) ; ou lorsqu'elle est fondée sur le consentement explicite de la personne concernée (point c).

Le RGPD exige que le responsable du traitement fournisse à la personne concernée une information sur « l'existence d'une prise de décision automatisée, y compris un profilage […] et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée » (art. 13 par. 2 point f, 14 par. 2 point g et 15 par. 1 point h du RGPD). Cette information est due à l'origine, mais également en réponse à l'exercice d'un droit d'accès (art. 15 RGPD). D'autre part, dans les cas visés à l'art. 22 par. 2, points a) et c) RGPD, « le responsable du traitement met en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision » (art. 22 par. 3 RGPD). Comme le résume Judith ROCHFELD, les droits minimaux de la personne sont les suivants[238] : « les droits d'être informé en amont, d'accéder à cette information en aval, de faire intervenir une appréciation humaine, d'exprimer son point de vue – sorte de droit de la défense ou du contradictoire – et de contester la décision – droit de recours ».

Le considérant n° 71 du RGPD explique notamment qu'un traitement automatisé devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, *d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation* et

238 ROCHFELD, *L'encadrement des décisions prises par des algorithmes*, p. 14.

de contester la décision. Force est de constater que le considérant précité va plus loin que l'art. 22 par. 3 RGPD[239].

Une controverse doctrinale – essentiellement nourrie par le considérant précité – a vu le jour. Dans une première contribution, Bryce GOODMAN et Seth FLAXMAN ont expliqué que le RGPD impose « un droit à l'explication » des décisions prises par des systèmes automatisés[240]. Dans une seconde contribution, Sandra WACHTER et al. ont répondu qu'un tel droit n'existe pas[241] : d'après eux, le RGPD n'exigerait qu'une explication *ex ante* du fonctionnement du système et pas une explication *ex post* des motifs de la décision, ce qu'ils appellent « un droit à être informé » – par opposition à un droit à une explication *ex post* des motifs d'une décision. Plusieurs auteurs sont d'avis que le raisonnement de WACHTER et al. est erroné. Maja BRKAN estime pour l'essentiel que le considérant n° 71 renforce l'interprétation de l'existence d'un droit à l'explication[242]. Le droit d'obtenir une explication de la décision prise après l'évaluation devrait toujours pouvoir être exercé[243]. Andrew D. SELBST et Julia POWLES considèrent, quant à eux, que le droit à l'explication doit être interprété de manière fonctionnelle et souple, et doit, à tout le moins, permettre à la personne concernée d'exercer ses droits en vertu du RGPD et du droit relatif aux droits de l'homme[244]. C'est cette seconde interprétation des dispositions du RGPD – moins rigide – qu'il convient à notre avis de privilégier.

En résumé, et malgré certaines controverses, il faut retenir que le RGPD règlemente les décisions prises par des algorithmes. Le responsable du traitement des données devra soit mettre un humain dans la boucle décisionnelle pour ne pas tomber sous le coup de l'art. 22 par. 1 RGPD, soit mettre en place des mesures appropriées pour sauvegarder les droits et libertés et les intérêts légitimes des personnes concernées par un traitement automatisé.

Pour être complet, on relèvera qu'en Suisse l'art. 19 du projet de Loi fédérale sur la protection des données introduit « un devoir d'information lors de décisions individuelles automatisées, ainsi que le droit pour la personne concernée, à certaines conditions, de faire valoir son point de vue et d'exiger qu'une personne physique revoie le décision »[245].

---

239 Dans ce sens : DE TERWANGNE/ROSIER, *Le Règlement général sur la protection des données*, p. 534.

240 GOODMAN/FLAXMAN, *European Union Regulations on Algorithmic Decision-Making*, *passim*.

241 WACHTER et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*, *passim*.

242 BRKAN, *Do Algorithms Rule the World ?*, p. 16.

243 MALGIERI/COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists*, p. 255.

244 SELBST/POWLES, *Meaningful Information*, p. 242.

245 FF 2017 6565, p. 6595, p. 6673-6676.

Enfin, certains auteurs suggèrent la création d'une autorité spécifique pour auditer les algorithmes avant ou après qu'ils ont été déployés[246].

3. Les conséquences pour les avocats

Aujourd'hui, la tendance est de « s'en remettre à un « ordinateur » et aux algorithmes qu'il applique pour décider du traitement à réserver à un individu »[247]. En d'autres termes, les décisions « seront de plus en plus souvent motivées « par le fait que l'ordinateur a dit non » (même si les responsables ou le personnel prenant la décision ne peuvent la justifier complètement) »[248].

L'art. 12 let. b LLCA prévoit que l'avocat doit exercer son activité professionnelle en toute indépendance, en son nom personnel et sous sa propre responsabilité. L'avocat doit être indépendant, notamment à l'égard des tiers[249].

Un avocat ne pourra pas prendre une décision exclusivement fondée sur un algorithme[250]. Il devra encore vérifier le résultat des conseils donnés par la machine et étayer la solution juridique qu'il propose. Comme l'avocat sera augmenté, il y aura deux experts : un humain et une machine. Même si l'avocat se voit déléguer le pouvoir décisionnel, il y aura inévitablement des désaccords. La machine estimera que les chances de succès d'un recours seront insuffisantes, alors que l'avocat sera d'un avis contraire (ou l'inverse). L'avocat se trouvera dans une position inconfortable. S'il s'appuie trop facilement et trop souvent sur l'expertise de la machine, il risque de mettre en danger son indépendance (art. 12 let. b LLCA). En effet, les algorithmes d'intelligence artificielle doivent être considérés comme des tiers pouvant influencer les décisions de l'avocat et compromettre son indépendance. Or cette perte d'indépendance est encore accentuée si le système que l'avocat utilise s'appuie sur un algorithme qui ne représente pour lui qu'une « boîte noire »[251]. La machine donnera à l'avocat une réponse qu'il trouvera peut-être pertinente, mais sans lui fournir d'explications rationnelles justifiant cette réponse. Au contraire, s'il fait confiance à son propre instinct et à son expérience, l'avocat devra systématiquement expliquer à son client pourquoi il est judicieux de s'écarter de l'expertise de la machine.

Dans ce contexte, nous pensons que l'avocat devrait s'inspirer des mesures prévues par le RGPD concernant les décisions automatisées. En particulier, il

---

246 WACHTER et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*, p. 98.

247 DE TERWANGNE, *La réforme de la Convention 108*, p. 104.

248 COMMISSION EUROPEENNE, *Étude comparative*, p. 21-22.

249 Voir à ce sujet p. ex. GURTNER, *La réglementation des sociétés d'avocats*, p. 237.

250 Voir *supra*, p. 80 ss.

251 Voir *supra*, p. 83 ss.

devrait être en mesure de comprendre et d'expliquer – à tout le moins dans les grandes lignes – comment l'algorithme qu'il utilise fonctionne. C'est à cette seule condition que l'avocat ne sera pas influencé par une machine qui pourrait lui fournir des résultats biaisés, sans qu'il ne s'en rende compte. Le modèle utilisé par l'avocat va refléter des buts et une idéologie – il n'est rien d'autre que des opinions intégrées aux mathématiques[252]. La société – et les programmeurs qui ont conçu l'algorithme – pourrait intentionnellement (ou même sans le savoir) favoriser certaines solutions. Il n'est pas non plus exclu que le système d'IA soit décentralisé dans un *cloud*, ce qui permettrait à la société qui fournit le système ou à un tiers d'intervenir dans le processus décisionnel pour tenter d'influencer l'avocat. Pour ne pas compromettre leur indépendance, les avocats devront prendre certaines précautions. Comme le suggère Thierry WICKERS, les barreaux pourraient disposer d'un moteur d'IA et le mettre à la disposition de leurs membres, ce qui pourrait constituer un enjeu stratégique pour la profession d'avocat[253]. Au-delà de cet enjeu stratégique, cette solution devrait être envisagée sérieusement, car elle permettrait aux barreaux et aux avocats de rester propriétaires de l'algorithme utilisé. Il serait ainsi beaucoup plus simple d'étudier et d'auditer l'algorithme pour s'assurer qu'il n'est pas compromis ou biaisé.

Enfin, si l'avocat augmenté est capable de mesurer avec précision les chances de succès d'une affaire, on peut se demander ce qu'il adviendra de l'aléa judiciaire. Pourra-t-on encore soutenir que l'avocat est soumis aux règles du contrat de mandat (art. 394 ss CO) ? Le Tribunal fédéral considère que lorsque le résultat qui doit être fourni peut être contrôlé d'après des critères objectifs et qualifié d'exact ou d'inexact, l'exactitude des conclusions de l'expertise peut être garantie et promise en tant que résultat[254]. Il s'agit alors d'un contrat d'entreprise (art. 363 ss CO). Comme l'avocat augmenté pourra plus difficilement invoquer l'aléa judiciaire, nous pensons qu'il n'est pas exclu que les règles du contrat d'entreprise s'appliquent dans certaines situations.

IV. Conclusions

La première partie de cette contribution a été consacrée à la responsabilité des avocats et à la cybersécurité. Il s'agit d'un sujet trop souvent négligé. On insiste beaucoup sur les compétences juridiques des avocats ; personne ne semble en revanche s'inquiéter que des avocats continuent de travailler avec des systèmes d'exploitation désuets qui ne sont plus mis à jour depuis plusieurs années et qui comportent des failles de sécurité importantes, qu'ils

252 Voir *supra*, p. 83 ss.

253 WICKERS, *Conclusion. L'avenir de la profession d'avocat*.

254 ATF 127 III 328, consid. 2c, SJ 2002 I 103.

stockent des informations confidentielles sur Dropbox, qu'ils utilisent des connexions Wi-Fi publiques non sécurisées pour envoyer des courriels avec leur compte Gmail, ou encore qu'ils enregistrent des dossiers de l'étude, sans les chiffrer, sur des clés USB qui peuvent facilement être égarées dans un train ou un taxi, mettant ainsi gravement en danger la sécurité des données de leurs clients. Il est temps de reconnaître à l'avocat le devoir d'être technologiquement compétent, au même titre qu'il doit l'être d'un point de vue juridique. Dans ce contexte, il est dans l'intérêt public qu'une sanction disciplinaire puisse être prononcée sur la base des art. 12 let. a et/ou 13 LLCA en cas de négligence d'un avocat et à titre préventif, sans qu'un secret ne soit nécessairement révélé. Par ailleurs, comme l'exige le RGPD et (probablement) la future loi suisse sur la protection des données, il est justifié que les avocats aient l'obligation d'annoncer les violations de la sécurité des données de leurs clients, lorsqu'elles sont susceptibles d'engendrer une atteinte à leurs droits et libertés. On peut même se demander si une obligation d'annonce en cas d'atteinte à la sécurité des données entraînant une violation du secret professionnel ne devrait pas être déduite des règles professionnelles de l'avocat, en particulier de l'art. 12 let. a LLCA.

La responsabilité des avocats et l'IA a fait l'objet de la seconde partie de cette contribution. Nous sommes confrontés à une nouvelle problématique : l'IA peut effectuer le travail seule et sans aucune supervision humaine, alors que les outils que l'avocat utilise depuis longtemps, comme un correcteur de textes ou une base de données, ne possèdent aucune autonomie. Dans un premier temps, l'avocat sera technologiquement augmenté, ce qui soulèvera de nouvelles questions concernant sa relation avec la machine. Contrairement à l'avis de certains auteurs qui suggèrent la création d'une personne électronique, nous pensons que les évolutions technologiques actuelles ne justifient pas d'abandonner la *summa divisio* issue du droit romain qui distingue les personnes et les choses. L'homme doit rester responsable de ce qu'il fait et de ce qu'il crée. Cela est d'autant plus vrai pour les avocats : la loi exige qu'ils exercent leur activité sous leur propre responsabilité. Les règles professionnelles ne devraient cependant pas bloquer toute évolution dans ce domaine ; il serait ainsi prudent de laisser une certaine marge de manœuvre aux avocats qui souhaitent utiliser l'IA. Enfin, les avocats devront être particulièrement vigilants lors de l'utilisation des algorithmes d'apprentissage automatique, dont l'opacité et les biais sont susceptibles de mettre en danger leur indépendance (art. 12 let. b LLCA).

V. Table des abréviations

ABA	American Bar Association
al.	alinéa(s)
art.	article(s)
ATF	Recueil officiel des arrêts du Tribunal fédéral
BGFA	= LLCA
CC	Code civil suisse, du 10 décembre 1907 (CC ; RS 210)
CCBE	Conseil des barreaux européens
CGA	Conditions générales d'assurance
ch.	chiffre(s)
Cloud Act	Clarifying Lawful Overseas Use of Data Act
CNB	Conseil National des Barreaux
CNUDCI	Commission des Nations Unies pour le droit commercial international
CO	Loi fédérale du 30 mars 1911 complétant le Code civil suisse (Livre cinquième : Droit des obligations) (Code des obligations (= OR, CO ; RS 220)
consid.	considérant
CP	Code pénal suisse du 21 décembre 1937 (CP ; RS 311.0)
CPDP	Computers, Privacy & Data Protection
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst. ; RS 101)
éd.	édition
édit.	éditeur ou éditeurs
et al.	*et alii* (= et autres)
etc.	*et caetera*
EU	= UE
FBI	Federal Bureau of Investigation
FF	Feuille fédérale
IA	Intelligence artificielle
infra	ci-dessous
JdT	Journal des Tribunaux

let.	lettre(s)
LLCA	Loi fédérale du 30 juin 2000 sur la libre circulation des avocats (Loi sur les avocats) (= BGFA, LLCA ; RS 935.61)
LPD	Loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1)
LRFP	Loi fédérale du 18 juin 1993 sur la responsabilité du fait des produits (LRFP ; RS 221.112.944)
No	numéro
OR	= CO
p. ex.	par exemple
p.	page
par.	paragraphe
passim	çà et là, en différents endroits
PFPDT	Préposé fédéral à la protection des données et à la transparence
P-LPD	Projet de Loi fédérale sur la protection des données
RDAF	Revue de droit administratif et de droit fiscal
RGPD	Règlement général européen sur la protection des données
RS	Recueil systématique du droit fédéral
SJ	Semaine judiciaire
ss	et suivant(e)s
SSL	Secure Sockets Layer
supra	ci-dessus
TF	Tribunal fédéral
TLS	Transport Layer Security
UE	Union européenne (= EU)
vol.	volume

VI. Bibliographie

ACKERMANN LUIS, « Artificial Intelligence and Advanced Legal Systems », in Michele DeStefano/Guenther Dobrauz-Saldapenna (édit.), *New Suits : Appetite for* Disruption *in the Legal World*, Berne 2019, p. 475-492 [Ackermann, *Artificial Intelligence*]

ADVISORY COMMITTEE ON PROFESSIONAL ETHICS, New Jersey Ethics Opinion 701, « Electronic Storage and Access of Client Files », le 10 avril 2006 [ADVISORY COMMITTEE ON PROFESSIONAL ETHICS, *New Jersey Ethics Opinion 701*]

ALARIE Benjamin/NIBLETT Anthony/YOON Albert, « How Artificial Intelligence Will Affect the Practice of Law », le 7 novembre 2017, p. 1-15, disponible sur : https://ssrn.com/abstract=3066816 [ALARIE et al., *How Artificial Intelligence Will Affect the Practice of Law*]

ALETRAS Nikolaos/TSARAPATSANIS Dimitrios/PREOȚIUC-PIETRO Daniel/ LAMPOS Vasileios, « Predicting Judicial Decisions of the European Court of Human Rights : a Natural Language Processing perspective », in *PeerJ Computer Science* 2:e93, 2016 [ALETRAS et al., *Predicting judicial decisions*]

AMERICAN BAR ASSOCIATION, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 477, « Securing Communication of Protected Client Information », le 11 mai 2017 [ABA Formal Opinion 477]

AMERICAN BAR ASSOCIATION, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 483, « Lawyers' Obligations After an Electronic Data Breach or Cyberattack », le 17 octobre 2018 [ABA Formal Opinion 483]

BAKERHOSTETLER, « 2019 Data Security Incident Response Report, Managing Enterprise Risks in a Digital World, Privacy, Cybersecurity, and Compliance Collide », disponible sur : https://bakerlaw.com/DSIR [BAKERHOSTETLER, *2019 Data Security Incident*]

BANDLER John, *Cybersecurity for the Home and Office – The Lawyer's Guide to Taking Charge of Your Own Information Security*, format Kindle, American Bar Association 2017 [BANDLER, *Cybersecurity*]

BARTH Tano, « Utilisation des nouvelles technologies : devoir de diligence de l'avocat », in *Jusletter* 3 septembre 2018 [BARTH, *Utilisation des nouvelles technologies*]

BERTHEREAU Jessica, « La justice prédictive – Quand les algorithmes s'attaquent au droit », *L'intelligence artificielle en pratique et en débat*, in *Paris Innovation Review*, 2018, p. 45-52 [BERTHEREAU, *La justice prédictive*]

BLESKIE Nicolai, « Künstliche Intelligenz und haftungsrechtliche Konsequenzen », in *Jusletter* IT du 24 mai 2018 [BLESKIE, *Künstliche Intelligenz*]

BOHNET François/MARTENET Vincent, *Droit de la profession d'avocat*, Berne 2009 [BOHNET/MARTENET, *Droit de la profession d'avocat*]

BONDALLAZ Stéphane, *La protection des personnes et de leurs données dans les télécommunications : analyse critique et plaidoyer pour un système en droit suisse*, Zurich 2007 [BONDALLAZ, *La protection des personnes*]

BOSTROM Nick, *Superintelligence – Paths, Dangers, Strategy*, format Kindle, Oxford (Oxford University Press) 2014 [BOSTROM, *Superintelligence*]

BRKAN Maja, « Do Algorithms Rule the World ? Algorithmic Decision-Making in the Framework of the GDPR and Beyond », 1er août 2017, p. 1-29, disponible sur : https://ssrn.com/abstract=3124901 [BRKAN, *Do Algorithms Rule the World ?*]

BURRELL Jenna, « How the Machine "Thinks" : Understanding Opacity in Machine Learning Algorithms », in *Big Data & Society*, Vol. 3, No 1, 2016, disponible sur : https://doi.org/10.1177%2F2053951715622512 [BURRELL, *How the Machine "Thinks"*]

BUYLE Jean-Pierre/VAN DEN BRANDEN Adrien, « La robotisation de la justice », in Hervé JACQUEMIN/Alexandre DE STREEL (édit.), *L'intelligence artificielle et le droit*, format Kindle, Bruxelles 2017 [BUYLE/VAN DEN BRANDEN, *La robotisation de la justice*]

CHAPPUIS Benoît, *La profession d'avocat*, Tome II, 2e éd., collection « Quid Iuris », Genève/Zurich 2017 [CHAPPUIS, *La profession d'avocat, Tome II*]

CHAPPUIS Benoît/ALBERINI Adrien, « Secret professionnel de l'avocat et solutions *cloud* », in *Revue de l'avocat*, Vol. 20, No 8, 2017, p. 337-343 [CHAPPUIS/ALBERINI, *Secret professionnel*]

COMMISSION EUROPÉENNE, « Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques », Rapport final, présenté par LRDP KANTOR Ltd (Leader) en association avec le Centre for Public Reform, janvier 2010, disponible sur : https://publications.europa.eu/fr/publication-detail/-/publication/9c7a02b9-ecba-405e-8d93-a1a8989f128b [COMMISSION EUROPÉENNE, *Étude comparative*]

CONSEIL DES BARREAUX EUROPÉENS, « Conseils du CCBE pour le renforcement de la sécurité informatique des avocats contre la surveillance illégale », disponible sur :

https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommentations/FR_ITL_20160520_CCBE_Guidance_on_Improving_the_IT_Security_of_Lawyers_Against_Unlawful_Surveillance.pdf [https://perma.cc/U3AX-6SYP] [CCBE, *Conseils du CCBE pour le renforcement de la sécurité informatique des avocats*]

CONSEIL DES BARREAUX EUROPÉENS, « Évaluation du CCBE de la loi CLOUD Act des États-Unis », le 28 février 2019, disponible sur : https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/FR_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf [https://perma.cc/RLK6-PMZH] [CCBE, *Évaluation du CCBE de la loi CLOUD Act des États-Unis*]

CONSEIL DES BARREAUX EUROPÉENS, « Recommandations du CCBE sur la protection des droits fondamentaux dans le contexte de la « sécurité nationale » », 2019, disponible sur : https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/FR_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf [https://perma.cc/G738-HQSD] [CCBE, *Recommandations du CCBE sur la protection des droits fondamentaux dans le contexte de la « sécurité nationale »*]

CONSEIL DES BARREAUX EUROPÉENS, « Recommandations du CCBE : sur la protection du secret professionnel dans le cadre des activités de surveillance », disponible sur : https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/FR_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf [https://perma.cc/XK6U-CA5F] [CCBE, *Recommandations du CCBE*]

CONSEIL NATIONAL DES BARREAUX, *Guide de l'avocat numérique*, Paris 2016, disponible sur : https://encyclopedie.avocats.fr/GED_BWZ/109574692775/CNB_HD.pdf [https://perma.cc/PX96-WRHQ] [CONSEIL NATIONAL DES BARREAUX, *Guide de l'avocat numérique*]

CONSEIL NATIONAL DES BARREAUX/BARREAU DE PARIS/CONFÉRENCE DES BÂTONNIERS, *Guide pratique – Les avocats et le Règlement Général sur la Protection des Données (RGPD)*, 1ère éd., mars 2018, disponible sur : https://www.cnb.avocat.fr/sites/default/files/documents/guide_rgpd_avocats-2018.pdf [https://perma.cc/9DGL-8HXL] [CONSEIL NATIONAL DES BARREAUX/BARREAU DE PARIS/CONFÉRENCE DES BÂTONNIERS, *Guide pratique*]

CORBOZ Bernard, « Le secret professionnel de l'avocat selon l'art. 321 CP », in *SJ* 1993 p. 77-109 [CORBOZ, *Le secret professionnel de l'avocat*]

DAHIYAT Emad Abdel Rahim, « Intelligent Agents and Liability : Is it a Doctrinal Problem or Merely a Problem of Explanation ? », in *Artificial Intelligence and Law*, Vol. 18, No 1, mars 2010, p. 103-121 [DAHIYAT, *Intelligent Agents and Liability*]

DE TERWANGNE Cécile, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », in Céline CASTETS-RENARD, *Quelle protection des données personnelles en Europe ?*, 1ère éd., Bruxelles (Larcier) 2015, p. 81-120 [DE TERWANGNE, *La réforme de la Convention 108*]

DE TERWANGNE Cécile/ROSIER Karen, *Le Règlement général sur la protection des données (RGPD/GDPR), Analyse approfondie*, 1ère éd., Bruxelles (Larcier) 2018 [DE TERWANGNE/ROSIER, *Le Règlement général sur la protection des données*]

DEFFERRARD Fabrice/PAPINEAU Christelle, « Le pouvoir de *jurisdictio* des algorithmes aux États-Unis : entre fantasme et réalité jurisprudentielle », in Stéphane PREVOST/Erwan ROYER (édit.), *Intelligence artificielle*, Édition 2019, Grand Angle, Paris (Dalloz) 2019, p. 139-143 [DEFFERRARD/PAPINEAU, *Le pouvoir de jurisdictio des algorithmes*]

ESTEVA Andre/KUPREL Brett/NOVOA Roberto A./KO Justin/SWETTER Susan M./BLAU Helen M./THRUN Sebastian, « Dermatologist-Level Classification of Skin Cancer with Deep Neural Networks », in *Nature* 542, janvier 2017, p. 115-118, disponible sur : https://www.nature.com/articles/nature21056 [ESTEVA et al., *Dermatologist-Level Classification of Skin Cancer*]

FANTI Sébastien, « Courrier électronique et responsabilité de l'avocat », in *Revue de l'avocat*, Vol. 14, No 11/12, 2011, p. 492-493 [FANTI, *Courrier électronique*]

FAVRE Katia, *Sorgfaltspflichten bei der Datenübertragung*, thèse, Zurich 2006 [FAVRE, *Sorgfaltspflichten*]

FELLMANN Walter, « Haftung des Anwaltes für unterlassene oder fehlerhafte Datenbank-Recherchen », in Thomas KOLLER/Heinrich KOLLER (édit.), *Journées 2003 d'informatique juridique du 29 août 2003 à Berne*, Berne 2004 [FELLMANN, *Haftung des Anwaltes*]

FELLMANN Walter, *Anwaltsrecht*, 2e éd., Berne 2017 [FELLMANN, *Anwaltsrecht*]

FELLMANN Walter, Obligationenrecht, Die einzelnen Vertragsverhältnisse, Der einfache Auftrag, Art. 394-406 OR, in *Berner Kommentar* VI/2/4, 4e éd., Berne 1992 [BK-FELLMANN]

FELLMANN Walter/ZINDEL Gaudenz G. (édit.), *Kommentar zum Anwaltsgesetz*, 2e éd., Zurich 2011 [BGFA-AUTEUR]

FLORIDI Luciano/SANDERS J. W., « On the Morality of Artificial Agents », in *Minds and Machines*, Vol. 14, No 3, 2004, p. 349-379 [FLORIDI/SANDERS, *On the Morality of Artificial Agents*]

FRIEDMAN Gabe, « FBI Alert Warns of Criminals Seeking Access to Law Firm Network », in *Big Law Business*, le 11 mars 2016, disponible sur : https://biglawbusiness.com/fbi-alert-warns-of-criminals-seeking-access-to-law-firm-networks [https://perma.cc/HP9J-VBZF] [FRIEDMAN, *FBI Alert*]

FURRER Andreas/ECKERT Martin/GLARNER Andreas, *Legal Tech, Les termes les plus importants – Die wichtigsten Begriffe, Glossaire – Glossar*, Berne 2019 [FURRER et al., *Legal Tech*]

GANASCIA Jean Gabriel, « Devons-nous craindre l'intelligence artificielle ? Il y a IA et IA – Entretien avec Gabriel Ganascia », in *L'intelligence artificielle en pratique et en débat*, Paris Innovation Review, 2018, p. 73-79 [GANASCIA, *Devons-nous craindre l'intelligence artificielle ?*]

GOODMAN Bryce/FLAXMAN Seth, « European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation" », in *AI Magazine*, Vol. 38, No 3, 2017, p. 50-57, disponible sur : https://arxiv.org/pdf/1606.08813 [https://perma.cc/E9R7-SCV4] [GOODMAN/FLAXMAN, *European Union Regulations on Algorithmic Decision-Making*]

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES, *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, adoptées le 3 octobre 2017, version révisée et adoptée le 6 février 2018, disponible sur : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 [GROUPE DE TRAVAIL « ARTICLE 29 », *Lignes directrices*]

GURTNER Jérôme, « L'innovation et l'avenir de la profession d'avocat », in *Revue de l'avocat*, Vol. 20, No 1, 2017, p. 15-18 [GURTNER, *L'innovation et l'avenir de la profession d'avocat*]

GURTNER Jérôme, *La réglementation des sociétés d'avocats : entre protectionnisme et libéralisme – Étude de droit comparé*, Neuchâtel 2016 [GURTNER, *La réglementation des sociétés d'avocats*]

HAWADIER Bernard, *L'avocat face à l'Intelligence Artificielle*, format Kindle, (Librinova) 2018 [HAWADIER, *L'avocat*]

HILDEBRANDT Mireille, *Smart Technologies and the End(s) of Law – Novel Entanglements of Law and Technology*, Cheltenham (Edward Elgar Publishing) 2015 [HILDEBRANDT, *Smart Technologies and the End(s) of Law*]

HUFF George B. Jr./DIMARIA John A./RAST Claudia, « Achieving Preparedness through Alignment with Voluntary Consensus Standards » (Chapter 14 : Best Practices for Incident Response), in Jill D. RHODES/Robert S. LITT (édit.), *The ABA Cybersecurity Handbook – A Resource for Attorneys, Law Firms, and Business Professionals*, 2e éd., Chicago (ABA Publishing) 2017 [HUFF et al., *Achieving Preparedness through Alignment with Voluntary Consensus Standards*]

INTERNET SOCIETY'S ONLINE TRUST ALLIANCE, « 2018 Cyber Incident & Breach Trends Report, Review and Analysis of 2018 Cyber Incidents and Key Trends to Address », le 9 juillet 2019, disponible sur : https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf [https://perma.cc/FBW7-PSDJ] [INTERNET SOCIETY, *2018 Cyber Incident*]

ISRANI Ellora Thadaney, « When an Algorithm Helps Send You to Prison », in *The New York Times*, le 26 octobre 2017, disponible sur : https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html [https://perma.cc/PY3R-Y4U5] [ISRANI, *When an Algorithm Helps Send You to Prison*]

JACQUEMIN Hervé/HUBIN Jean-Benoît, « Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle », in Hervé JACQUEMIN/Alexandre DE STREEL (édit.), *L'intelligence artificielle et le droit*, format Kindle, Bruxelles 2017 [JACQUEMIN/HUBIN, *Aspects contractuels*]

KALINICH Kevin P./RHYNER James L., « Cyber Insurance for Law Firms and Legal Organizations » (Chapter 15), in Jill D. RHODES/Robert S. LITT (édit.), *The ABA Cybersecurity Handbook – A Resource for Attorneys, Law Firms, and Business Professionals*, 2e éd., Chicago (ABA Publishing) 2017 [KALINICH/RHYNER, *Cyber Insurance for Law Firms*]

KAMARINOU Dimitra/MILLARD Christopher/SINGH Jatinder, « Machine Learning with Personal Data », in Ronald LEENES/Rosamunde VAN BRAKEL/Serge GUTWIRTH/Paul DE HERT (édit.), *Data Protection and Privacy : The Age of Intelligent Machines*, Oxford (Hart Publishing) 2017, p. 89-114 [KAMARINOU et al., *Machine Learning with Personal Data*]

KATHRANI Paresh, « An "Existential" Shift ? Technology and Some Questions for the Legal Profession », in *Legal Ethics*, Vol. 20, No 1, 2017, p. 144-146 [KATHRANI, *An "Existential" Shift ?*]

KATZ Daniel Martin/BOMMARITO Michael J. II/BLACKMAN Josh, « A General Approach for Predicting the Behavior of the Supreme Court of the United States », in *PLoS ONE* 12(4): e0174698, 2017, disponible sur : https://doi.org/10.1371/journal.pone.0174698 [KATZ et al., *A general Approach*]

KILLIAS Martin/KUHN André/DONGOIS Nathalie, *Précis de droit pénal général*, 4e éd., Berne 2016 [KILLIAS/KUHN/DONGOIS, *Précis de droit pénal général*]

KOOPS Bert-Jaap/HILDEBRANDT Mireille/JAQUET-CHIFELLE David-Olivier, « Bridging the Accountability Gap : Rights for New Entities in the Information Society ? », in *Minnesota Journal of Law, Science & Technology*, Vol. 11, No 2, 2010, p. 497-561, disponible sur : https://serval.unil.ch/resource/serval:BIB_7C207F3B2BD5.P001/REF [https://perma.cc/BR74-HD3Z] [KOOPS et al., *Bridging the Accountability Gap*]

KORT Fred, « Predicting Supreme Court Decisions Mathematically : A Quantitative Analysis of the "Right to Counsel" Cases », in *American Political Science Review*, Vol. 51, No 1, 1957, p. 1-12 [KORT, *Predicting Supreme Court Decisions Mathematically*]

LASSEGUE Jean/GARAPON Antoine, *Justice digitale – Révolution graphique et rupture anthropologique*, format Kindle, Paris (Presses Universitaires de France) 2018 [LASSEGUE/GARAPON, *Justice digitale*]

LAWLOR Reed C., « What Computers Can Do : Analysis and Prediction of Judicial Decisions », in *American Bar Association Journal*, Vol. 49, No 4, 1963, p. 337-344 [LAWLOR, *What Computers Can Do*]

LEMKE Christian, « Chapitre 2. L'avenir des services juridiques. Conclusion », in Michel BENICHOU (édit.), *L'innovation et l'avenir de la profession d'avocat en Europe*, Bruxelles (Éditions Bruylant) 2017 [LEMKE, L'avenir des services juridiques – Conclusion]

LEVIATHAN Yaniv/MATIAS Yossi, « Google Duplex : An AI System for Accomplishing Real-World Tasks Over the Phone », in *Google AI Blog*, le 8 mai 2018, disponible sur : https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html [https://perma.cc/SE27-FXXG] [LEVIATHAN/MATIAS, *Google Duplex*]

MACALUSO Alain/MOREILLON Laurent/QUELOZ Nicolas, *Code pénal II*, Commentaire romand, Bâle 2017 [CR CPII-AUTEUR]

MALGIERI Gianclaudio/COMANDÉ Giovanni, « Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation », in *International Data Privacy Law*, Vol. 7, No 4, 2017, p. 243-265, disponible sur : https://doi.org/10.1093/idpl/ipx019 [MALGIERI/COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists*]

MALLARD Stéphane, *Disruption : Intelligence artificielle, fin du salariat, humanité augmentée*, format Kindle, Malakoff (Dunod) 2018 [MALLARD, *Disruption*]

MARKOVIC Milan, « Rise of the Robot Lawyers? », in Arizona Law Review, Vol. 61, 2019, p. 325-350, disponible sur : https://ssrn.com/abstract=3286380 [MARKOVIC, *Rise of the Robot Lawyers?*]

MCGINNIS John O./PEARCE Russell G., « The Great Disruption : How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services », in *Fordham Law Review*, Vol. 82, 2014, p. 3041-3066 [MCGINNIS/PEARCE, *The Great Disruption*]

METILLE Sylvain, « Annoncer les failles de sécurité n'est plus une option : nouvelles obligations lorsque des données personnelles sont exposées », in *Expert Focus*, No 11, 2017, p. 863-867 [METILLE, *Annoncer les failles de sécurité*]

MICHEL Anne, « « Panama Papers » : le cabinet Mossack Fonseca cesse ses activités », in *Le Monde*, le 15 mars 2018, disponible sur : https://www.lemonde.fr/evasion-fiscale/article/2018/03/15/panama-papers-le-cabinet-mossack-fonseca-cesse-ses-activites_5271058_4862750.html [https://perma.cc/KJE5-Q8GX] [MICHEL, *Panama Papers*]

MINSKY Marvin, « Steps Toward Artificial Intelligence », in *Proceedings of the IRE*, Vol. 49, No 1, 1961, p. 8-30, disponible sur: https://courses.csail.mit.edu/6.803/pdf/steps.pdf [https://perma.cc/9QSV-9CDQ] [MINSKY, *Steps Toward Artificial Intelligence*]

MITTELSTADT Brent Daniel/ALLO Patrick/TADDEO Mariarosaria/WACHTER Sandra/FLORIDI Luciano, « The Ethics of Algorithms : Mapping the Debate », in *Big Data & Society*, Vol. 3, No 2, 2016, disponible sur : https://doi.org/10.1177%2F2053951716679679 [MITTELSTADT et al., *The Ethics of Algorithms*]

MÜLLER Christoph, *Contrats de droit suisse*, Berne 2012 [MÜLLER, *Contrats*]

NATIONS UNIES, *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation, 1996, avec le nouvel article 5bis tel qu'adopté en 1998*, New York 1999, disponible sur : http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf [https://perma.cc/LZ4W-L4GA] [NATIONS UNIES, *Loi type de la CNUDCI*]

NEVEJANS Nathalie, Règles européennes de droit civil en robotique, Étude pour la Commission JURI, PE 571.379, 2016, disponible sur : http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_FR.pdf [https://perma.cc/2J8C-H43T] [NEVEJANS, *Règles européennes de droit civil en robotique*]

NOTHWANG William D./MCCOURT Michael J./ROBINSON Ryan M./BURDEN Samuel A./CURTIS J. Willard, « The Human Should be Part of the Control Loop ? », in *2016 Resilience Week (RWS)*, Chicago 2016, p. 214-220, disponible sur : http://faculty.washington.edu/sburden/_papers/NothwangRobinson2016resil.pdf [https://perma.cc/XU7W-W5SV] [NOTHWANG et al., *The Human Should be Part of the Control Loop ?*]

O'NEIL Cathy, *Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy*, New York (Crown) 2016 [O'NEIL, *Weapons of Math Destruction*]

ÖHNER Christian/GRAF Silke, « Lawyer Bots : Rise of the Machines », in Michele DESTEFANO/Guenther DOBRAUZ-SALDAPENNA (édit.), *New Suits : Appetite for Disruption in the Legal World*, Berne 2019, p. 271-287 [ÖHNER/GRAF, *Lawyer Bots*]

PAGALLO Ugo, *The Laws of Robots : Crimes, Contracts, and Torts*, format Kindle, Dordrecht (Springer) 2013 [PAGALLO, *The Laws of Robots*]

PARLEMENT EUROPEEN, *Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL))*, P8_TA(2017)0051, disponible sur : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//FR [https://perma.cc/MHR8-N5GB] [PARLEMENT EUROPEEN, *Résolution 2015/2103(INL)*]

ROCHFELD Judith, « L'encadrement des décisions prises par algorithme », in Stéphane PREVOST/Erwan ROYER (édit.), *Intelligence artificielle*, Édition 2019, Grand Angle, Paris (Dalloz) 2019, p. 11-18 [ROCHFELD, *L'encadrement des décisions prises par algorithme*]

ROUVROY Antoinette, « La robotisation de la vie ou la tentation de l'inséparation », in Hervé JACQUEMIN/Alexandre DE STREEL (édit.), *L'intelligence artificielle et le droit*, format Kindle, Bruxelles 2017 [ROUVROY, *La robotisation de la vie*]

RUGER Theodore W./KIM Pauline T./MARTIN Andrew D./QUINN Kevin M., « The Supreme Court Forecasting Project : Legal and Political Science Approaches to Predicting Supreme Court Decisionmaking », in *Columbia Law Review*, Vol. 104, 2004, p. 1150-1209 [RUGER et al., *The Supreme Court Forecasting Project*]

RUSSEL Stuart J./NORVIG Peter, *Artificial Intelligence – A Modern Approach*, 3e éd., Boston 2016 [RUSSEL/NORVIG, *Artificial Intelligence*]

SCHILLER Kaspar, *Schweizerisches Anwaltsrecht – Grundlagen und Kernbereich*, Zurich 2009 [SCHILLER, *Anwaltsrecht*]

SELBST Andrew D./POWLES Julia, « Meaningful Information and the Right to Explanation », in *International Data Privacy Law*, Vol. 7, No 4, 2017, p. 233-242, disponible sur : https://doi.org/10.1093/idpl/ipx022 [SELBST/POWLES, *Meaningful Information*]

SLOVAK BAR ASSOCIATION, « Code of Conduct for Processing of Personal Data by Lawyers under the EU General Data Protection Regulation (GDPR) », Approved by the Office for Personal Data Protection of the Slovak Republic by Decision No 00676/2018-Os-9 of 4 December 2018 and entered into force on 10 December 2018, disponible sur : https://www.sak.sk/blox/cms/sk/sak/doc/224/225/__docList__/rows/730/attr/name/preview [https://perma.cc/4XD7-VWK3] [SLOVAK BAR ASSOCIATION, *Code of Conduct for Processing of Personal Data by Lawyers under the EU GDPR*]

STRAUB Wolfgang, « « Durchklick » : Was bringt die IT der Anwaltskanzlei ? (Teil 1) », in *Revue de l'avocat*, Vol. 15, No 11-12, 2012, p. 521-525 [STRAUB, *Durchklick (Teil 1)*]

THEVENOZ Luc/WERRO Franz (édit.), *Code des obligations I*, Commentaire romand, 2e éd., Bâle 2012 [CR COI-AUTEUR]

THOMSON Lucy L., « Understand Cybersecurity Risks » (Chapter 2), in Jill D. RHODES/Robert S. LITT (édit.), *The ABA Cybersecurity Handbook – A Resource for Attorneys, Law Firms, and Business Professionals*, 2e éd., Chicago (ABA Publishing) 2017 [THOMSON, *Understand Cybersecurity Risks*]

TURNER Jacob, *Robot Rules, Regulating Artificial Intelligence*, Cham (Palgrave Macmillan) 2019 [TURNER, *Robot Rules*]

VON UNGERN-STERNBERG Antje, « Artificial Agents and General Principles of Law », le 28 janvier 2018, p. 1-22, disponible sur : https://ssrn.com/abstract=3111881 [VON UNGERN-STERNBERG, *Artificial Agents*]

WACHTER Sandra/MITTELSTADT Brent/FLORIDI Luciano, « Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation », in *International Data Privacy Law*, Vol. 7, No 2, 2017, p. 76-99, disponible sur : https://doi.org/10.1093/idpl/ipx005 [WACHTER et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*]

WAGNER Dominik/ZWIRNER Sonia, « Cyber Risk in Anwaltskanzleien – Schlussfolgerungen aus dem Panama-Papers-Skandal », in Leo STAUB, *Beiträge zu aktuellen Themen an der Schnittstelle zwischen Recht und Betriebswirtschaft III*, Zurich 2017, p. 161-184 [WAGNER/ZWIRNER, *Cyber Risk in Anwaltskanzleien*]

WELCH Chris, « Google Just Gave a Stunning Demo of Assistant Making an Actual Phone Call », in *The Verge*, le 8 mai 2018, disponible sur : https://www.theverge.com/2018/5/8/17332070/google-assistant-makes-phone-call-demo-duplex-io-2018 [https://perma.cc/VW42-2JCV] [WELCH, *Google Demo*]

WERRO Franz, *La responsabilité civile*, 3e éd., Berne 2017 [WERRO, *La responsabilité civile*]

WICKERS Thierry, « Conclusion. L'avenir de la profession d'avocat », in Michel BENICHOU (édit.), *L'innovation et l'avenir de la profession d'avocat en Europe*, Bruxelles (Éditions Bruylant) 2017, version numérique [WICKERS, *Conclusion. L'avenir de la profession d'avocat*]

WRIGHT Peter, *Cyber Security Toolkit*, The Law Society 2016 [WRIGHT, *Cyber Security Toolkit*]